Implementation Guide

Cloud Migration Factory on AWS

Cloud Migration Factory on AWS: Implementation Guide

Table of Contents

Coordinate and automate large scale migrations to the AWS Cloud using the Cloud Migration Factory on AWS solution

The Cloud Migration Factory on AWS solution is designed to coordinate and automate manual processes for large-scale migrations involving a substantial number of applications. This solution helps enterprises improve performance and prevents long cutover windows by providing an orchestration platform for migrating workloads to AWS at scale. AWS Professional Services, AWS Partners, and other enterprises have already used this solution to help customers migrate thousands of servers to the AWS Cloud.

This solution helps you to:

- Integrate the many different types of tools that support migration, such as discovery tools, migration tools, and configuration management database (CMDB) tools.
- Automate migrations that involve many small, manual tasks, which take time to run and are slow and hard to scale.

For a complete end-to-end deployment guide using this solution, refer to Automating large-scale server migrations with Cloud Migration Factory in the *AWS Prescriptive Guidance Cloud Migration Factory Guide*.

This implementation guide discusses architectural considerations and configuration steps for deploying the Cloud Migration Factory on AWS solution in the Amazon Web Services (AWS) Cloud. It includes links to AWS CloudFormation templates that launch and configure the AWS services required to deploy this solution using AWS best practices for security and availability.

The guide is intended for IT infrastructure architects, administrators, and DevOps professionals who have practical experience architecting in the AWS Cloud.

Use this navigation table to quickly find answers to these questions:

If you want to . . .	Read . . .
Know the cost for running this solution.	Cost

If you want to . . .	Read . . .
The estimated cost for running this solution in the `us-east-1` Region is USD $14.31 per month for AWS resources.	
Understand the security considerations for this solution.	Security
Know how to plan for quotas for this solution.	Quotas
Know which AWS Regions support this solution.	Supported AWS Regions
View or download the AWS CloudFormation templates included in this solution to automatically deploy the infrastructure resources (the "stack") for this solution.	AWS CloudFormation templates

Features and benefits

The solution provides the following features:

Manage, track and initiate you workload migration to AWS from a single web interface, supporting multiple target AWS accounts and regions.

Provided with Amazon S3 static web site hosting, or in private deployment from an Amazon EC2 instance running a web server. All activities performed by the solution are initiated from with a single web interface, provided by the solution. See Migration Factory web interface for details.

Prepackaged automation tasks to perform many of the tasks required to fully migrate workloads to AWS using AWS Application Migration Service.

The solution provides all the automation tasks required to migrate thousands of workloads to AWS without requiring scripting and with limited knowledge required to get started. All automations can be initiated from the web interface and behind the scenes use AWS System Manager to initiate and run the automation jobs on the provided automation server(s).

Customize the solution with automation packages and attribute schema extensions

The majority of migrations require custom automation tasks to be run for applications and other environmental specific reasons, Cloud Migration Factory on AWS supports user customization of the provided scripts as well as the ability to load custom script into the solution. The solution also allows for the migration metadata store to be extended in seconds, providing administrators the ability to add and remove attributes to the schema that are needing to be tracked or used during the migration.

Integration with Service Catalog AppRegistry and AWS Systems Manager Application Manager

This solution includes a Service Catalog AppRegistry resource to register the solution's CloudFormation template and its underlying resources as an application in both Service Catalog AppRegistry and AWS Systems Manager Application Manager. With this integration, you can centrally manage the solution's resources and enable application search, reporting, and management actions.

Use cases

Migrate and manage large-scale migrations of workloads to AWS

Enable a single pane of glass view of large-scale workload migrations to AWS. Providing prebuilt automation, reporting and role-based access via a single web interface designed specifically for migrations.

Concepts and definitions

This section describes key concepts and defines terminology specific to this solution:

application

A group of resources that make up a single business service or application.

wave

A group of applications that will be migrated in the same event. This could be based on affinity between one another, or any other reason.

server

Source server to be migrated.

database

Source database to be migrated.

pipeline

A chain of tasks used to automate migration patterns containing multiple scripts and manual activities. This helps you to automate application migrations and transformations.

> **Note**
>
> For a general reference of AWS terms, refer to the AWS Glossary.

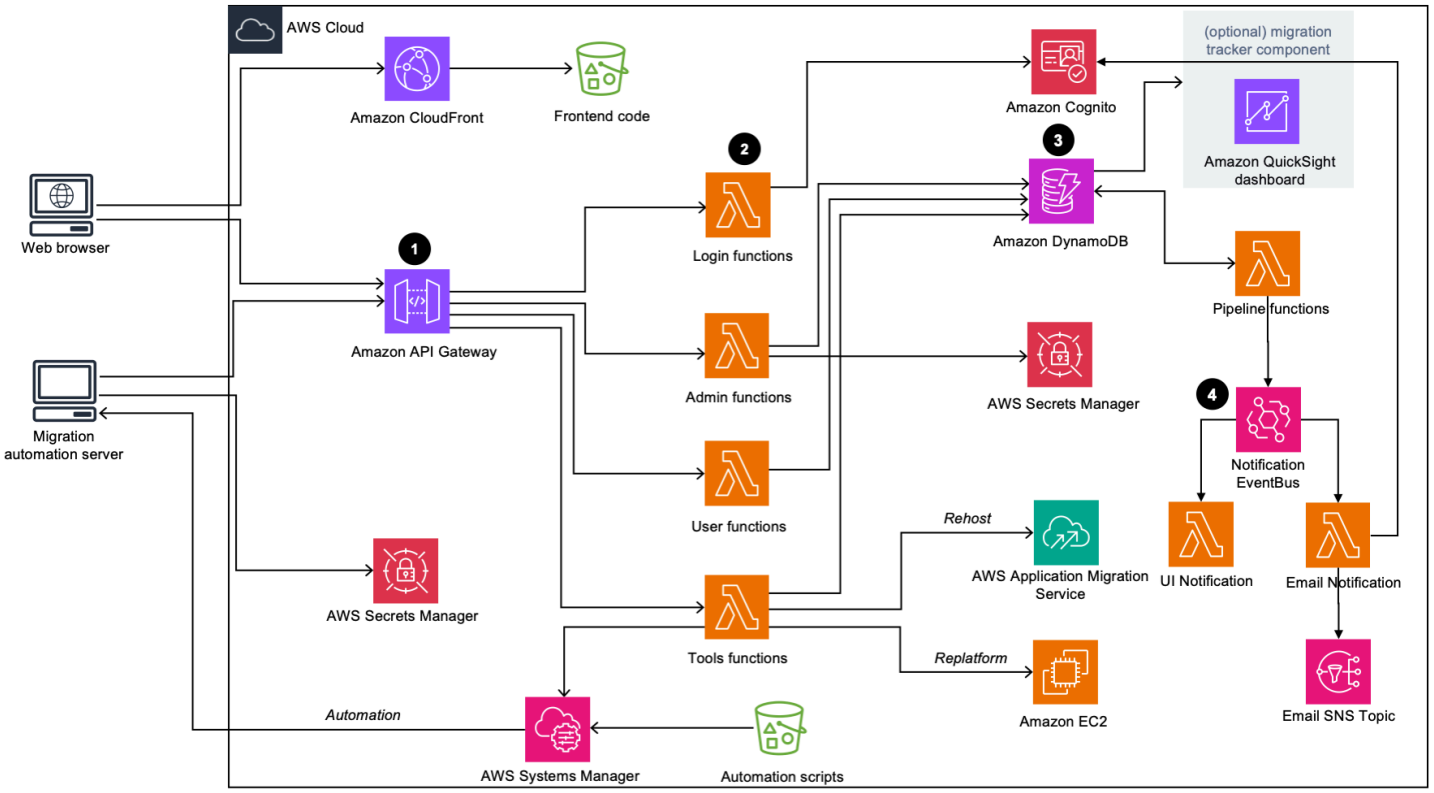
Architecture overview

This section provides a reference implementation architecture diagram for the components deployed with this solution.

Architecture diagram

Deploying the default solution builds the following serverless environment in the AWS Cloud.

Cloud Migration Factory on AWS architecture diagram



The solution's AWS CloudFormation template launches the AWS services necessary to help enterprises migrate their servers.

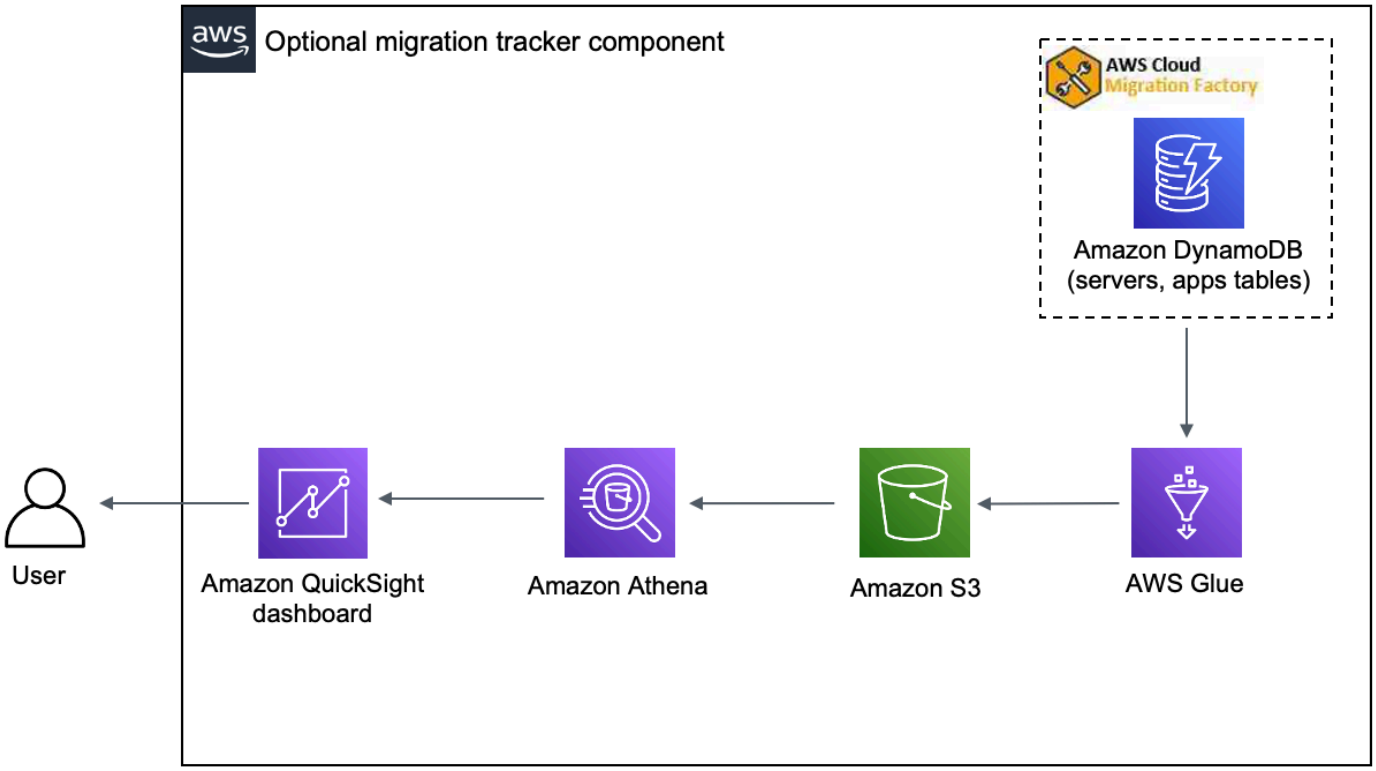
> **Note**
>
> The Cloud Migration Factory on AWS solution uses a migration automation server which is not a part of the AWS CloudFormation deployment. For more details on manually building the server, refer to Build a migration automation server.

1. Amazon API Gateway receives migration requests from the migration automation server through RestAPIs.
2. AWS Lambda functions provide the necessary services for you to log in to the web interface, perform the necessary administrative functions to manage the migration, and connect to third-party APIs to automate the migration process.
   - The `user` Lambda function ingests the migration metadata into an Amazon DynamoDB table. Standard HTTP status codes are returned to you through the Rest API from API Gateway. An Amazon Cognito user pool is used for user authentication to the web interface and Rest APIs, and you can optionally configure it to authenticate against external Security Assertion Markup Language (SAML) identity providers.
   - The `tools` Lambda function processes external Rest APIs and calls external tool functions, such as AWS Application Migration Service (AWS MGN) for AWS migration. The `tools` Lambda function also calls the Amazon EC2 for launching EC2 instances, and calls AWS Systems Manager to run automation scripts on the Migration Automation Server.
3. The migration metadata stored in Amazon DynamoDB is routed to the AWS MGN API to initiate Rehost migration jobs and launch servers. If your migration pattern is Replatform to EC2, the `tools` Lambda function launches CloudFormation templates in the target AWS account to launch Amazon EC2 instances.
4. All notifications are sent to a Notifications Event Bus. Event bridge rules set up to route UI notifications to the UI notifications lambda and Email notifications to the Email notifications lambda. The Email notifications lambda uses Amazon SNS to publish email notifications.

Optional migration tracker

This solution also deploys an optional migration tracker component that tracks the progress of your migration.

Optional migration tracker component



The CloudFormation template deploys AWS Glue to get the migration metadata from the Cloud Migration Factory DynamoDB table and exports the metadata to Amazon Simple Storage Service (Amazon S3) twice a day (at 5:00 AM and 1:00 PM UTC). After the AWS Glue job completes, an Amazon Athena save query is initiated, and you can set up Amazon QuickSight to pull the data from the Athena query results. You can then create the visualizations and build a dashboard that meets your business needs. For guidance on creating visuals and building a dashboard, refer to Build a migration tracker dashboard.

This optional component is managed by the **Tracker** parameter in the CloudFormation template. By default, this option is activated, but you can deactivate this option by changing the **Tracker** parameter to `false`.

AWS Well-Architected design considerations

This solution uses the best practices from the AWS Well-Architected Framework, which helps customers design and operate reliable, secure, efficient, and cost-effective workloads in the cloud.

This section describes how the design principles and best practices of the Well-Architected Framework benefit this solution.

Operational excellence

This section describes how we architected this solution using the principles and best practices of the operational excellence pillar.

- Resources defined as IaC using CloudFormation.
- All actions and audit logging sent to Amazon CloudWatch, allowing for automated responses to be deployed.

Security

This section describes how we architected this solution using the principles and best practices of the security pillar.

- IAM used for authentication and authorization.
- Role permissions scoped to be as narrow as possible, though in many cases this solution requires wildcard permissions to be able to act on any resources.
- Optional use of WAF to further secure the solution.
- Amazon Cognito and optional ability to federate with external IDPs.

Reliability

This section describes how we architected this solution using the principles and best practices of the reliability pillar.

- Serverless services allow the solution to provide a fault tolerant architecture.

Performance efficiency

This section describes how we architected this solution using the principles and best practices of the performance efficiency pillar.

- Serverless services allow the solution to scale as needed.

Cost optimization

This section describes how we architected this solution using the principles and best practices of the cost optimization pillar.

- Serverless services allow you to pay for only what you use.

Sustainability

This section describes how we architected this solution using the principles and best practices of the sustainability pillar.

- Serverless services allow you to scale up or down as needed.

Architecture details

Migration automation server

This solution leverages a migration automation server to run migrations using Rest APIs. This server isn't automatically deployed with the solution and must be built manually. For more information, refer to Build a Migration Automation Server. We recommend that you build the server in your AWS environment, but you can also build on-premises in your network environment. The server must meet the following requirements:

- Windows Server 2019 or later versions
- Minimum 4 CPUs with 8 GB RAM
- Deployed as a new virtual machine with no additional applications installed
- (If built in AWS) In the same AWS account and Region as Cloud Migration Factory

Once installed, the server requires internet access and non-restrictive internal network connectivity to the in-scope source servers (servers to be migrated to AWS).

If port restriction is required from the migration automation server to the source servers, the following ports must be open from the migration automation server to the source servers:

- SMB port (TCP 445)
- SSH port (TCP 22)
- WinRM port (TCP 5985, 5986)

We recommend that the migration automation server be in the same Active Directory domain as the source servers. If the source servers reside in multiple domains, the security configuration for the domain trust in each domain determines whether you need more than one migration automation server.

While the traditional approach uses a Windows-based automation server, scripts can now alternatively be executed directly through AWS Systems Manager Automation Document.

- If domain trust exists in all the domains with source servers, a single migration automation server will be able to connect to and run automation scripts for all domains.

- If a domain trust does not exist in all the domains, you must create an additional migration automation server for each untrusted domain, or for each action to be performed on the automation server alternative credentials will need to be provided with appropriate permissions on the source servers.

Migration services Rest APIs

The Cloud Migration Factory on AWS solution automates the migration process using Rest APIs that are processed through AWS Lambda functions, an Amazon API Gateway, AWS Managed Services, and AWS Application Migration Service (AWS MGN). When you make a request or initiate a transaction, such as adding a server or viewing a list of servers or applications, Rest API calls are made to Amazon API Gateway which initiates an AWS Lambda function to run the request. The following services detail the components for the automated migration process.

Log in services

Log in services include the `login` Lambda functions and Amazon Cognito. Once you log in to the solution using the `login` API via the API Gateway, the function validates the credentials, retrieves an authentication token from Amazon Cognito, and returns the token details back to you. You can use this authentication token to connect to the other services in this solution.

Admin services

Admin services include the Amazon API Gateway, `admin` Lambda functions, and Amazon DynamoDB. Administrators for the solution can use the `admin` Lambda function to define the migration metadata schema, which are the application and server attributes. The admin services API provides the schema definition for the DynamoDB table. User data including application and server attributes must adhere to this schema definition. Typical attributes include the `app_name`, `wave_id`, `server_name`, and other fields as identified in Import migration metadata into the factory. By default, the AWS CloudFormation template deploys a common schema automatically, but this can be customized after deployment.

Administrators can also use admin services to define migration roles for the members of their migration team. The administrator has granular control to map specific user roles to specific attributes and migration stages. A migration stage is a period of time to run certain migration tasks, for example, a build stage, a testing stage, and a cutover stage.

User services

User services include the Amazon API Gateway, `user` Lambda functions, and Amazon DynamoDB. Users can manage the migration metadata, allowing them to read, create, update, and delete the wave, application, and server data in the migration metadata pipeline.

> **Note**
>
> A migration wave is a concept of application grouping with a start and an end or cutover date. Wave data includes the migration candidate applications and application groupings scheduled for a particular migration wave.

User services offer an API for the migration team to manipulate the data in the solution: create, update, and delete the data using the Python script and source CSV files. For detailed steps, refer to Automated migration activities using Migration Factory web console and Automated migration activities using command prompt.

Tools services

Tool services upon deployment include the Amazon API Gateway, extensible `tools` Lambda functions, Amazon DynamoDB, AWS Managed Services, and AWS Application Migration Service. You can use these services to connect to third-party APIs and automate the migration process. On-deployment integration with AWS Application Migration Service can help a migration team to orchestrate the server launch process with a single button press to launch all servers in the same wave consisting of a group of applications and servers that have the same cutover date.

With the pipeline capability built into this solution, a migration team can compose complex migration sequences that contain many tasks, providing a fully managed and automated experience. The migration team can use tasks from the provided automation capabilities in the tools and AWS provided scripts, or write their own custom automation scripts.

Migration Factory web interface

The solution includes a Migration Factory web interface which can be hosted, by default in an Amazon S3 bucket, or on a provided web server (not part of the solution deployment) which allows you to complete the following tasks using a web browser:

- Update wave, application, and server metadata from your web browser

- Manage application and server schema definitions
- Create end-to-end migration pipelines to automate and manage all aspects of application migrations
- Run automation scripts to automate migration activities such as check prerequisites, install MGN agents
- Create migration credentials to connect to the source servers
- Connect to AWS services such as AWS Application Migration Service and AWS Systems Manager to automate the migration process

AWS services in this solution

AWS service	Description	
Amazon API Gateway	**Core.** Provides REST APIs to the whole solution, used to access backend data and initiate and manage migration automation tasks.	
AWS Lambda	**Core.** Provide the necessary services for you to log in to the web interface, perform the necessary administrative functions to manage the migration, and connect to third-party APIs to automate the migration process.	
Amazon DynamoDB	**Core.** Metadata store for all user and system managed data, accessed via Amazon API Gateways and Lambda functions.	
Amazon Cognito	**Core.** User authorization and authentication, optional	

AWS service	Description	
	federation with other IDPs is also achieved through Amazon Cognito.	
AWS Systems Manager	**Supporting.** Supports the running of Cloud Migration Factory on AWS automatio n packages on the customer provided Automation server.	
Amazon EC2	**Supporting.** Automation server running AWS Systems Manager agents to allow running of automation packages.	
Amazon S3	**Supporting.** Used in multiple areas of the solution, 1/ using the static web hosting feature of Amazon S3, it serves the main web interface (via Amazon CloudFront), 2/ logs and other automation outputs are stored in Amazon S3 by the solution.	
AWS Secrets Manager	**Supporting.** When using the automation features of the solution, AWS Secrets Manager is used to securely store the credentials that are used to access migrating resources in order to run tasks and actions to facilitate and migrate workloads.	

AWS service	Description	
Amazon CloudFront	**Optional.** For standard deployments Amazon CloudFront provides the distribution of the web interface content from Amazon S3, making it highly available globally, and providing secure TLS access to the web interface content from anywhere.	
AWS Application Migration Service (AWS MGN)	**Optional.** When performing rehost migrations of Windows or Linux workloads, Cloud Migration Factory on AWS uses AWS MGN to facilitat e the system migration to Amazon EC2.	
Amazon QuickSight	**Optional.** Allows for customizable migration dashboards to be created based on the data stored in the migration metastore held in Amazon DynamoDB, providing teams the data they need to track and report on their migrations.	

AWS service	Description	
AWS Glue	**Optional.** Regularly extracts data held in Amazon DynamoDB to Amazon S3, providing reporting data for use in Amazon Athena and Amazon QuickSight dashboards.	
Amazon Athena	**Optional.** Provides access to reporting data extracted by AWS Clue from the migration metadata, allowing dashboards to be created using Amazon QuickSight.	
AWS Web Application Firewall	**Optional.** Apply additiona l security on the endpoints for Amazon API Gateway and Amazon CloudFront to restrict access to specific devices based on source IP address or other access criteria.	

Plan your deployment

This section helps you plan your cost, security, AWS Regions, and deployment types for the Cloud Migration Factory on AWS solution.

Cost

You are responsible for the cost of the AWS services used while running this solution. As of this revision, the estimated cost for running this solution with default settings in the US East (N. Virginia) Region and assuming that you are migrating 200 servers a month with this solution is approximately **$14.31 per month**. The cost for running this solution depends on the amount of data being loaded, requested, stored, processed, and presented as shown in the following table.

AWS service	Factors	Cost/month [USD]
Core services		
Amazon API Gateway	10,000 requests/month x ($3.50/million)	$0.035
AWS Lambda	10,000 invocations/month (avg 3,000 ms duration and 128 MB memory)	$0.065
Amazon DynamoDB	20,000 write requests/month x ($1.25/million) 40,000 read requests/month x ($0.25/million) Data storage: 1 GB x $0.25	$0.035
Amazon S3	Storage (10MB) & 50,000 get requests/month	$0.25
Amazon CloudFront	Regional data transfer out to internet: first 10 TB	$0.92

AWS service	Factors	Cost/month [USD]
	Regional data transfer out to origin: all data transfer HTTPS requests: 50,000 requests/month X ($0.01/10,000 requests)	
AWS Systems Manager	10,000 steps/month	$0.00
AWS Secrets Manager	5 secrets x 30 days duration	$2.00
Amazon Cognito (direct sign-in)	Up to 50,000 monthly active users (MAUs) covered by AWS Free Tier	$0.00
Amazon Athena	10MB daily x $5.00 per TB of data scanned	$0.0015
Optional services		
AWS Glue (optional migration tracker)	2 mins daily x Default 10 DPU x $0.44 per DPU-Hour	$4.40
AWS WAF	2 Web ACLs $5.00 per month (prorated hourly)2 Rules $1.00 per month (prorated hourly) 10,000 requests x ($0.60 per 1 million requests)	$6.60
Amazon Cognito (SAML sign-in)	Up to 50 MAUs covered by AWS Free TierAbove 50 MAUs, $0.015/MAU	$0.00
	Total:	**~$14.31/month**

(Recommended) Deploy an Amazon Elastic Compute Cloud instance to help run automation scripts

We recommend deploying an Amazon Elastic Compute Cloud (Amazon EC2) instance to automate the connection to the solution's APIs and AWS Boto3 APIs with IAM roles. The following cost estimate assumes that the Amazon EC2 instance is located in the `us-east-1` Region and runs eight hours a day, five days a week.

AWS service	Factors	Cost/month [USD]
Amazon EC2	176 hours a month x $0.1108/per hour (`t3.large`)	$19.50
Amazon Elastic Block Store (Amazon EBS)	30 GB x $0.08/GB-month (gp3) x (176 hours/720 hours)	$0.59
	Total:	**~$20.09**

Prices are subject to change. For full details, refer to the pricing webpage for each AWS service you will be using in this solution.

Security

When you build systems on AWS infrastructure, security responsibilities are shared between you and AWS. This shared model can reduce your operational burden as AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. For more information about security on AWS, visit AWS Cloud Security.

IAM roles

AWS Identity and Access Management (IAM) roles allow you to assign granular access policies and permissions to services and users in the AWS Cloud. This solution creates IAM roles that grants the AWS Lambda function access to the other AWS services used in this solution.

Amazon Cognito

The Amazon Cognito user created by this solution is a local user with permissions to access only the RestAPIs for this solution. This user does not have permissions to access any other services in your AWS account. For more information, refer to Amazon Cognito User Pools in the *Amazon Cognito Developer Guide*.

The solution optionally supports external SAML sign-in through the configuration of federated identity providers and the hosted UI functionality of Amazon Cognito.

Amazon CloudFront

This default solution deploys a web console hosted in an Amazon S3 bucket. To help reduce latency and improve security, this solution includes an Amazon CloudFront distribution with an origin access identity, which is a special CloudFront user that helps provide public access to the solution's website bucket contents. For more information, refer to Restricting Access to Amazon S3 Content by Using an Origin Access Identity in the *Amazon CloudFront Developer Guide*.

If a **private** deployment type is selected during stack deployment, then a CloudFront distribution is not deployed, and requires that another web hosting service is used to host the web console.

AWS WAF - Web Application Firewall

If deployment type selected in the stack is Public with AWS WAF then the CloudFormation will deploy the required AWS WAF Web ACLs and Rules configured to protect CloudFront, API Gateway, and Cognito endpoints created by the CMF solution. These endpoints will be restricted to allow only specified source IP addresses to access these endpoints. During stack deployment, two CIDR ranges must be supplied with the facility to add additional rules after deployment via the AWS WAF console.

> **Important**
>
> When configuring WAF IP restrictions, ensure that the IP address of your CMF automation server or the outgoing NAT Gateway IP is included in the allowed CIDR ranges. This is critical for the proper functioning of CMF automation scripts that need to access the solution's API endpoints.

Supported AWS Regions

This solution uses Amazon Cognito and Amazon QuickSight, which are currently available in specific AWS Regions only. Therefore, you must launch this solution in a Region where these services are available. For the most current service availability by Region, refer to the AWS Regional Services List.

Note

Data transfer during the migration process is not affected by Regional deployments.

Cloud Migration Factory on AWS is available in the following AWS Regions:

Region names	
US East (Ohio)	Canada (Central)
US East (N. Virginia)	*Canada West (Calgary)
US West (N. California)	Europe (Frankfurt)
US West (Oregon)	Europe (Ireland)
*Africa (Cape Town)	Europe (London)
*Asia Pacific (Hong Kong)	*Europe (Milan)
*Asia Pacific (Hyderabad)	*Europe (Spain)
*Asia Pacific (Jakarta)	Europe (Paris)
*Asia Pacific (Melbourne)	Europe (Stockholm)
Asia Pacific (Mumbai)	*Europe (Zurich)
Asia Pacific (Osaka)	*Israel (Tel Aviv)
Asia Pacific (Seoul)	*Middle East (Bahrain)
Asia Pacific (Singapore)	*Middle East (UAE)

Region names	
Asia Pacific (Sydney)	South America (São Paulo)
Asia Pacific (Tokyo)	

Important

*Only available for private deployment type due to Amazon CloudFront access logging, see Configuring and using standard logs (access logs) in the *Amazon CloudFront Developer Guide* for latest details.

Cloud Migration Factory on AWS is not available in the following AWS Regions:

Region name	Unavailable service(s) or service option
AWS GovCloud (US-East)	Amazon Cognito
AWS GovCloud (US-West)	Amazon Cognito

Quotas

Service quotas, also referred to as limits, are the maximum number of service resources or operations for your AWS account.

Quotas for AWS services in this solution

Make sure you have sufficient quota for each of the services implemented in this solution. For more information, refer to AWS service quotas.

Select one of the following links to go to the page for that service. To view the service quotas for all AWS services in the documentation without switching pages, view the information in the Service endpoints and quotas page in the PDF instead.

AWS CloudFormation quotas

Your AWS account has CloudFormation quotas that you should be aware of when launching the stack for this solution. By understanding these quotas, you can avoid limitation errors that would prevent you from deploying this solution successfully. For more information, refer to AWS CloudFormation quotas in the *AWS CloudFormation Users Guide*.

Deploy the solution

This solution uses AWS CloudFormation templates and stacks to automate its deployment. The CloudFormation template(s) specifies(y) the AWS resources included in this solution and their properties. The CloudFormation stack provisions the resources that are described in the template(s).

Prerequisites

Source server permissions

A domain user with local admin permissions to the in-scope source servers targeted for migration is required for Windows and Linux (sudo permissions) servers. If source servers are not in a domain, other users may be used, including an LDAP user with sudo/administrator permissions or a local sudo/administrator user. Before launching this solution, verify that you have the necessary permissions or have coordinated with the appropriate person in your organization with permissions.

AWS Application Migration Service (AWS MGN)

If you use AWS MGN for this solution, you must first initialize the AWS MGN service in every target account and region before launching the target account stack, refer to Initializing Application Migration Service in the *Application Migration Service User Guide* for more details.

Private deployment

If you have chosen to deploy a **Private** instance of CMF, deploy a web server in your environment before proceeding with the CMF solution deployment.

AWS CloudFormation templates

This solution uses AWS CloudFormation to automate the deployment of the Cloud Migration Factory on AWS solution in the AWS Cloud. It includes the following AWS CloudFormation template, which you can download before deployment.

View template

aws-cloud-migration-factory-solution.template - Use this template to launch the Cloud

Migration Factory on AWS solution and all associated components. The default configuration deploys AWS Lambda functions, Amazon DynamoDB tables, an Amazon API Gateway, Amazon CloudFront, Amazon S3 buckets, an Amazon Cognito user pool, AWS Systems Manager Automation Document, and AWS Secrets Manager secrets, but you can also customize the template based on your specific needs.

View template

aws-cloud-migration-factory-solution-target-account.template - Use this template to launch the Cloud Migration Factory on AWS solution target account(s). The default configuration deploys IAM roles and a user, but you can also customize the template based on your specific needs.

Deployment process overview

Before you launch the automated deployment, review the architecture, components, and other considerations discussed in this guide. Follow the step-by-step instructions in this section to configure and deploy the Cloud Migration Factory on AWS solution into your account.

Time to deploy: Approximately 20 minutes

> **Note**
>
> If you deploy this solution to AWS Regions other than US East (N. Virginia), the Migration Factory CloudFront URL may take longer to become available. During this time, you will receive an **Access Denied** message when accessing the web interface.

Step 1: Choose your deployment option

Step 2: Launch the Stack

Step 3: Launch the target account stack in the target AWS account

Step 4: Create the first user

Step 5: (Optional) Deploy private web console static content

Step 6: Update the factory schema

Step 7: Build a migration automation server

Step 8: Test the solution using the automation scripts

Step 9: (Optional) Build a migration tracker dashboard

Step 10: (Optional) Configure additional identity providers in Amazon Cognito

Important

This solution includes an option to send anonymized operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Notice.

To opt out of this feature, download the template, modify the AWS CloudFormation mapping section, and then use the AWS CloudFormation console to upload your updated template and deploy the solution. For more information, see the Anonymized data collection section of this guide.

Step 1: Choose your deployment option

There are three options for deployment of the initial stack and choosing the correct one depends on the security policies for the target environment.

These options are:

- Public (default): All Cloud Migration Factory on AWS endpoints are publicly addressable with user authentication. This option deploys the following entry points: CloudFront, Public API Gateway Endpoints, and Cognito.
- Public with AWS WAF: Access to Cloud Migration Factory endpoints is restricted to customizable CIDR ranges. This option deploys the following entry points: CloudFront, Public API Gateway Endpoints, Cognito, and AWS WAF restricting access to specific CIDR ranges.
- Private: All Cloud Migration Factory endpoints are accessible only from your VPC networks and the Cloud Migration Factory on AWS web console must be hosted on a private web server deployed separately. This option deploys the following entry points: Private API Gateway Endpoints (accessible within a VPC only) and Cognito.

Step 2: Launch the stack

Important

This solution includes an option to send anonymized operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. AWS owns the data gathered though this survey. Data collection is subject to the AWS Privacy Policy.

To opt out of this feature, download the template, modify the AWS CloudFormation mapping section, and then use the AWS CloudFormation console to upload your template and deploy the solution. For more information, refer to the Anonymized data collection section of this guide.

This automated AWS CloudFormation template deploys the Cloud Migration Factory on AWS solution in the AWS Cloud.

Note

You are responsible for the cost of the AWS services used while running this solution. Refer to the Cost section for more details. For full details, refer to the pricing webpage for each AWS service you will be using in this solution.

1. Sign into AWS Management Console and select the button to launch `cloud-migration-factory-solution` CloudFormation template.

   Launch solution

   You can also download the template as a starting point for your own implementation.
2. The template launches in the US East (N. Virginia) Region by default. To launch this solution in a different AWS Region, use the Region selector in the console navigation bar.

   Note

   This solution uses Amazon Cognito and Amazon QuickSight, which are currently available in specific AWS Regions only. Therefore, you must launch this solution in an

AWS Region where these services are available. For the most current availability by Region, refer to the AWS Regional Services List.
When deployed in Public and Public with WAF deployment types, the solution also uses Amazon CloudFront logging to Amazon S3. Today, log delivery from Amazon CloudFront to Amazon S3 is only available in specific Regions. Refer to Choosing an Amazon S3 bucket for your standard logs to verify your Region is supported.

3. On the **Create stack** page, verify that the correct template URL shows in the **Amazon S3 URL** text box and choose **Next**.
4. On the **Specify stack details** page, assign a name to your solution stack.
5. Under **Parameters**, review the parameters for the template and modify them as necessary. This solution uses the following default values.

Parameter	Default	Description
Application name	`migration-factory`	Enter a prefix to the AWS CloudFormation **Physical ID** that identifies the AWS services deployed by this solution.NOTE: The **Application name** is used as a prefix to identify the AWS resources that are deployed: *<application-name>* -*<environment-name>* -*<aws-resource>* . If you change the default name, we recommend that you keep the combined prefix labels to 40 characters or less to ensure that you don't exceed character limitations.
Environment name	`test`	Enter a name to identify the network environme nt where the solution is

Parameter	Default	Description
		deployed. We recommend a descriptive name such as `test`, `dev`, or `prod`. NOTE: The **Environment name** is used as a prefix to identify the AWS resources that are deployed: *<application-name>* -*<environment-name>* -*<aws-resource>* . If changing the default name, we recommend that you keep the combined prefix labels to 40 character s or less to ensure you do not exceed character limitations.
Migration Tracker	`true`	By default, the optional migration tracker dashboard is activated, but you can deactivate it by changing this parameter to `false`.
Replatform EC2	`true`	By default, the Replatfor m EC2 feature is activated, but you can deactivate it by changing this parameter to `false`.
ServiceAccountEmail	`serviceaccount@you rdomain.com`	Default service account email address, the migration factory automation scripts use this account to connect to the factory API.

Parameter	Default	Description
Allow additional identity provider to be configured in Cognito	`false`	By default, the solution uses Amazon Cognito to create and manage access. Changing this parameter to `true` will configure the solution to allow external SAML identity providers to be added to Amazon Cognito and used to sign in.
Deployment Type	`Public`	By default, the deploymen t type is `Public`, and all Cloud Migration Factory endpoints are publicly accessible with user authentication. **Public with AWS WAF**: Access to CMF endpoints is restricted to customizable CIDR ranges. We recommend this option based on AWS security best practices. **Private**: All Cloud Migration Factory endpoints are accessible only from your VPC networks and the Cloud Migration Factory Web UI must be hosted on a private web server deployed separately.
(Optional) Private Deployment Type Only		

Parameter	Default	Description
Full URL used to access web user interface	`[not set]`	Required when **Deployment Type** is set to `Private`. Specify the migration factory web interface URL that will serve the static web content. Example https://cmf.yourdomain.local. **Important** • Do not add a trailing forward slash to the URL, this will cause the web interface to fail when loading. • In private deployments a web server is required to host the static content and needs to be deployed before deployment of the CloudFormation template.
VPC ID to host API Gateway Endpoints	`[not set]`	Required when **Deployment Type** is set to `Private`. Specify a single VPC ID where the private API Gateway endpoints will be created.

Parameter	Default	Description
Subnets to host API Gateway Interface Endpoints	`[not set]`	Required when **Deployment Type** is set to `Private`. Specify a two Subnet IDs where the private API Gateway endpoints will be created. The Subnet IDs specified have to be within the VPC specified above.
(Optional) Public with AWS WAF Deployment Type Only		

Parameter	Default	Description
Allowed CIDR	`[not set]`	Required when **Deployment Type** is set to `Public with AWS WAF`. Specify two CIDR ranges from which the users and the automation server will be accessing the endpoints from. **Important** • You must specify 2 CIDR ranges. • The IP address of the CMF automation server OR the outgoing NAT Gateway IP must be included in the allowed IP addresses. Without the internal IP of the CMF EC2 instance OR the NAT Gateway IP, the CMF automation scripts will fail to access the solution endpoints. • Once deployed, it is possible to add additional ranges and restrictions to

Parameter	Default	Description
		the AWS WAF rules as required.

6. Choose **Next**.
7. On the **Configure stack options** page, choose **Next**.
8. On the **Review** page, review and confirm the settings. Check the boxes acknowledging that the template will create AWS Identity and Access Management (IAM) resources and that it might require the capability **CAPABILITY_AUTO_EXPAND**.
9. Choose **Submit** to deploy the stack.

   You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a **CREATE_COMPLETE** status in approximately 20 minutes.

Important

If you are using AWS MGN, you must complete the prerequisite for AWS MGN before continuing to Step 3.

Step 3: Launch the target account stack in the target AWS account

This automated AWS CloudFormation template deploys IAM roles in the target AWS account to allow the factory account to assume roles and perform MGN actions in the target account. Repeat this step for each target account. If the factory stack in the previous step is a target account, it will need to have this target stack deployed to it.

Note

The target account must be initialized for AWS Application Migration Service before launching this stack, refer to Initializing Application Migration Service in the *Application Migration Service User Guide* for more details.

The target account stack must be launched in the same Region as the factory stack in the previous step regardless of which Region will be used as the migration target Region. This stack is for cross account permissions only.

1. Sign in to the AWS CloudFormation console. Choose **Create stack** then select **With new resources**, to start the deployment of the template. You can also download the template as a starting point for your own implementation.
2. On the **Specify stack details** page, assign a name to your solution stack.
3. Under **Parameters**, review the parameters for the template and modify them as necessary. This solution uses the following default values.

Parameter	Default	Description
FactoryAWSAccountId	111122223333	Enter an account ID where the Migration Factory was deployed. **Note** Launch this stack in the same AWS Region as the Migration Factory stack.
Replatform	Yes	Turn on this option if you plan to use the Replatform EC2 module of this solution
RehostMGN	Yes	Turn on this option if you plan to use the Rehost MGN module of this solution

4. Choose **Next**.
5. On the **Configure stack options** page, choose **Next.**

6. On the **Review** page, review and confirm the settings. Check the box acknowledging that the template will create AWS Identity and Access Management (IAM) resources.
7. Choose **Submit** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a **CREATE_COMPLETE** status in approximately 5 minutes.

Step 4: Create the first user

Create the initial user and log in to the solution

Use the following procedure to create the initial user.

1. Navigate to the Amazon Cognito console.
2. From the navigation pane, choose **User pools**.
3. On the **User pools** page, choose the user pool that starts with the `migration-factory` prefix.
4. Select the **Users** tab and choose **Create user**.
5. In the **Create user** screen, **User information** section, do the following:
   a. Verify that the **Send an invitation** option is selected.
   b. Enter an email address.

> **Important**
>
> This email address must be different from the one you used in the `ServiceAccountEmail` parameter, which the solution uses when deploying the primary CloudFormation template.

   c. Select **Set a password**.
   d. In the **Password** field, enter a password.

> **Note**
>
> The password must be at least eight characters in length, including upper- and lower-case letters, numbers, and special characters.

6. Choose **Create user**.

> **Note**
>
> You will receive an email with the temporary password. Until you change the temporary password, the **Account status** for this user will display as **Force change password**. You can update the password later in the deployment.

Add a user to the admin group

In the Amazon Cognito console, use the following procedure to add a user to the default Admin group.

1. Navigate to the Amazon Cognito console.
2. From the navigation menu, choose **User pools**.
3. On the **User pools** page, choose the user pool that starts with the `migration-factory` prefix.
4. Select the **Groups** tab and open the group named **admin** by selecting the name.
5. Choose **Add user to group**, then select the user name to add.
6. Choose **Add**.

   The chosen user will now be added to the members list of the group. This default admin group authorizes the user to manage all aspects of the solution.

   > **Note**
   >
   > After you create the initial users, you can manage group membership in the solution UI by selecting **Administration**, then **Permissions**, then **Groups**.

Identify the CloudFront URL (Public and Public with AWS WAF deployments only)

Use the following procedure to identify the solution's Amazon CloudFront URL. This allows you to log in and change the password.

1. Navigate to the AWS CloudFormation console and select the solution's stack.
2. On the **Stacks** page, select the **Outputs** tab and select the **Value** for the **MigrationFactoryURL**.

> **Note**
>
> If you launched the solution in an AWS Region other than US East (N. Virginia), CloudFront may take longer to deploy and the **MigrationFactoryURL** may not be accessible immediately (you will receive an access denied error). It can take up to four hours before the URL becomes available. The URL includes `cloudfront.net` as part of the string.

3. Sign in with your username and temporary password, then create a new password and choose **Change Password**.

> **Note**
>
> The password must be at least eight characters in length, including upper- and lower-case letters, numbers, and special characters.

Step 5: (Optional) Deploy private web console static content

If you selected the Private deployment type during the stack deployment, you are required to manually deploy the CMF web console code to the web server that you created and then specified in **Full URL used to access web user interface** parameter of the stack. For all other deployment types, skip this step.

Setup and configuration instructions for each web server are different, so this guide will only provide generic instructions on where to copy the content from, and you should configure the web server to your own requirements before updating the content.

1. Ensure that the web server has access to S3, and the AWS CLI installed and configured. Alternatively, download the contents of the front-end bucket and copy them to the web server using another device.
2. Using the AWS CLI, run the following command, replacing the environment name with the one specified during the stack deployment, AWS account ID with the ID of the AWS account the stack was deployed into, and the target directory with that of the web server's default root directory. This will copy the static Cloud Migration Factory web console code along with the specific configuration needed for this Cloud Migration Factory solution deployment:

Windows example:

```
aws s3 cp s3://migration-factory-<environment name>-<AWS Account Id>-front-end/ C:
\inetpub\wwwroot --recursive
```

Linux example:

```
aws s3 cp s3://migration-factory-<environment name>-<AWS Account Id>-front-end/ /var/
www/html --recursive
```

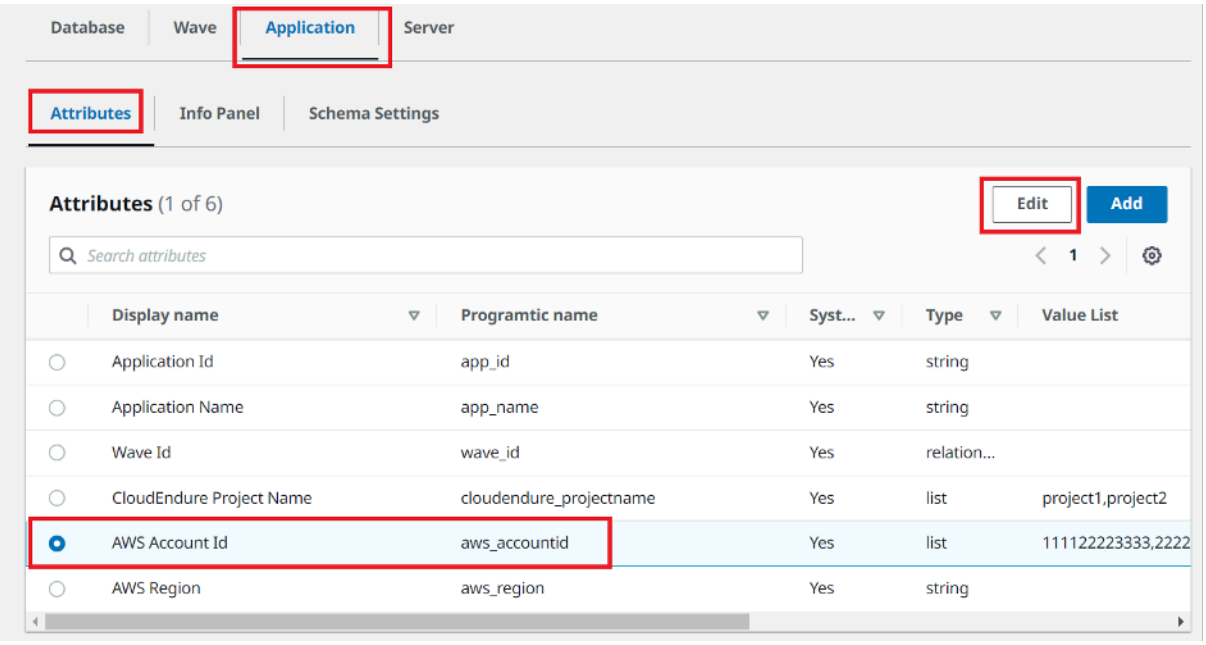
> **Note**
>
> If an update is made to the stack parameters, it is required to replace the files on the web server from the frontend bucket to ensure that any configuration changes are available to the web console.

Step 6: Update the factory schema

Update the target AWS Account Id for AWS MGN migrations

1. On the **Migration Factory** web interface, select **Administration**, then select **Attributes**.
2. On the **Attribute Configuration** page, select **Application**, then select **Attributes**.
3. Select **AWS Account Id**, then choose **Edit**.

Migration Factory web interface Attribute Details tab



4. On the **Amend attribute** page, update * Value list* with your target AWS account IDs and choose **Save**.

> **Note**
>
> If you have more than one AWS account ID, separate the ID with commas.

Step 7: Configuring a migration automation server

The migration automation server is used to run migration automation.

Build a Windows Server 2019 or later server

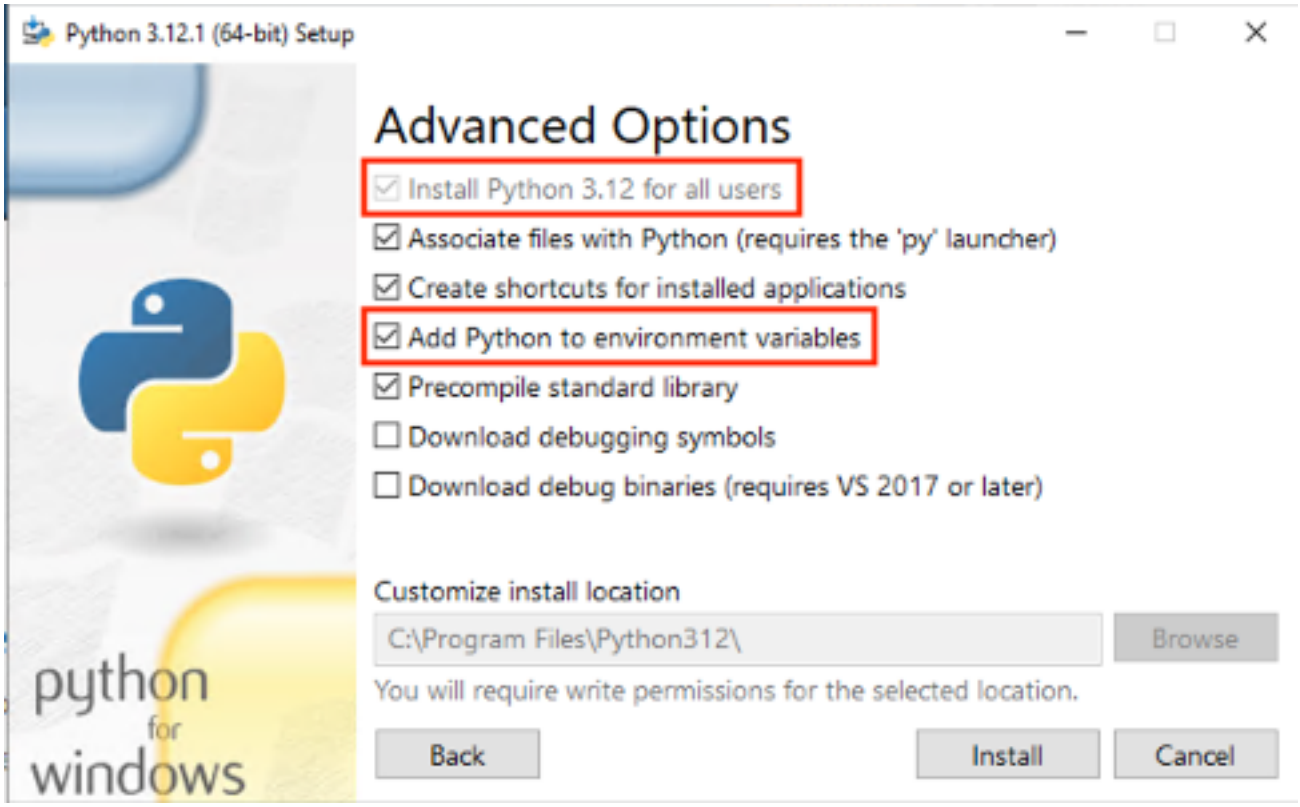
We recommend creating the server in your AWS account, but it can also be created in your on-premises environment. If built in an AWS account, it must be in the same AWS account and Region as Cloud Migration Factory. To review the server requirements, refer to Migration automation server.

Wherever you deploy the Windows instance, it should be deployed as a standard Windows 2019 or later installation that meets your security and operational requirements.

Installing required software to support the automations

1. Download Python v3.12.1.
2. Log in as administrator and install Python v3.12.1, and choose **Customize installation**.
3. Choose **Next**, and select **Install for all users** and **Add Python to environment variables**. Choose **Install**.

   Migration Factory web interface Attribute Details tab



4. Verify that you have administrator privileges, open `cmd.exe`, and run the following commands to install the Python packages one at a time:

```
python -m pip install requests
python -m pip install paramiko
python -m pip install boto3
```

   If any of these commands fail, upgrade pip by running the following command:

```
python -m pip install --upgrade pip
```

5. Install AWS CLI (Command Line Interface).

6. Install using the PowerShell for AWS module , ensuring that you have the *-Scope AllUsers * parameter included in the command.

```
Install-Module -Name AWSPowerShell -Scope AllUsers
```

7. Open PowerShell Script Execution, by opening the PowerShell CLI as Administrator and run the following command:

```
Set-ExecutionPolicy RemoteSigned
```

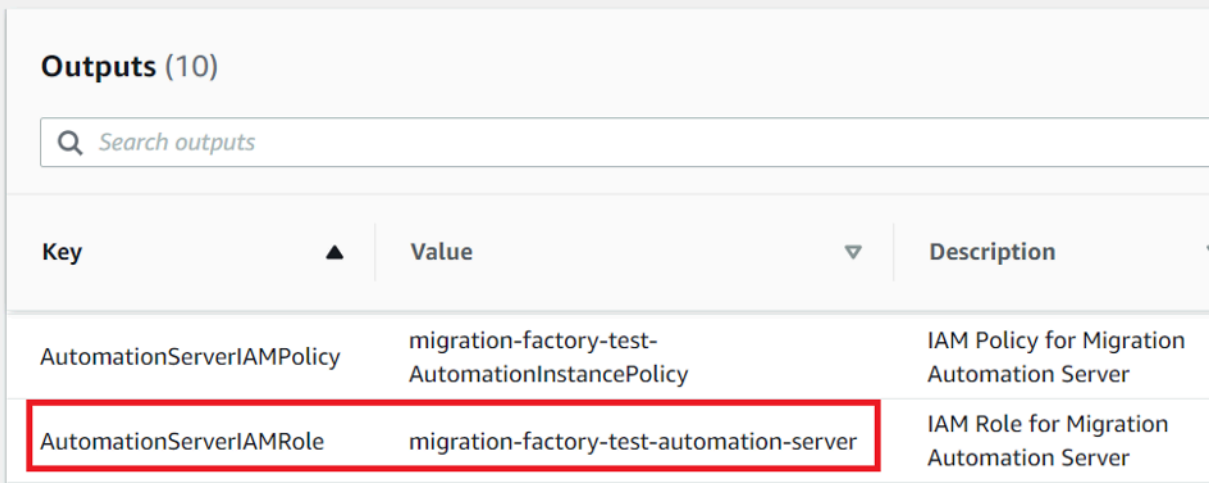
Configure AWS permissions for the migration automation server and install AWS Systems Manager Agent (SSM Agent)

Depending on where you deploy the migration execution server, choose one of the options below to configure AWS permissions for the migration automation server. The IAM role or policy provides the permission to the automation server and the access to AWS Secrets Manager to get agent installation keys and factory service account credentials. You can deploy the migration automation server either to AWS as an EC2 instance or on-premises.

Option 1: Use the following procedure to configure the permissions for the migration automation server in Amazon EC2 and in the same AWS account and Region as the factory.

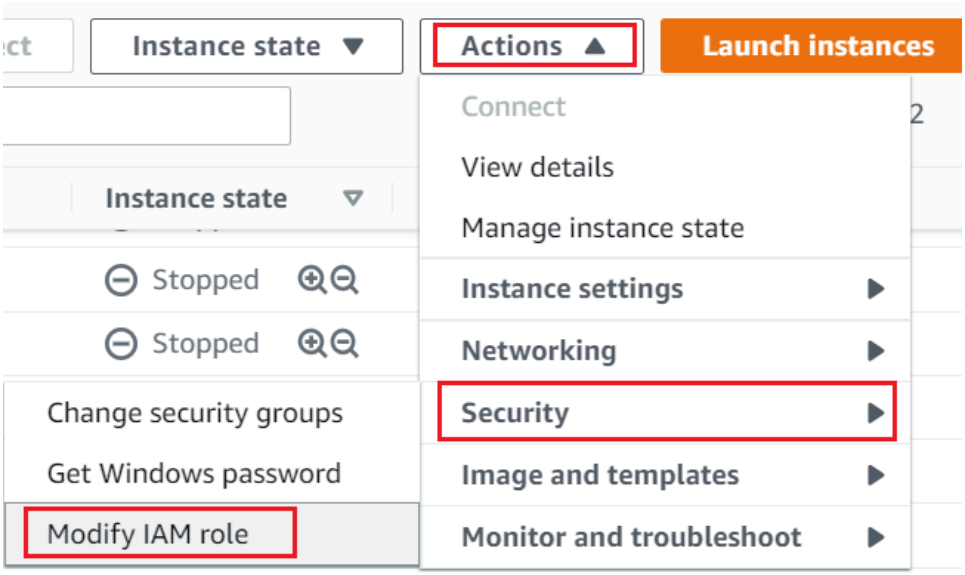
1. Navigate to the AWS CloudFormation console and select the solution's stack.
2. Select the **Outputs** tab, under the **Key** column, locate `AutomationServerIAMRole` and record the **Value** to use later in the deployment.

Outputs tab



3. Navigate to the Amazon Elastic Compute Cloud console.
4. From the left navigation pane, select **Instances**.
5. On the **Instances** page, use the Filter Instances field and enter the name of the migration execution server to find the instance.
6. Select the instance and select **Actions** on the menu.
7. Select **Security** from the drop-down list, and then select **Modify IAM role**.

Amazon EC2 console

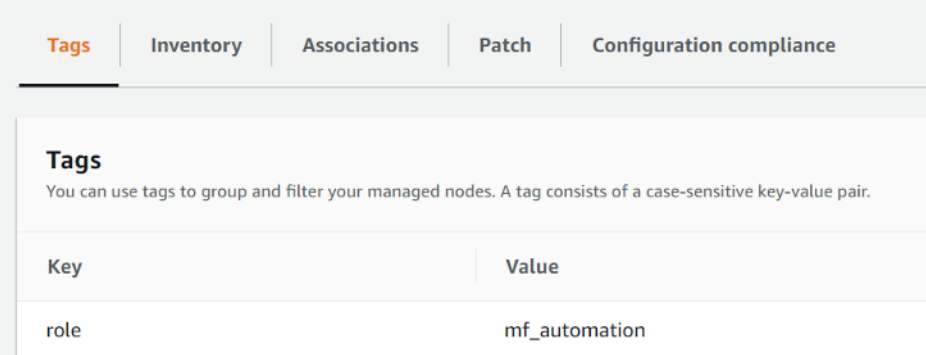


8. From the list of IAM roles, locate and select the IAM role containing the value for `AutomationServerIAMRole` that you recorded in Step 2, and choose **Save**.
9. Use your remote desktop protocol (RDP) to log in to the migration automation server.
10. Download and install SSM Agent on the migration automation server.

> **Note**
>
> By default, AWS Systems Manager agent is preinstalled on Windows server 2016 Amazon Machine Images. Perform this step only if the SSM Agent is not installed.

11. Add the following tag to the migration automation server EC2 instance: **Key**= `role` and **Value** = `mf_automation`.

Amazon EC2 console

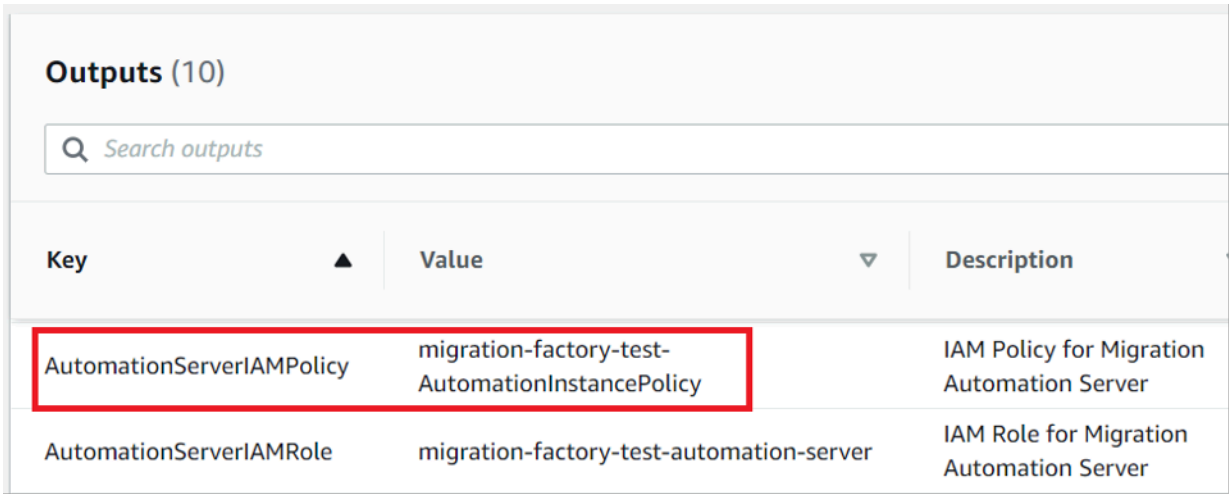


12. Open the AWS Systems Manager console and choose **Fleet Manager**. Check the automation server status, and make sure the SSM Agent ping status is **online**.

Option 2: Use the following procedure to configure the permissions for the migration automation server on-premises.

1. Navigate to the AWS CloudFormation console and select the solution's stack.
2. Select the **Outputs** tab, under the **Key** column, locate `AutomationServerIAMPolicy` and record the value to use later in the deployment.

Outputs tab



3. Navigate to the Identity and Access Management console.
4. From the left navigation pane, select **Users**, then choose **Add users**.
5. In the **User name** field, create a new user.
6. Choose **Next**.
7. On the **Set permissions** page, under **Permissions options**, select **Attach policies directly**. A list of policies displays.
8. From the list of policies, locate and select the policy containing the value for `AutomationServerIAMPolicy` that you recorded in Step 2.
9. Choose **Next**, then verify that the correct policy is selected.
10. Choose **Create user**.
11. After you're redirected to the **Users** page, choose the user you created in the previous step, and then choose the **Security credentials** tab.
12. In the **Access keys** section, choose **Create access key**.

> **Note**
>
> Access keys consist of an access key ID and secret access key, which are used to sign programmatic requests that you make to AWS. If you don't have access keys, you can create them from the AWS Management Console. As a best practice, do not use the root user access keys for any task where it's not required. Instead, create a new administrator IAM user with access keys for yourself.
>
> The only time that you can view or download the secret access key is when you create the keys. You cannot recover them later. However, you can create new access keys at any

time. You must also have permissions to perform the required IAM actions. For more information, see Permissions required to access IAM resources in the *IAM User Guide*.

13. To view the new access key pair, choose **Show**. You will not have access to the secret access key again after this dialog box closes. Your credentials will look something like this:
    - `Access key ID: AKIAIOSFODNN7EXAMPLE`
    - `Secret access key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
14. To download the key pair, choose **Download .csv file**. Store the keys in a secure location. You will not have access to the secret access key again after this dialog box closes.

> **Important**
>
> Keep the keys confidential to protect your AWS account and never email them. Do not share them outside your organization, even if an inquiry appears to come from AWS or Amazon.com. No one who legitimately represents Amazon will ever ask you for your secret key.

15. After you download the `0csv` file, choose **Close**. When you create an access key, the key pair is active by default, and you can use the pair right away.
16. Use your remote desktop protocol (RDP) to log in to the migration execution server.
17. Signed in as an administrator, open a command prompt (`CMD.exe`).
18. Run the following command to configure the AWS credentials on the server. Replace *<your_access_key_id>*, *<your_secret_access key>*, and *<your_region>* with your values:

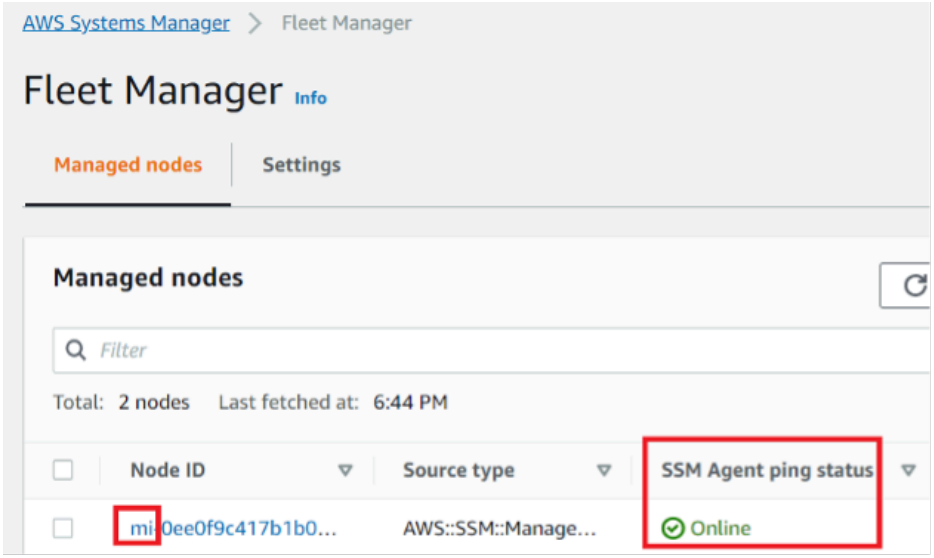
```
SETX /m AWS_ACCESS_KEY_ID <your_access_key_id>
SETX /m AWS_SECRET_ACCESS_KEY <your_secret_access key>
SETX /m AWS_DEFAULT_REGION <your_region>
```

19. Reboot automation server.
20. Install the AWS Systems Manager agent using Hybrid mode (on-prem servers).
    a. Create a hybrid activation; see Create an activation (console) in the *AWS Systems Manager User Guide*. During this process, when asked to provide an IAM Role, select an existing IAM role and choose the role with the suffix **-automation-server** which was automatically created when the Cloud Migration Factory stack was deployed.
    b. Log in to the migration automation server as administrator.

c. Install AWS Systems Manager Agent (SSM Agent); see Install SSM Agent for a hybrid and multicloud environment in the *AWS Systems Manager User Guide*. Use the hybrid activation created in step 20.a.

d. Once the agent is successfully installed, in the AWS Systems Manager console, choose **Fleet Manager**. Identify the node ID with **mi-** prefix with **Online** status.

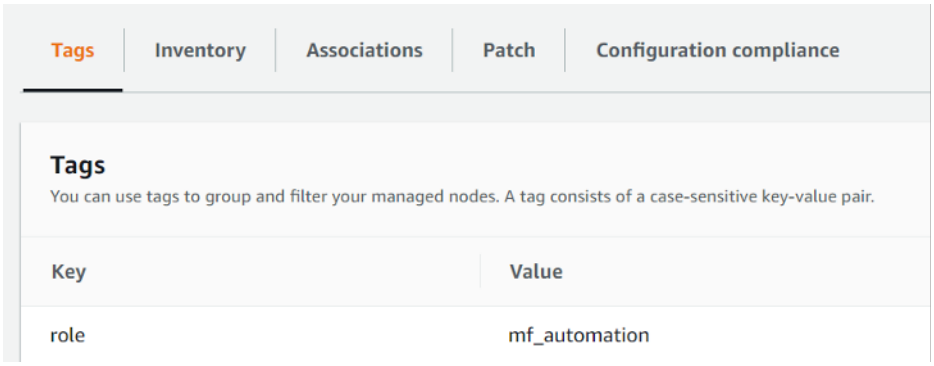
Fleet Manager



e. Select the **Node ID** and make sure the IAM role is the one you selected with **automation-server** suffix.

f. Add the following tag for this Hybrid node: **Key** = `role` and **Value** = `mf_automation`. All lower case.

Tag - hybrid node



Step 8: Test the solution using the automation scripts

Import migration metadata into the factory

To start the migration process, download the server-list.csv file from the GitHub repository. The `server-list.csv` file is an example AWS MGN Service migration intake form to import the attributes for the in-scope source servers.

> **Note**
>
> The .csv file and the sample automation scripts were part of the package from the same GitHub repository.

You can customize the form for your migration by replacing the sample data with your specific server and application data. The following table details the data to replace to customize this solution for your migration needs.

Field name	Required?	Description
wave_name	Yes	The wave name is based on priority and application server dependencies. Obtain this identifier from your migration plan.
app_name	Yes	The names of the applicati ons that are in-scope for migration. Confirm that your application grouping includes all the applications sharing the same servers.
aws_accountid	Yes	A 12-digit identifier for your AWS account located in your account profile. To access, select your account profile from the upper-right corner

Field name	Required?	Description
		of the AWS Management Console and select **My Account** from the drop-down menu.
aws_region	Yes	AWS Region code. For example, `us-east-1` . Refer to the full Region code list.
server_name	Yes	The name of the on-premises servers that are in-scope for migration.
server_os_family	Yes	The operating system (OS) that is running on the in-scope source servers. Use either **windows** or **linux** since this solution supports only these operating systems.
server_os_version	Yes	The version of the OS running on the in-scope source servers. **Note** Use the OS version, not the Kernel version, for example, use RHEL 7.1, Windows Server 2019, or CentOS 7.5, 7.6. Do not use Linux 3.xx, 4.xx, or Windows 8.1.x.

Field name	Required?	Description
server_fqdn	Yes	The source server's fully qualified domain name, which is the server name followed by the domain name. For example, server123.company.com.
server_tier	Yes	A label to identify whether the source server is a **web**, **app**, or a **database** server. We recommend designating the source server as **app** if the server functions as more than one tier, for example, if the server runs web, app, and database tiers together.
server_environment	Yes	A label to identify the server's environment. For example, **dev**, **test**, **prod**, **QA**, or **pre-prod**.
r_type	Yes	A label to identify the migration strategy. For example, **Retire, Retain, Relocate, Rehost, Repurchase, Replatform, Rearchitect, TBC.**
subnet_IDs	Yes	The subnet ID for the target Amazon EC2 instance for the migration post-cutover.

Field name	Required?	Description
securitygroup_IDs	Yes	The security group ID for the target Amazon EC2 instance for the migration post-cuto ver.
subnet_IDs_test	Yes	The target subnet ID for the source server that will be tested.
securitygroup_IDs_test	Yes	The target security group ID for the source server that will be tested.
instanceType	Yes	The Amazon EC2 instance type identified in the discovery and planning effort. For information about EC2 instance types, refer to Amazon EC2 Instance Types.
tenancy	Yes	The tenancy type, which is identified during the discovery and planning efforts. Use one of the following values to identify the tenancy: **Shared**, **Dedicated**, or **Dedicated Host**. You can use **Shared** as the default value unless an application's license requires a specified type.
Tags	No	The tags for the server resources, such as `CostCente r=123;BU=IT;Locati on=US` .

Field name	Required?	Description
private_ip	No	The private IP for the target instance. If not included, instance will get an IP from DHCP.
iamRole	No	IAM role for the target instance. If not included, no IAM role will be attached to the target instance.

1. Log in to the Cloud Migration Factory web console.
2. Under **Migration Management**, select **Import** and choose **Select file**. Select the intake form you completed previously and choose **Next**.
3. Review the changes and make sure you do not see any errors (information message is normal), and choose **Next.**
4. Choose **Upload** to upload servers.

Access the domains

The sample automation scripts included with this solution connect to the in-scope source servers to automate migration tasks, such as the installation of the replication agent, and shutting down the source servers. In order to conduct a test run of the solution, a domain user with local admin permissions to the source servers is required, for Windows and Linux (sudo permissions) servers. If Linux is not in the domain, other users such as LDAP user with sudo permissions or a local sudo user may be used. For more information about automated migration tasks, refer to Automated migration activities using Migration Factory web console and Automated migration activities using command prompt.

Conduct a test run of the migration automation

This solution lets you conduct a test run of the migration automation. Using automation scripts, the migration process imports the data from the migration CSV file into the solution. Prerequisite checks are conducted for the source servers, the replication agent is pushed to the source servers, replication status is verified, and the target server is launched from the Migration Factory web

interface. For step-by-step instructions on running a test, refer to Automated migration activities using Migration Factory web console and Automated migration activities using command prompt.

Step 9: (Optional) Build a migration tracker dashboard

If you deployed the optional migration tracker component, you can set up an Amazon QuickSight dashboard that will visualize the migration metadata stored in the Amazon DynamoDB table.

Use the following procedures to:

1. Set the QuickSight permissions and connections
2. Create a dashboard

> **Note**
>
> If the Migration Factory is empty and there is no wave, application, and server data, then there will not be any data to build a QuickSight dashboard.

Set the QuickSight permission and connections

If you have not set up Amazon QuickSight in your AWS account, refer to Setting Up for Amazon QuickSight in the *Amazon QuickSight User Guide*. After you have set up a QuickSight subscription, use the following procedure to set the permissions and connections between QuickSight and this solution.

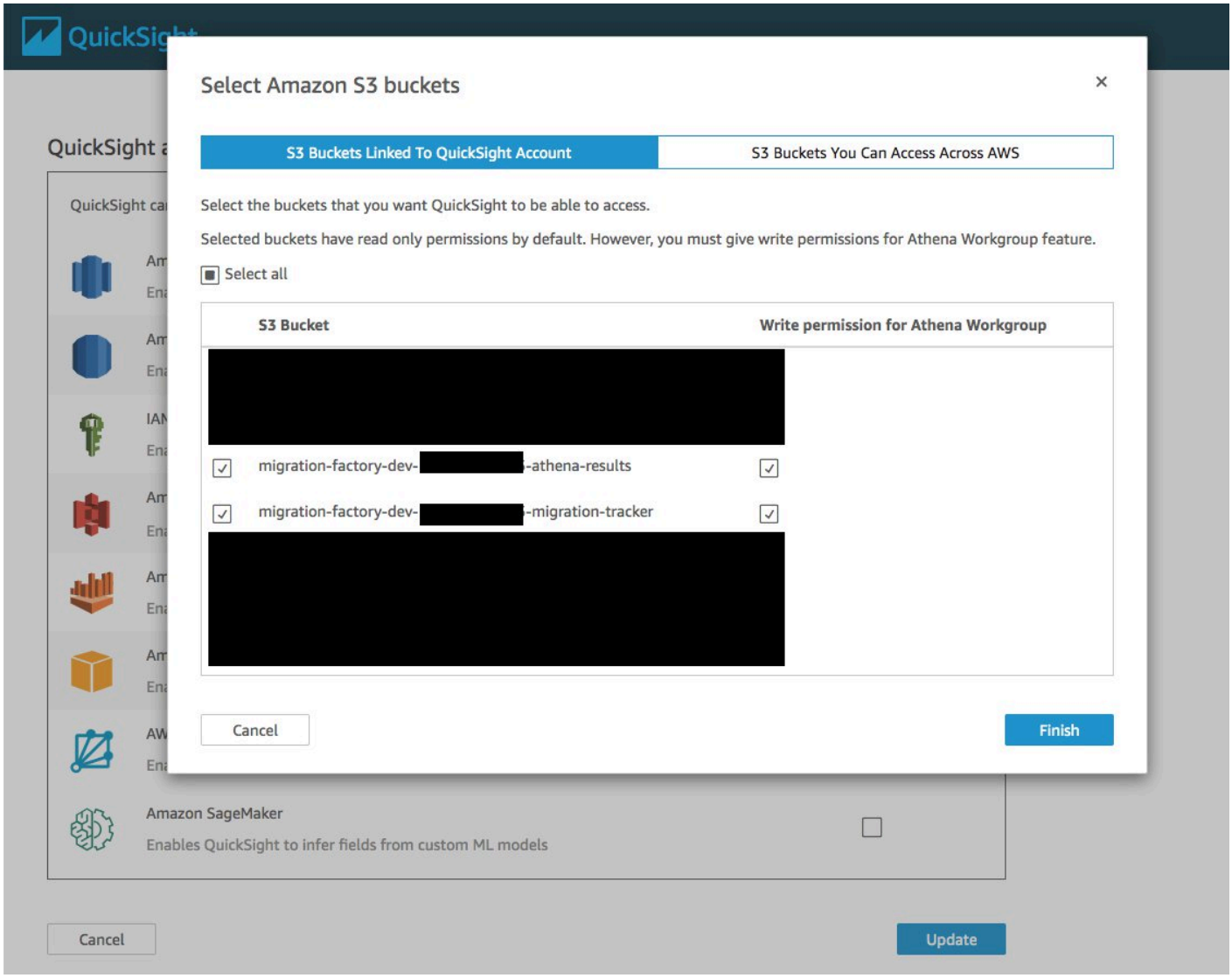
> **Note**
>
> This solution uses Amazon QuickSight enterprise license. However, if you don't want the email reporting, insights, and the hourly data refresh, you can opt for a standard license, which can also be used with migration tracker.

First, connect QuickSight with the Amazon S3 bucket:

1. Navigate to the QuickSight console.
2. On the **QuickSight** page, choose the icon displaying a person in the upper-right corner and **Manage QuickSight**.

3. On the **Account name** page, from the left menu pane, select **Security & permissions**.
4. On the **Security & permissions** page, under the **QuickSight access to*AWS services section, select *Manage**.
5. From the **QuickSight access to AWS services** page, select the checkbox for **Amazon S3**.
6. On the **Select Amazon S3 buckets** dialog box, verify that you are in the **S3 Buckets Linked to QuickSight Account** tab and tick both the right and left checkboxes for the **athena-results** and *migration-tracker * S3 buckets.

QuickSight S3 bucket selection dialog with options for Athena Workgroup write permissions.



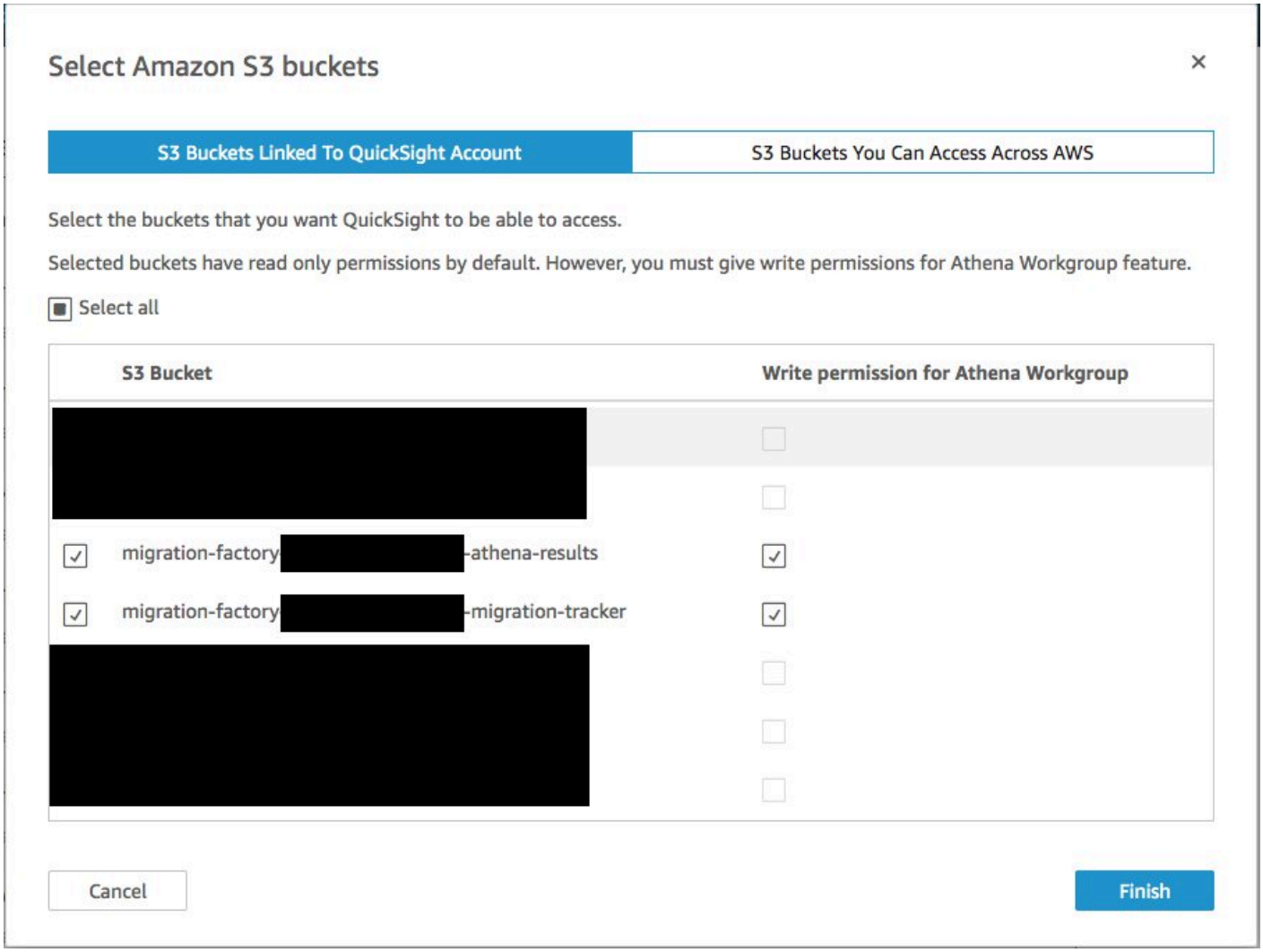
> **Note**
>
> If you are already using QuickSight for other S3 data analysis, clear and reselect the Amazon S3 option to display the bucket selection dialog box.

7. Choose **Finish**.

Next, set up permissions for Amazon Athena:

1. From the **QuickSight access to AWS services** page, tick the checkbox for **Amazon Athena**.
2. On the **Amazon Athena permissions** dialog box, choose **Next**.
3. On the **Amazon Athena resources** dialog box, verify that you are in the **S3 Buckets Linked to QuickSight Account** tab and verify that the same S3 buckets are checked - **athena-results** and **migration-tracker**.

   QuickSight Amazon Athena resources dialog box



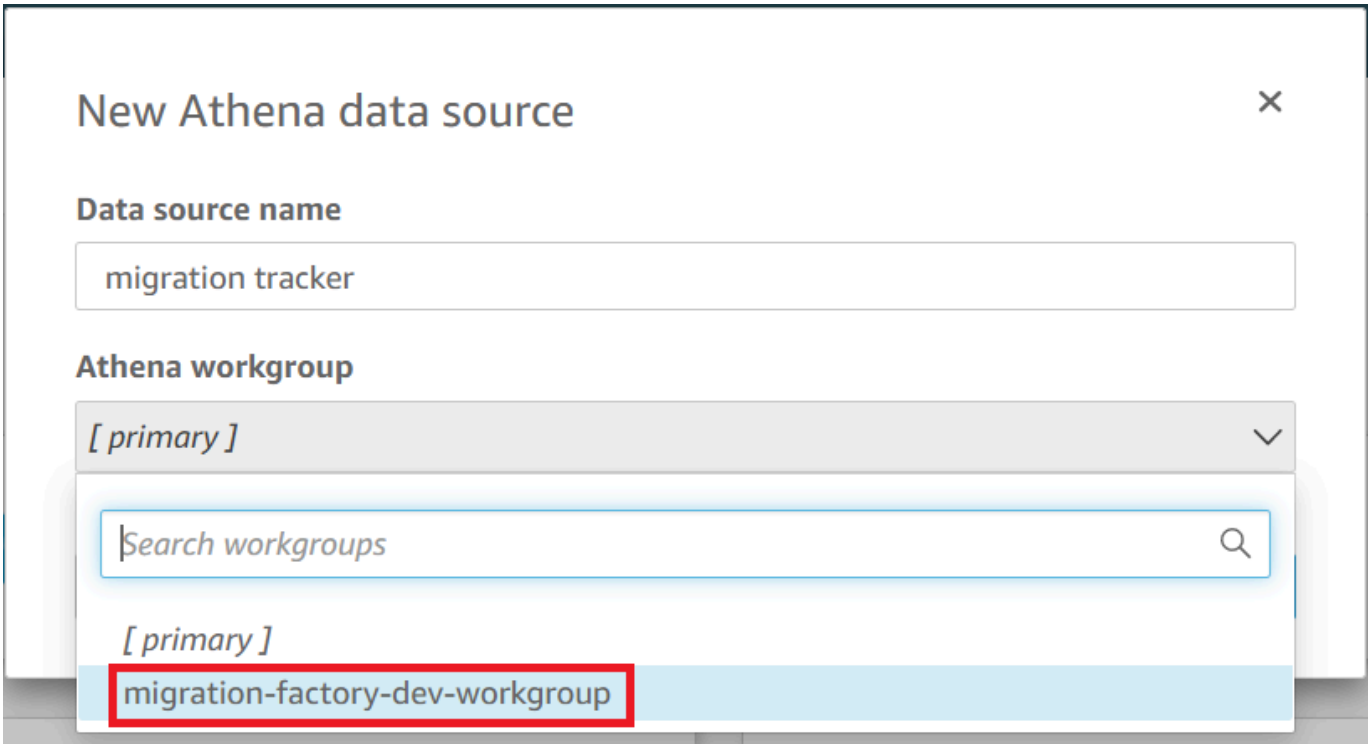
4. Choose **Finish**.
5. From the *QuickSight access to***AWS services** page, choose **Save**.

Next, set up a new analysis:

1. Select the QuickSight logo to return to the QuickSight homepage.
2. On the **Analysis** page, choose **New Analysis**.
3. Choose **New dataset**.
4. On the **Create a Data Set** page, choose **Athena**.
5. In the **New Athena data source** dialog box, take the following actions:
   a. In the **Data source name** field, enter a name for the data source
   b. In the **Athena workgroup** field, select the appropriate *<migration-factory>*-workgroup.

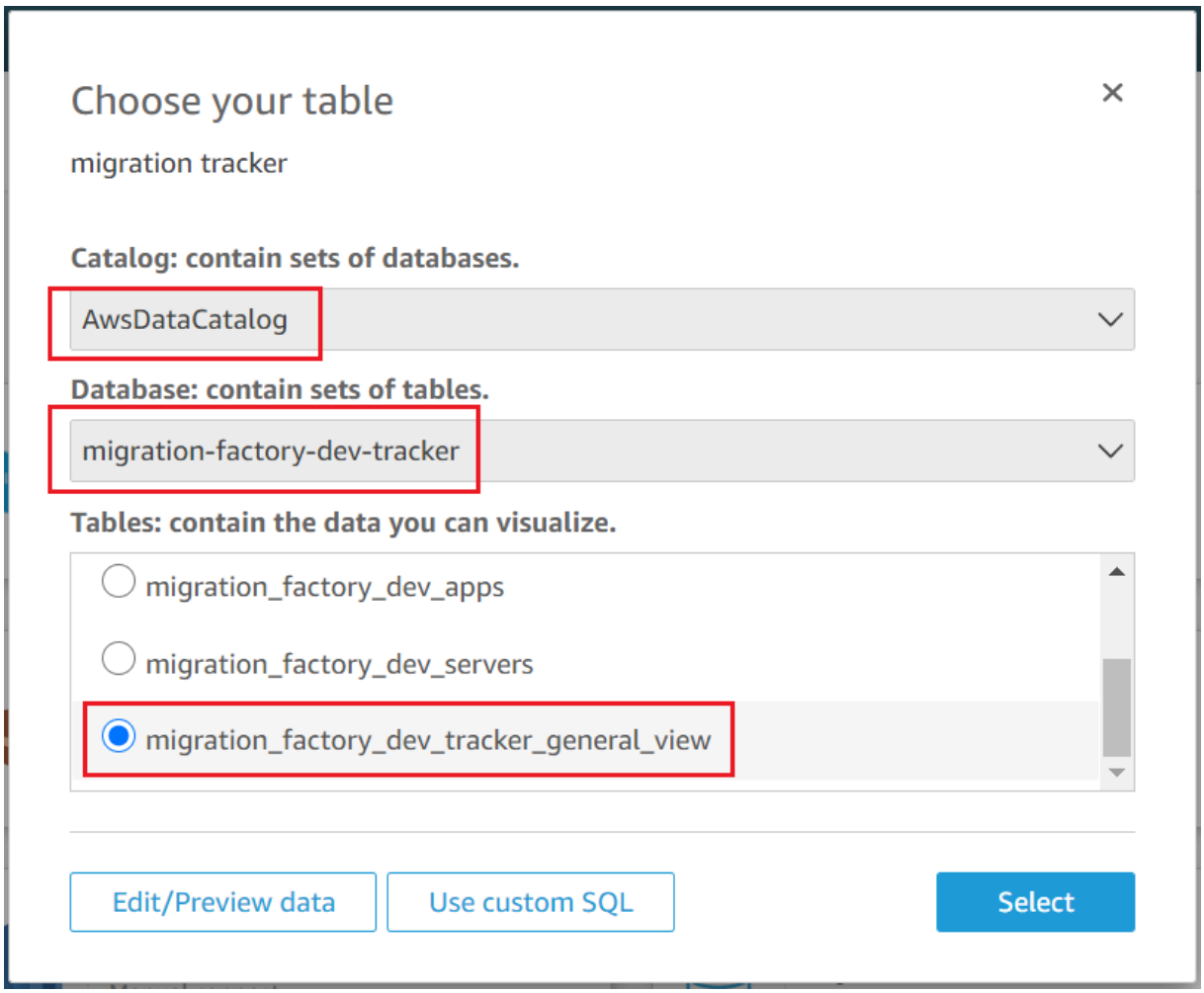
> **Note**
>
> If you have deployed this solution multiple times, there will be more than one workgroup. Select the one that was created for your current deployment.

New Athena data source dialog box



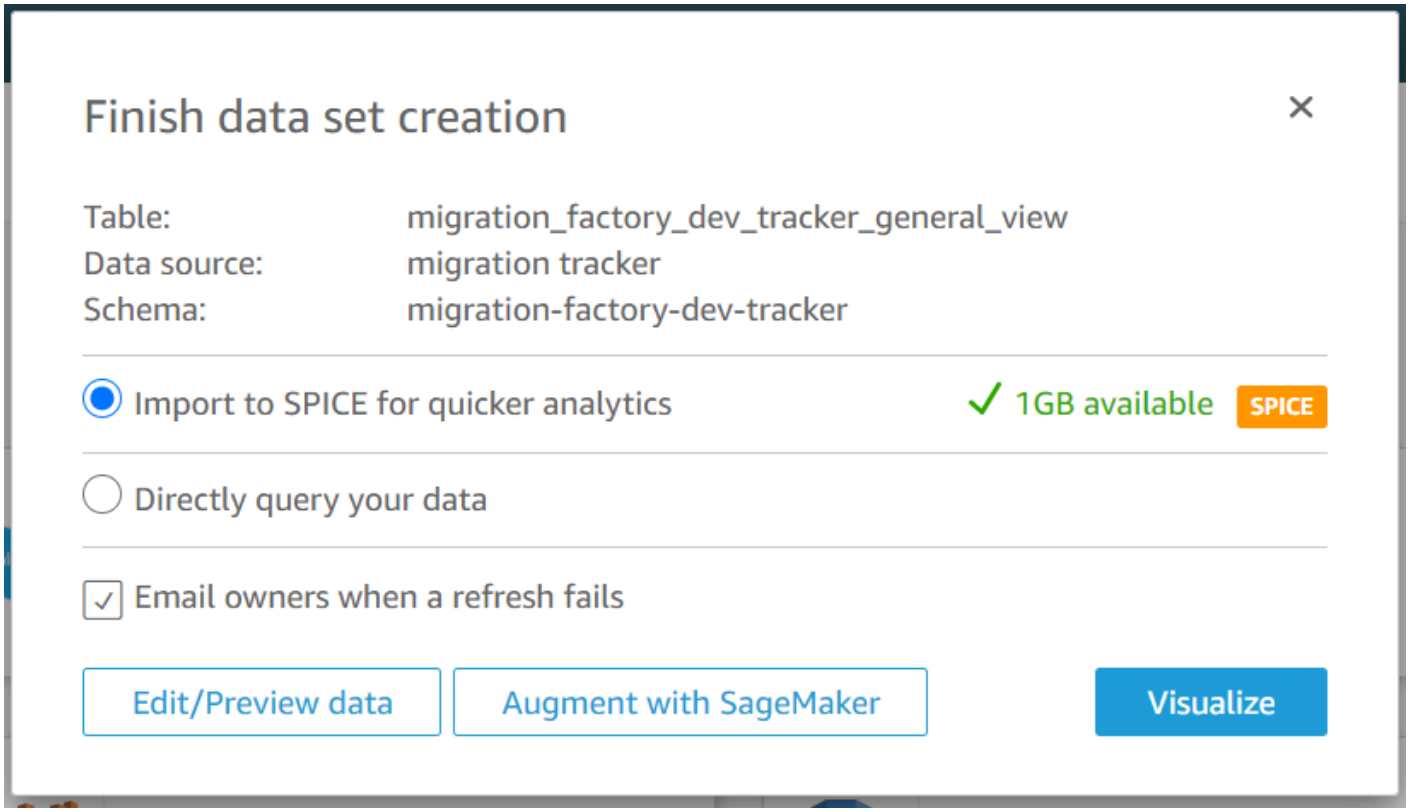
6. Choose **Validate connection** to ensure that QuickSight can communicate with Athena.
7. After the connection is validated, choose **Create data source**.
8. In the next dialog box, **Choose your table**, take the following actions:
   a. From the **Catalog** list, choose **AwsDataCatalog**.
   b. From the **Database** list, choose *<Athena-table>*-tracker.
   c. From the **Tables** list, choose *<tracker-name>*-general-view.
   d. Choose **Select**.

Choose your table dialog box



9. In the next dialog box, **Finish data set creation**, choose **Visualize**.

Finish data set creation dialog box

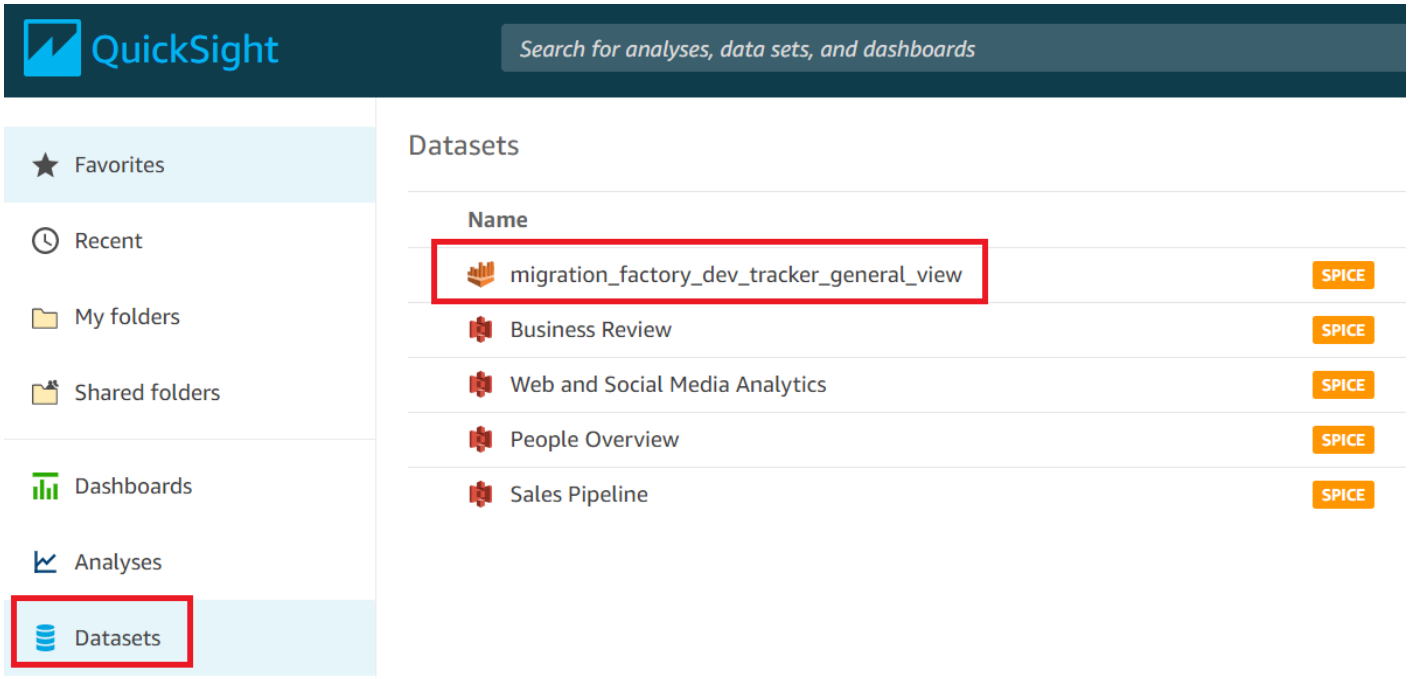


10In **New sheet**, choose **Interactive sheet**, then choose **Create**.

After the data is imported, you will be redirected to the Analysis page. However, before creating your visuals, set up a schedule to refresh your dataset.

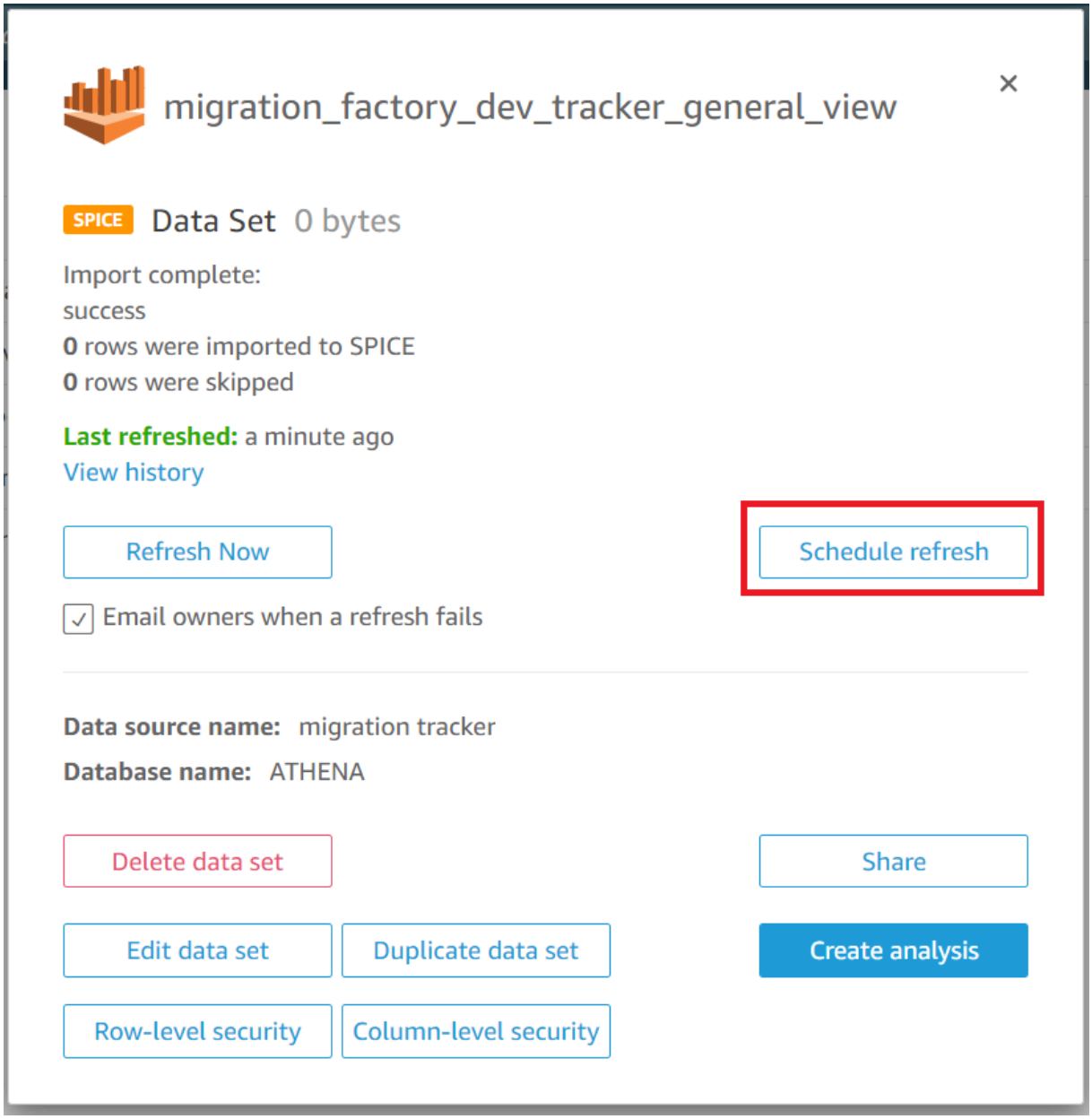
1. Navigate to the QuickSight homepage.
2. In the navigation pane, choose **Datasets**.
3. On the **Datasets** page, select the *<migration-factory>*-general-view dataset.

QuickSight Datasets page



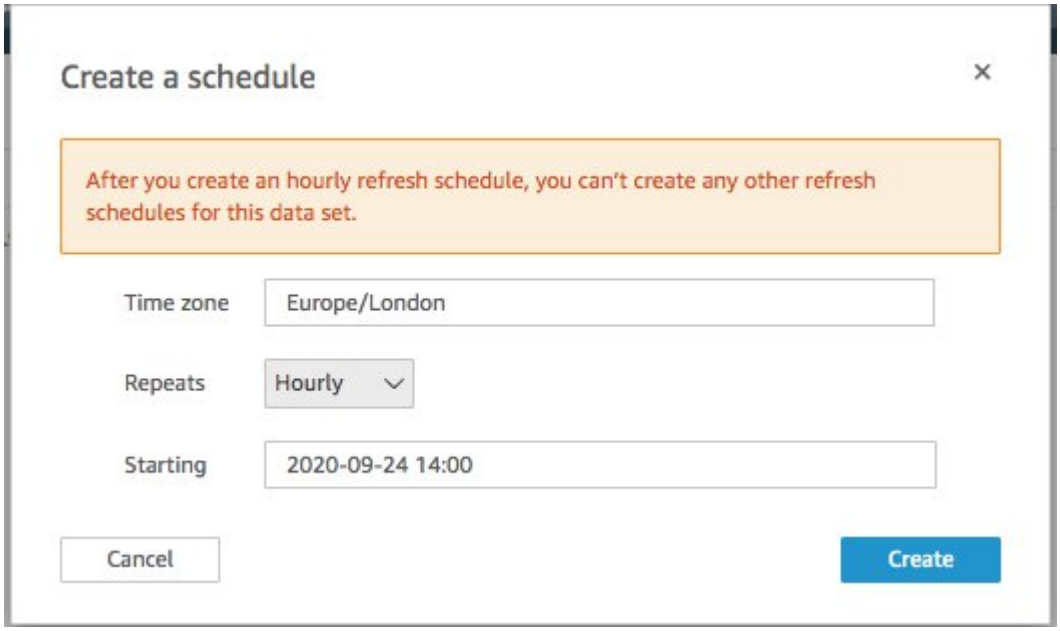
4. On the *<migration-factory>*-general-view **Datasets** page, choose the **Refresh** tab.

Migration tracker general view dialog box



5. Choose **Add new schedule**.
6. On the **Create a refresh schedule** page, select **Full refresh**, select the appropriate **Time zone**, enter a **Start time**, and select the Frequency.
7. Choose **Save**.

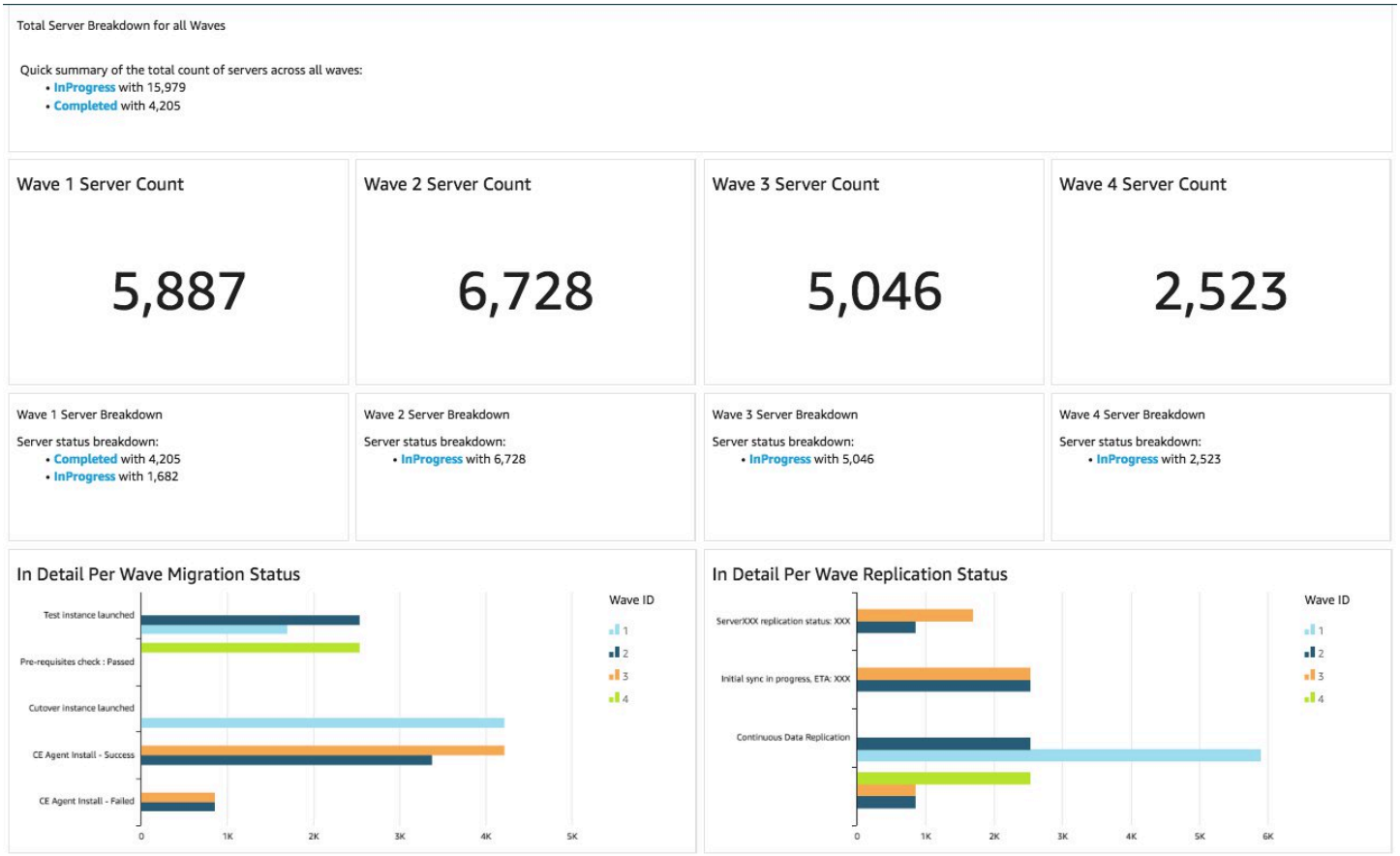
Create a schedule dialog box



Create a dashboard

Amazon QuickSight offers the flexibility of building a custom dashboard that helps you to visualize your migration metadata. The following tutorial creates a dashboard containing a count visual that shows the server count by waves and bar charts showing the migration status. You can customize this dashboard to meet your business needs.

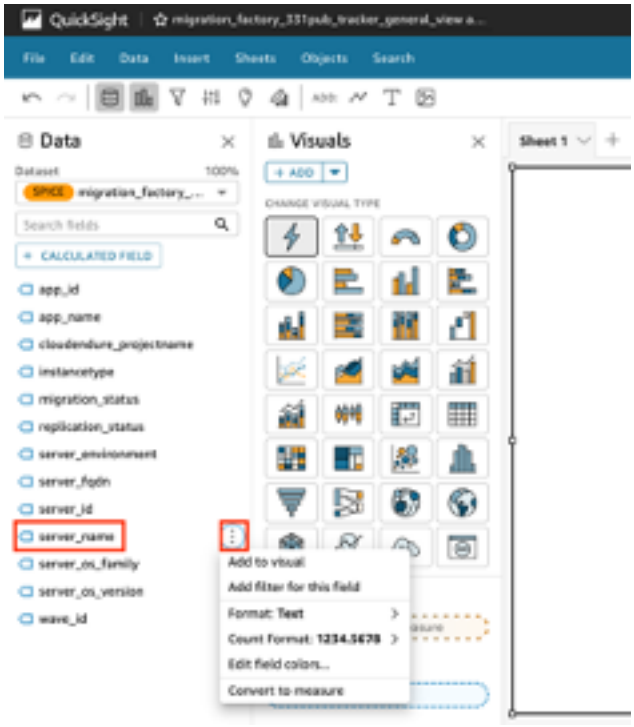
Example QuickSight dashboard



Use the following steps to create a count overview by migration waves. This view counts all the servers in the dataset that are grouped per wave, providing a granular view of the total number of servers in a wave. To create this view, you will convert the **server_name** into a measure, which allows you to count distinct servers names. Then you will create a wave-by-wave filter.

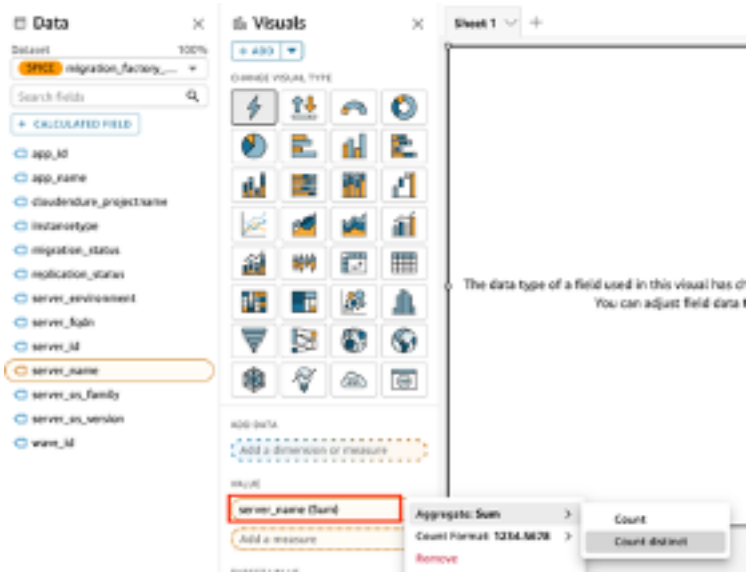
1. Navigate to the QuickSight homepage.
2. In the navigation pane, choose **Analyses**.
3. Select *<migration-factory>*-general-view.
4. On the **Visualize** page, hover over the **server_name** and choose the ellipsis to the right.

QuickSight Visualize a data set page



5. Select **Convert to measure** to convert the dataset from a dimension to a measure. The **server_name** text turns green to indicate that the dataset has been converted to a measure.
6. Select **server_name** to visualize the image. The visual will contain an error message indicating that the field data types must be updated.
7. On the **Visuals** pane, select the **server_name (Sum)**, under **Value**, select **Aggregate: Sum**, then select **Count distinct**.

Field wells page



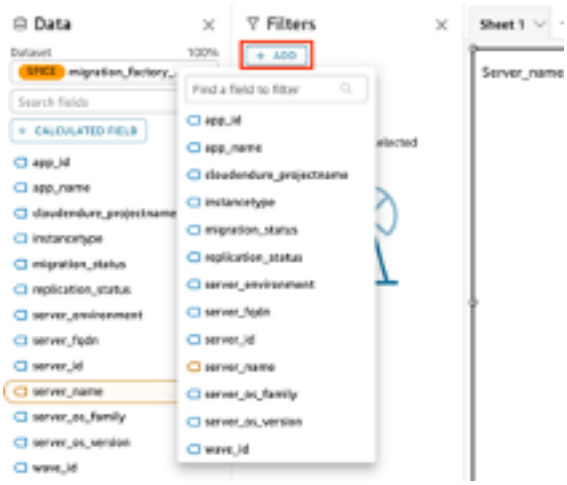
A count of the number of unique server names you have in your dataset is displayed. You can resize the visualization as needed to ensure it displays the information clearly on your monitor.

> **Note**
>
> You may need to convert your dataset back to dimension when you create another visual.

Next, add filters to the visualization to identify the server count for each migration wave. The following steps will apply a **wave_id** filter to your visualization.

1. Verify that the visualization is selected. In the top navigation pane, select **Filter**.
2. From the left Filters pane, choose **ADD** and select **wave_id** from the list.

Filters pane drop-down list



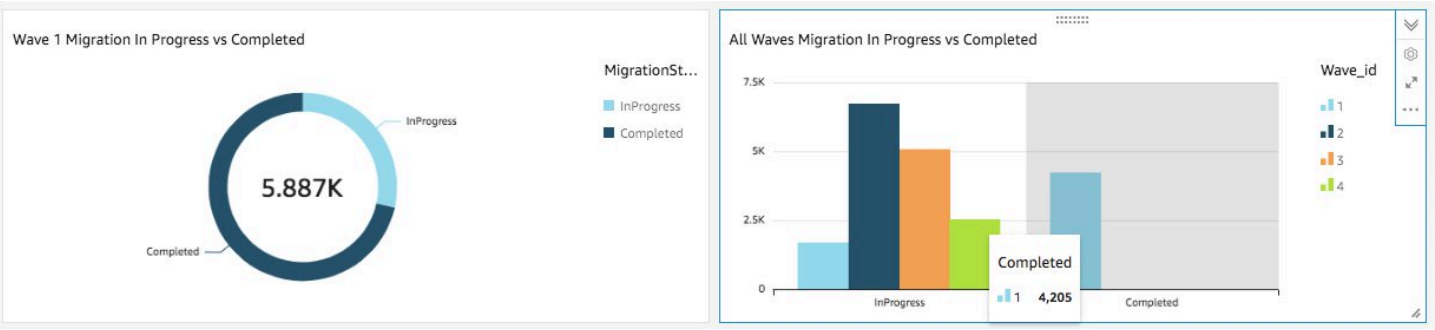
3. Choose **wave_id** from the filters list.
4. In the **Filter** pane, under **Search values** select the checkbox next to the value **1**.
5. Choose **Apply**.
6. In the visualization, change the title to **Wave 1 Server Count** by double clicking on the current title.

Repeat these steps for the other waves that are visualized in your dashboard.

The next visualization we will add in the dashboard is a doughnut graph showing servers that are in progress of being migrated versus ones that have completed the migration. This chart uses Super-fast, Parallel, In-memory Calculation Engine (SPICE) Queries by creating a new column in the

dataset that determines that an incomplete status will be identified as *in progress*. All values in the dataset that are not completed are combined and categorized as *in progress*.

Doughnut graph and bar chart visualizing migration progress

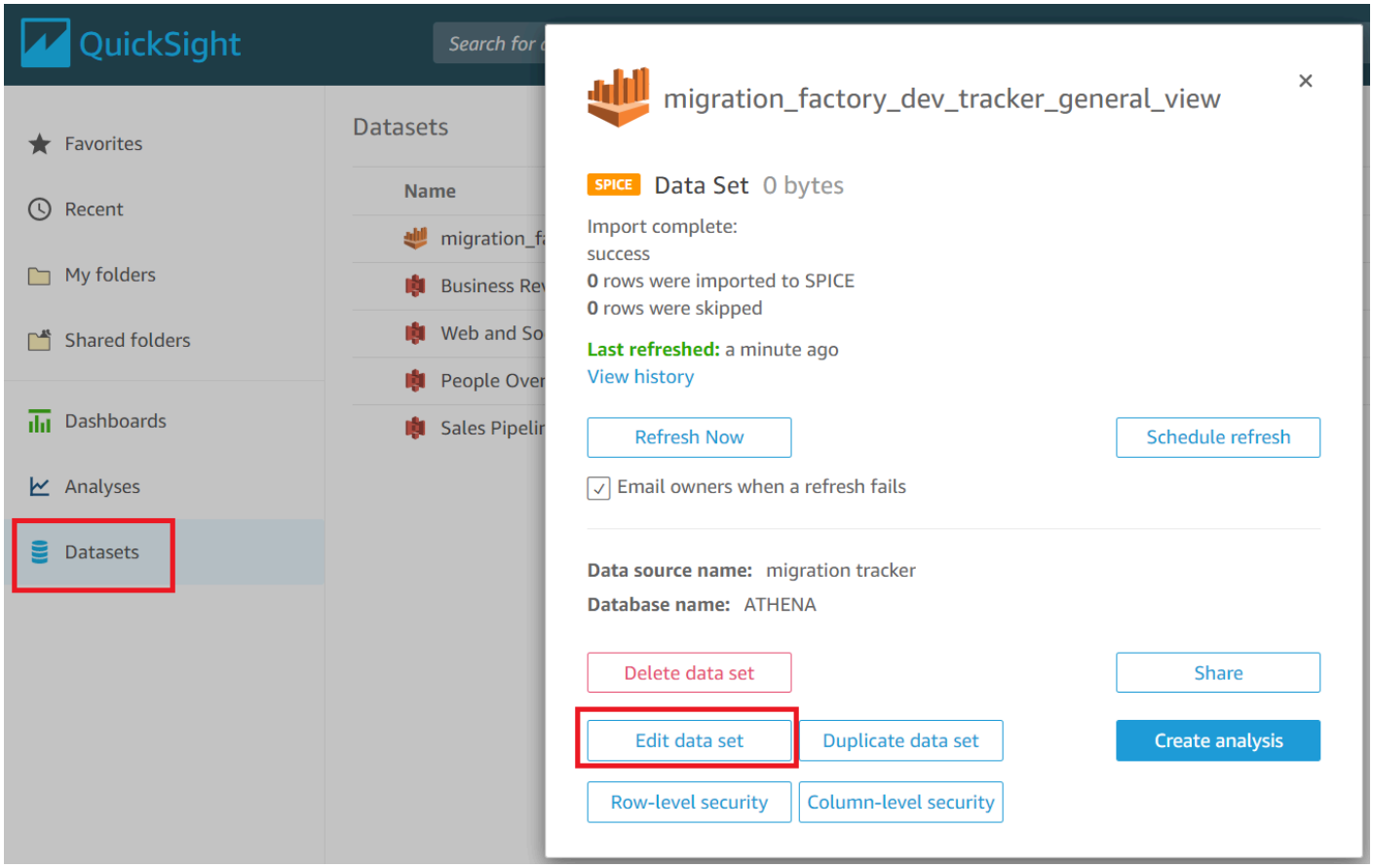


> **Note**
>
> By default, when there is no custom query applied to the dataset, up to five migration/replication statuses can be shown. For this solution, a **MigrationStatusSummary** query is created in a new column: `ifelse(migration_status ='Cutover instance launched', 'Completed', 'InProgress')`
> This query combines the values of the statuses to create one column that is used for the visualization. For information about creating a query, refer to Using the Query Editor in the *Amazon QuickSight User Guide*.

Use the following steps to create the **MigrationStatusSummary** column:

1. Navigate to the QuickSight homepage.
2. In the navigation pane, select **Datasets**.
3. On the **Datasets** page, select the *<migration-factory>*-general-view dataset.
4. On the dataset page, choose **Edit dataset**.

Migration factory dataset dialog box



5. In the **Fields** pane, choose **\+**, then choose **Add calculated field**.
6. On the **Add calculated field** page, enter a name for your SQL query, for example, **MigrationStatusSummary**.
7. Enter the following SQL query into the SQL editor:

```
ifelse(migration_status ='Cutover instance launched', 'Completed', 'InProgress')
```

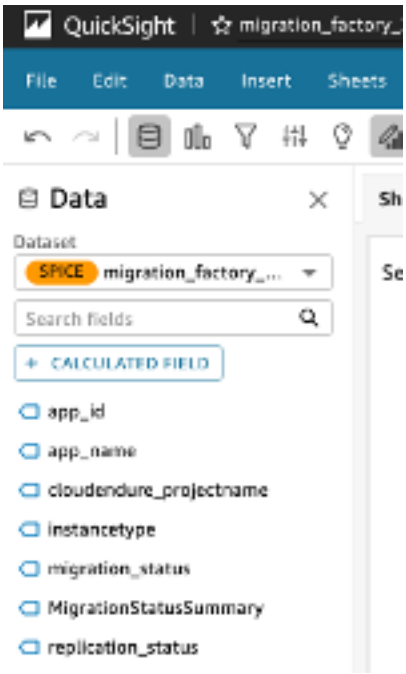
8. Choose **Save**.

Add calculated field dialog box

9. On the **Dataset** page, choose **Save & publish**.

Your newly added query will be listed in the **Data set Fields list**.

Dataset Fields list

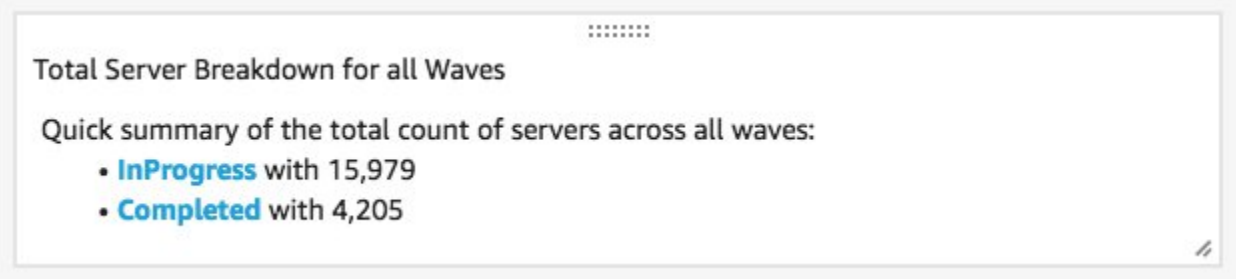


Next, build the dashboard.

1. Navigate to the QuickSight homepage.
2. Choose **Analyses**, and then choose the migration_factory analyses created earlier.
3. Ensure that no charts are selected in **Sheet 1.**
4. From the Data set pane, hover over the **MigrationStatusSummary** and choose the ellipsis to the right.
5. Choose **Add to visual**.
6. Then, choose **wave_id**.
7. In the **Visuals** pane, select and move the **MigrationStatusSummary** to the x-axis dimension and select **wave_name** as the* GROUP/COLOR. *

If you have an enterprise license for Amazon QuickSight, insights will be generated after the custom columns are created. You can customize your narratives for each insight. For example:

Example dashboard insights



You can also customize the data by breaking down the metadata into waves. For example:

Example wave 1 server breakdown

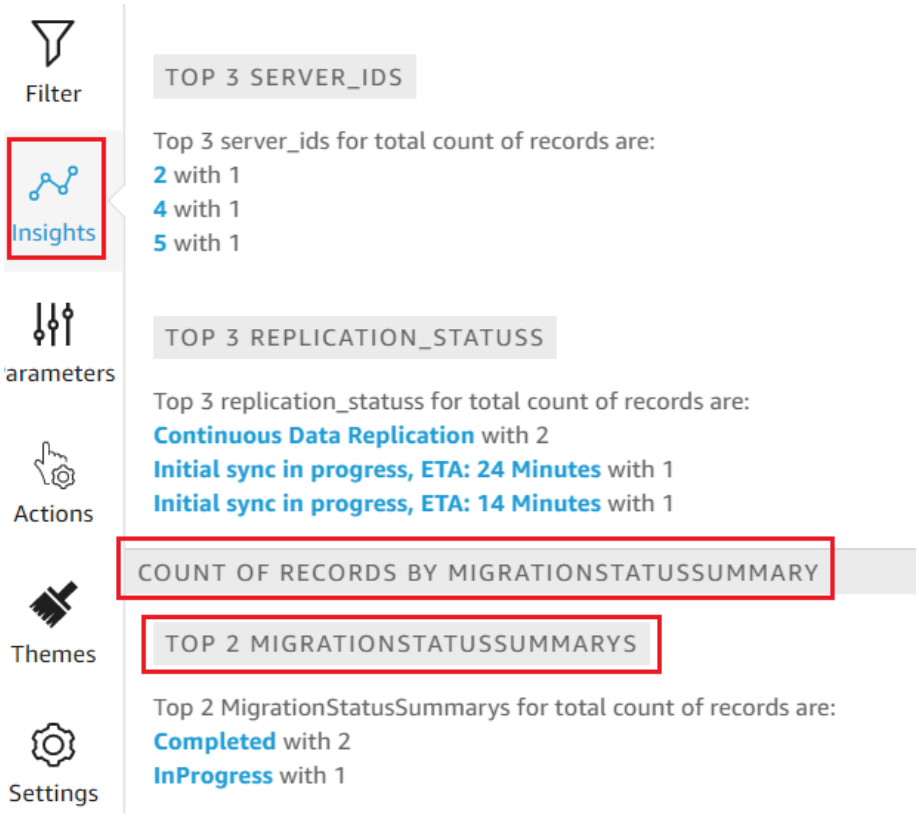
(Optional) View Insights on the Amazon QuickSight dashboard

> **Note**
>
> You can use the following procedure if you have an enterprise license for Amazon QuickSight.

Use the following steps to add an insight to your dashboard which shows a breakdown of completed and in progress migrations.

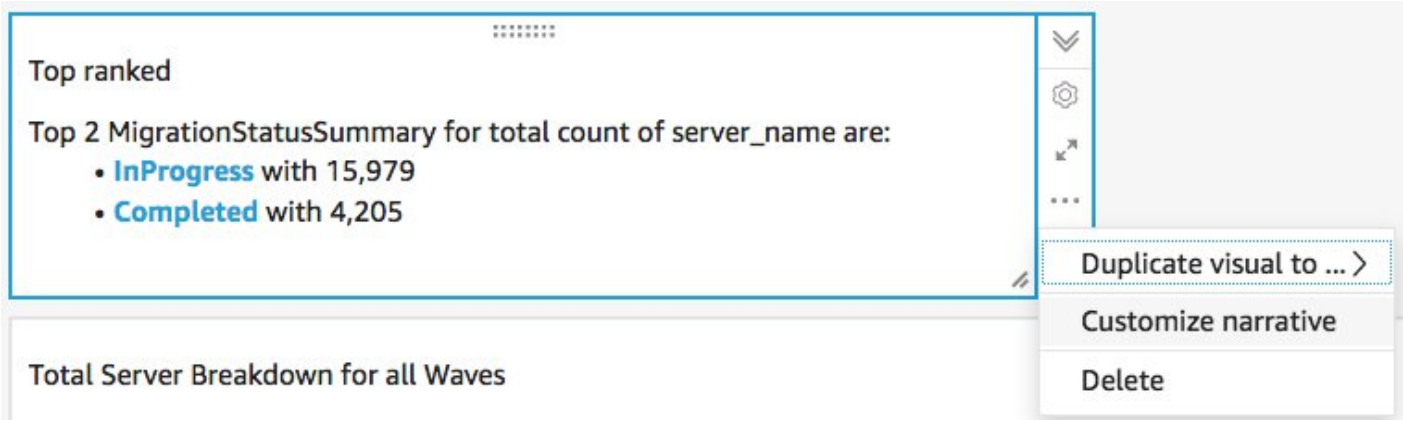
1. In the top navigation pane, choose **Insights**.
2. On the **Insights** page, in the **Count of Records BY MIGRATIONSTATUSSUMMARY** section, hover over **Top 2 MigrationSummarys** item and choose the **\+** to add an insight to the visual.

   Add an insight to a visual

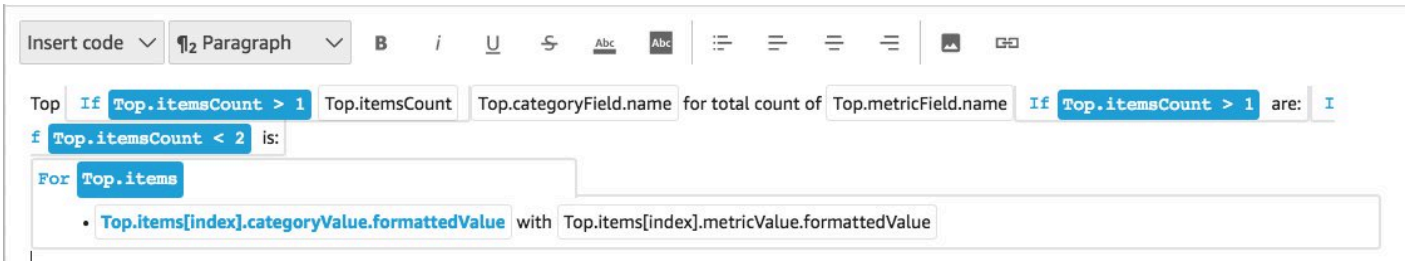


3. Customize the insight for your analysis by choosing **Customize Narrative** on the visual.

Add an Insight to your dashboard

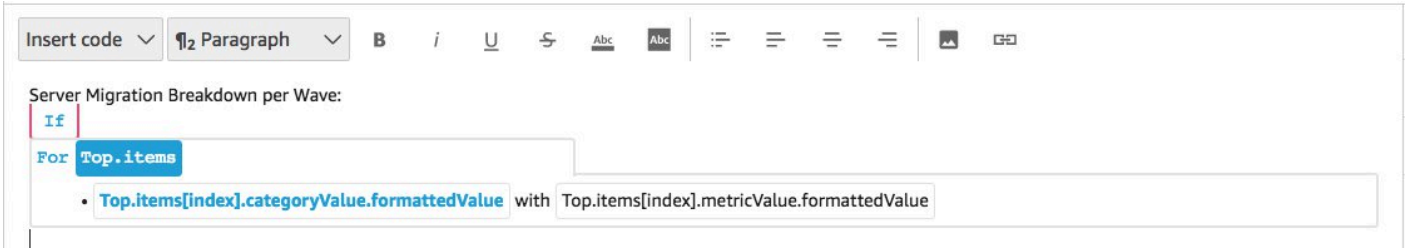


Customize narrative option



4. Edit the narrative to fit your use case and choose **Save**. For example:

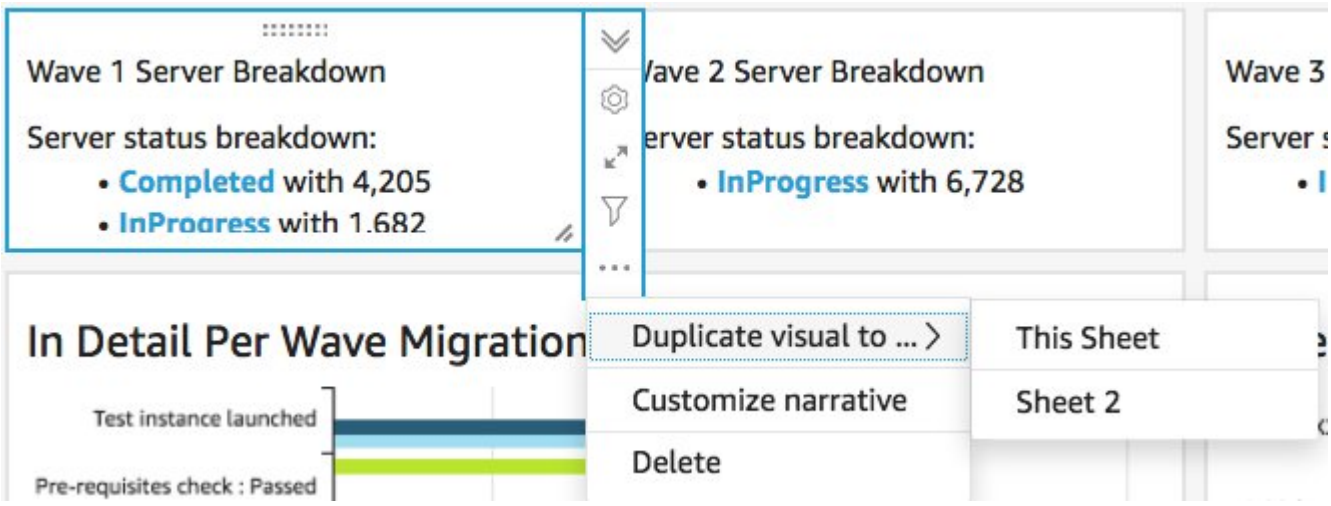
Edit your narrative



Return to the dashboard and filter it to show each wave:

5. On the left menu pane, choose **Filter**.
6. Choose the **+** button and select **wave_id**.
7. Select a wave to visualize and choose **Apply**.
8. To visualize all the migration waves, duplicate the visuals by choosing the ellipsis to the left side of the visual and selecting **Duplicate visual**.

Visualize the migration waves



9. Modify the filter for each visual to show a breakdown for each migration wave.

This insight is customized summarize the total count of servers across all waves. For more information and guide on how to customize insights, refer to Working with Insights in the *QuickSight User Guide*. You can access this QuickSight dashboard from any device and seamlessly embed it into your applications, portals, and websites. For more information about QuickSight dashboards, refer to Working with Dashboards in the *Amazon QuickSight User Guide*.

Step 10: (Optional) Configure additional identity providers in Amazon Cognito

If you selected `true` for the optional **Allow additional identity provider to be configured in Cognito** parameter when launching the stack, you can set up additional IdPs in Amazon Cognito to allow sign in using existing SAML IdP. The process for setting up the external IdP varies between providers. This section describes the Amazon Cognito configuration and generic steps to configure the external IdP.

Perform the following steps to collect information from Amazon Cognito to provide to the external IdP:

1. Navigate to the AWS CloudFormation console and select the **Cloud Migration Factory on AWS** stack.
2. Select the **Outputs** tab.
3. In the **Key** column, locate **UserPoolId** and record the **Value** to use later during setup.
4. Navigate to the Amazon Cognito console.
5. Choose the User pool that matches the User pool ID from the solution stack output.
6. Choose the **App Integration** tab and record the **Cognito domain** to use later during setup.

Perform the following steps within your existing IdP's management interface:

> **Note**
>
> These instructions are generic and will differ between providers. Consult your IdP's documentation for full details on setting up SAML applications.

1. Navigate to your IdP's management interface.
2. Choose the option to add applications or setup SAML authentication for an application, and create or add a new application.
3. Within the setup of this SAML application, you will be asked for the following values:
   a. **Identifier (Entity ID)** or something similar. Provide the following value:

```
urn:amazon:cognito:sp:<UserPoolId recorded earlier>
```

b. **Reply URL (Assertion Consumer Service URL)** or something similar. Provide the following value:

```
https://<Amazon Cognito domain recorded earlier>/saml2/idpresponse
```

c. **Attributes and Claims** or something similar. At a minimum, ensure that a unique identifier or subject is configured along with an attribute that provides the email address of the user.

4. There will either be a **Metadata URL** or the ability to download a **Metadata XML** file. Download a copy of the file or record the URL provided to use later during setup.
5. Within the setup, configure the access list of users from the IdP that are allowed to sign in to the CMF application. All users that are granted access to the application in the IdP will automatically be granted read only access to the CMF console.

Perform the following steps to add the new IdP to the Amazon Cognito user pool created during the stack deployment:

1. Navigate to the Amazon Cognito console.
2. Choose the User pool that matches the User pool ID from the solution stack output.
3. Choose the **Sign-in experience** tab.
4. Choose **Add identity provider** then choose **SAML** as the third-party provider.
5. Provide a name for the provider; this will be displayed to the user on the CMF sign-in screen.
6. In the **Metadata document source** section, either provide the **Metadata URL** captured from the IDP SAML setup or upload the **Metadata XML** file.
7. In the **Map attributes** section, choose **Add another attribute**.
8. Choose **email** for the **User pool attribute** value. For the **SAML attribute**, enter the name of the attribute that your external IdP will provide the email address to.
9. Choose **Add identity provider** to save this configuration.
10. Choose the **App integration** tab.
11. From within the **App client list** section, choose the migration factory application client (there should only be one listed) by clicking the name.
12. From the **Hosted UI** section, choose **Edit**.
13. Update the **Identity providers** selected by selecting the new IdP name you added in step 5 and deselecting **Cognito User Pool**.

> **Note**
>
> Cognito User Pool is not required because this is built into the CMF sign-in screen, and if selected, it will show twice.

14. Choose **Save changes**.

The configuration is now complete. On the CMF sign-in page, you will see the button **Sign in with your corporate ID**. Choosing this option will display the provider you have configured previously. Users who choose this option will be directed to sign in and then return to the CMF console once successfully signed in.

Monitor the solution with Service Catalog AppRegistry

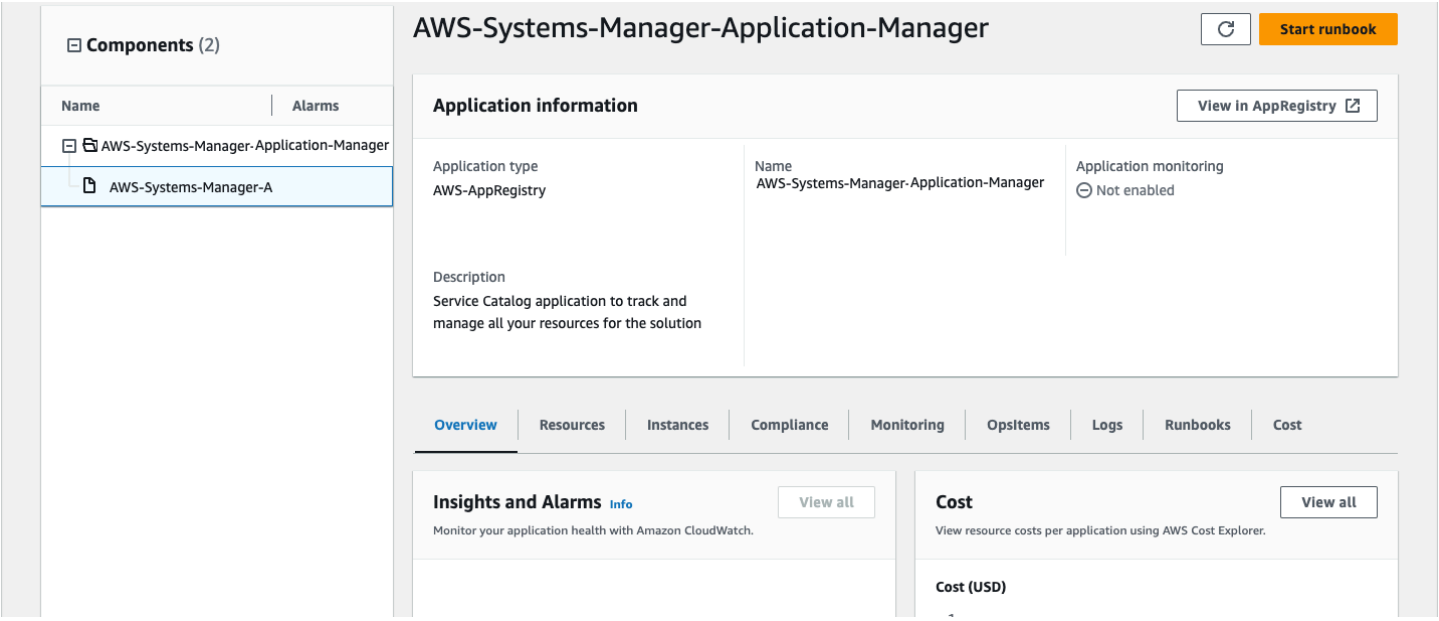
This solution includes a Service Catalog AppRegistry resource to register the CloudFormation template and underlying resources as an application in both Service Catalog AppRegistry and AWS Systems Manager Application Manager.

AWS Systems Manager Application Manager gives you an application-level view into this solution and its resources so that you can:

- Monitor its resources, costs for the deployed resources across stacks and AWS accounts, and logs associated with this solution from a central location.
- View operations data for the resources of this solution (such as deployment status, CloudWatch alarms, resource configurations, and operational issues) in the context of an application.

  The following figure depicts an example of the application view for the solution stack in Application Manager.

Depicts an AWS Solution stack in Application Manager



Activate CloudWatch Application Insights

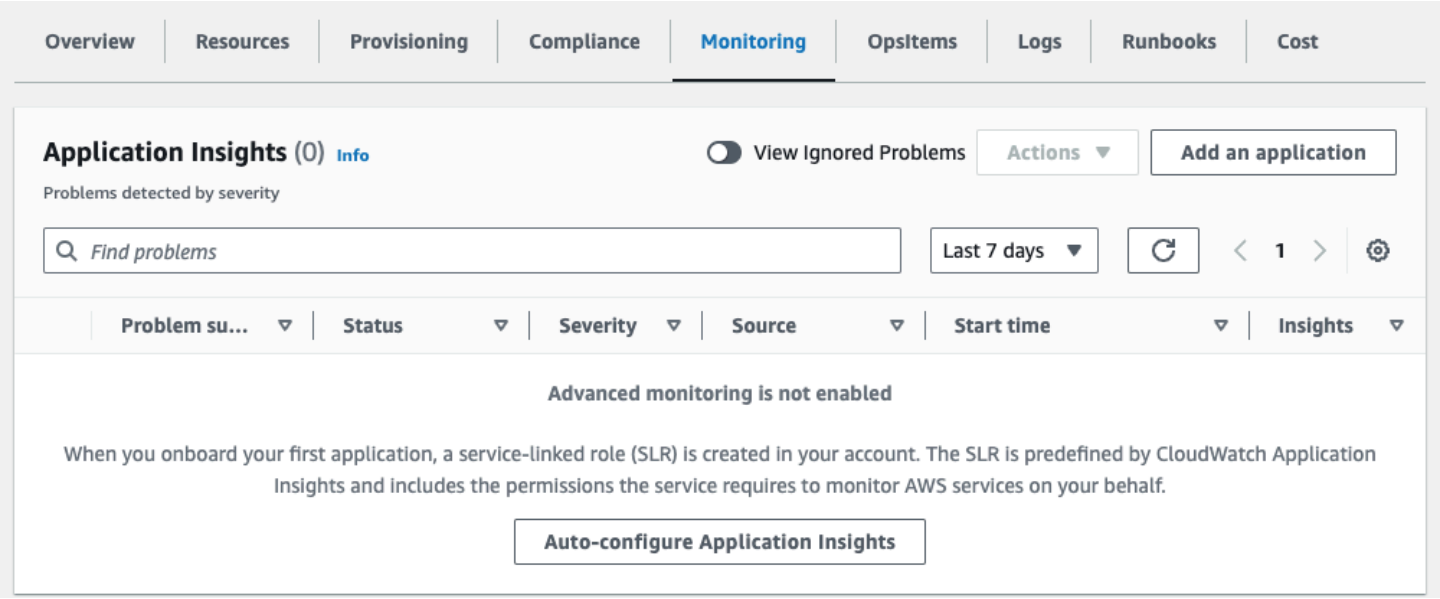
1. Sign in to the Systems Manager console.
2. In the navigation pane, choose **Application Manager**.

3. In **Applications**, search for the application name for this solution and select it.

   The application name will have App Registry in the **Application Source** column, and will have a combination of the solution name, Region, account ID, or stack name.

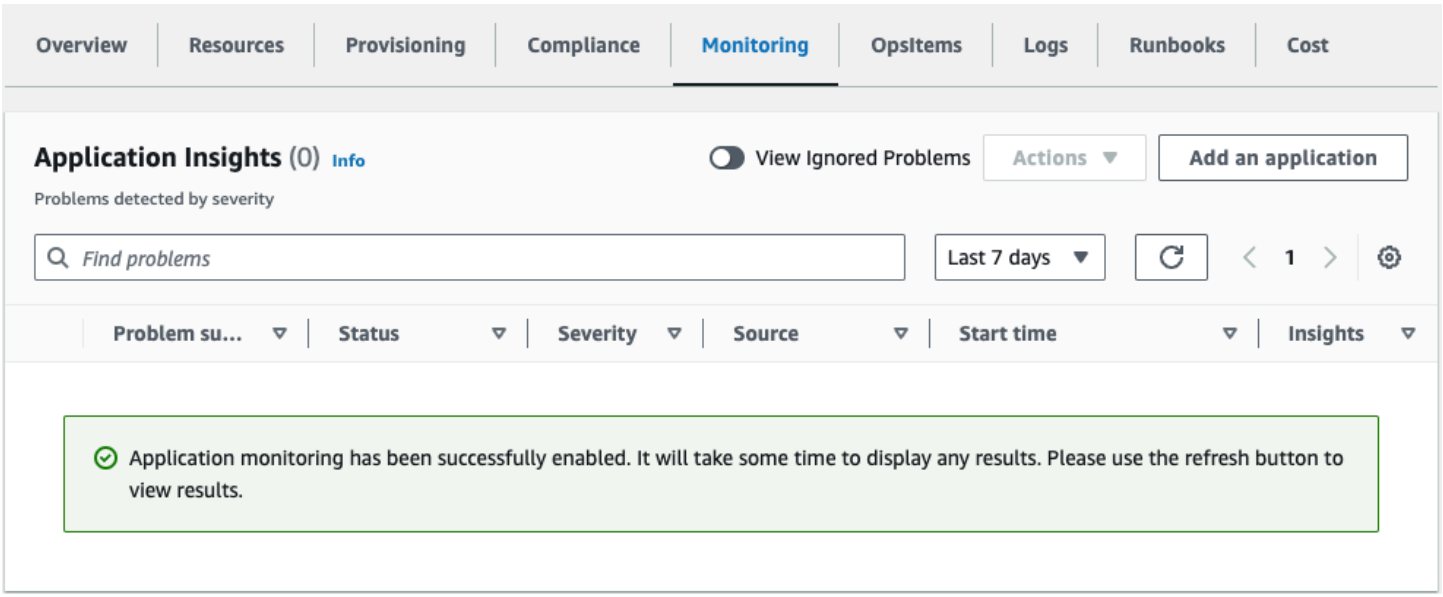
4. In the **Components** tree, choose the application stack you want to activate.
5. In the **Monitoring** tab, in **Application Insights**, select **Auto-configure Application Insights**.

Application Insights dashboard showing no detected problems and advanced monitoring not enabled.



Monitoring for your applications is now activated and the following status box appears:

Application Insights dashboard showing successful monitoring activation message.

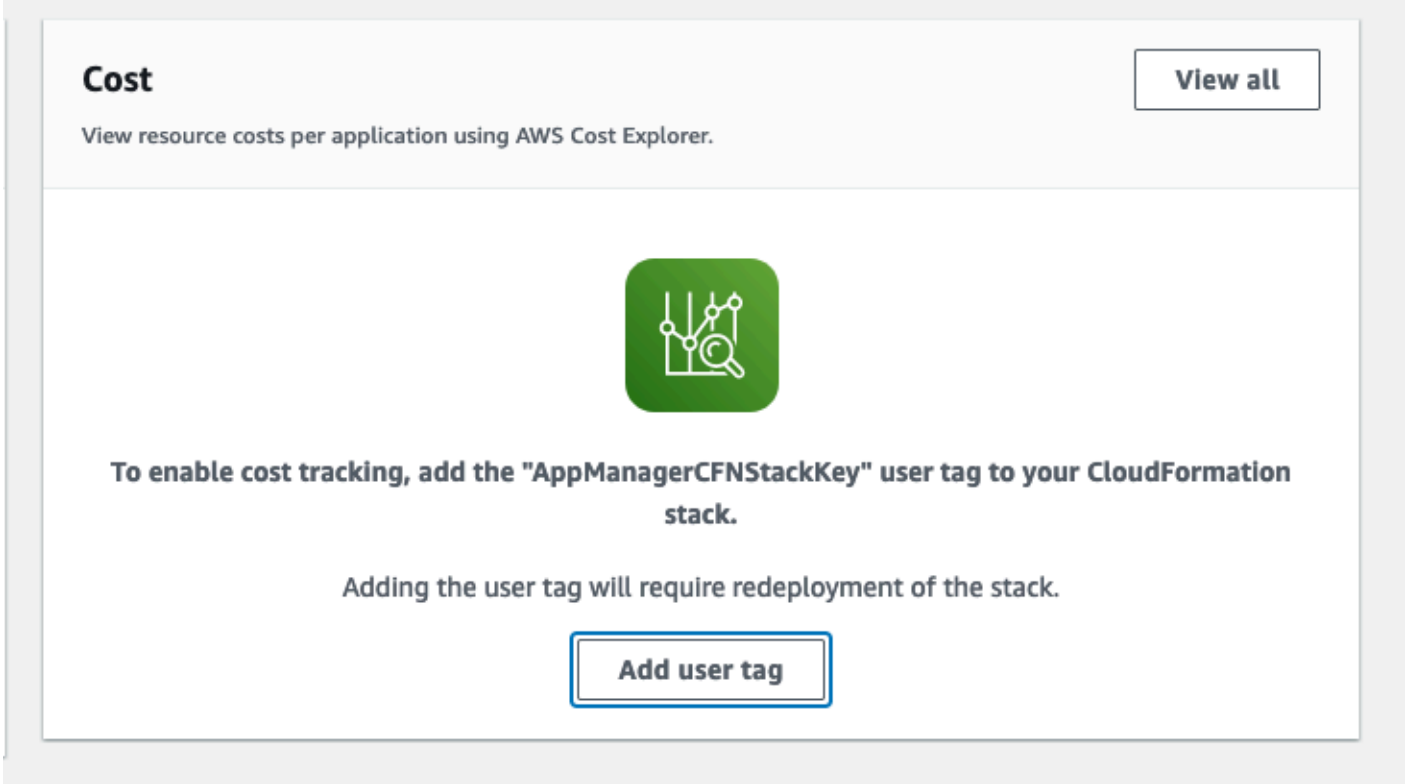


Confirm cost tags associated with the solution

After you activate cost allocation tags associated with the solution, you must confirm the cost allocation tags to see the costs for this solution. To confirm cost allocation tags:

1. Sign in to the Systems Manager console.
2. In the navigation pane, choose **Application Manager**.
3. In **Applications**, choose the application name for this solution and select it.
4. In the **Overview** tab, in **Cost**, select **Add user tag**.

Screenshot depicting the Application Cost add user tag screen



5. On the **Add user tag** page, enter `confirm`, then select **Add user tag**.

The activation process can take up to 24 hours to complete and the tag data to appear.

Activate cost allocation tags associated with the solution

After you confirm the cost tags associated with this solution, you must activate the cost allocation tags to see the costs for this solution. The cost allocation tags can only be activated from the management account for the organization.

To activate cost allocation tags:

1. Sign in to the AWS Billing and Cost Management and Cost Management console.
2. In the navigation pane, select **Cost Allocation Tags**.
3. On the **Cost allocation tags** page, filter for the `AppManagerCFNStackKey` tag, then select the tag from the results shown.
4. Choose **Activate**.

AWS Cost Explorer

You can see the overview of the costs associated with the application and application components within the Application Manager console through integration with AWS Cost Explorer. Cost Explorer helps you manage costs by providing a view of your AWS resource costs and usage over time.

1. Sign in to the AWS Cost Management console.
2. In the navigation menu, select **Cost Explorer** to view the solution's costs and usage over time.

Update the solution

If you have previously deployed the solution, follow this procedure to update the Cloud Migration Factory on AWS solution CloudFormation stack to get the latest version of the solution's framework.

1. Sign in to the AWS CloudFormation console, select your existing Cloud Migration Factory on AWS solution CloudFormation stack, and select **Update**.
2. Select **Replace current template**.
3. Under **Specify template**:
   a. Select **Amazon S3 URL**.
   b. Copy the link for the latest template.
   c. Paste the link in the **Amazon S3 URL** box.
   d. Verify that the correct template URL shows in the **Amazon S3 URL** text box, and choose **Next**. Choose **Next** again.
4. Under **Parameters**, review the parameters for the template and modify them as necessary. Refer to Step 2. Launch the Stack for details about the parameters.
5. Choose **Next**.
6. On the **Configure stack options** page, choose **Next**.
7. On the **Review** page, review and confirm the settings. Be sure to check the box acknowledging that the template might create AWS Identity and Access Management (IAM) resources.
8. Choose **View change set** and verify the changes.
9. Choose **Update stack** to deploy the stack.

You can view the status of the stack in the AWS CloudFormation console in the **Status** column. You should receive a **UPDATE_COMPLETE** status in approximately 10 minutes.

Redeploy the API Gateway APIs

After updating the stack, it is required that you redeploy the API Gateway APIs: admin, login, tools, and user. This ensures that any changes to the configuration are available to all APIs.

1. Sign in to the Amazon API Gateway console , select *APIs *from the left navigation, and then select the CMF API.

2. From the API Resources, select **Actions**, and select **Deploy API**.
3. Select **Deployment Stage *of *prod**, and choose **Deploy**.
4. Repeat steps 1-3 for each of the Cloud Migration Factory on AWS APIs.

> **Note**
>
> Updating the solution adds the current versions of the built-in scripts to the deployment, but it won't set the default versions of the scripts to the latest version. The reason is that we don't want to overwrite any customizations that might have been applied to the solution.

Use the latest versions of the scripts

To use the latest versions of the scripts:

1. Navigate to the Cloud Migration Factory on AWS console.
2. In the navigation menu, select **Automation,** then select **Scripts**.
3. Goto the Cloud Migration Factory on AWS console.
4. Select **Automation**, then **Scripts**.
5. Select the existing script that you want to update to the latest version. Then select **Actions** and choose *Change default version. *
6. For **Script Default Version**, choose the latest version of the script.
7. Choose **Save**.

Update customized scripts

To update scripts that have been customized:

1. Download the updated scripts from the following repository.
2. Extract the contents to see the individual scripts.
3. From one of the new scripts extract the `mfcommon.py` file.
4. Goto the Cloud Migration Factory on AWS console.
5. Select **Automation**, then **Scripts**.

6. Select the existing script to update, and then select **Actions** and choose *Download default version. *
7. Extract the contents of the script archive.
8. Replace the `mfcommon.py` file with the version extracted in Step 3.
9. Compress all the contents of the script, with the new `mfcommon.py` file.
10. Upload this new version, following the instructions in the Add new version of a script package section.

    On the **Automation Scripts** page, for each script you want the latest version to be the default:

    a. Select the script.

    b. From **Actions**, choose **Change default version**.

    c. From **Script Default Version**, choose the latest available version number.
11. Choose **Save**.

(Private deployment only) Redeploy private web console static content

To redeploy private web console static content, complete the steps documented in Step 5: (Optional) Deploy private web console static content section.

Troubleshooting

If you need help with this solution, contact Support to open a support case for this solution.

Contact Support

If you have AWS Developer Support, AWS Business Support, or AWS Enterprise Support, you can use the Support Center to get expert assistance with this solution. The following sections provide instructions.

Create case

1. Sign in to Support Center.
2. Choose **Create case**.

How can we help?

1. Choose **Technical**.
2. For **Service**, select **Solutions**.
3. For **Category**, select **Other Solutions**.
4. For **Severity**, select the option that best matches your use case.
5. When you enter the **Service**, **Category**, and **Severity**, the interface populates links to common troubleshooting questions. If you can't resolve your question with these links, choose **Next step: Additional information**.

Additional information

1. For **Subject**, enter text summarizing your question or issue.
2. For **Description**, describe the issue in detail.
3. Choose **Attach files**.
4. Attach the information that AWS Support needs to process the request.

Help us resolve your case faster

1. Enter the requested information.
2. Choose **Next step: Solve now or contact us**.

Solve now or contact us

1. Review the **Solve now** solutions.
2. If you can't resolve your issue with these solutions, choose **Contact us**, enter the requested information, and choose **Submit**.

Uninstall the solution

You can uninstall the Cloud Migration Factory on AWS solution from the AWS Management Console or by using the AWS Command Line Interface. You must manually empty all the Amazon Simple Storage Service (Amazon S3) buckets created by this solution. AWS Solutions Implementations do not automatically delete S3 buckets in case you have stored data to retain.

Empty the Amazon S3 buckets

If you decide to delete the AWS CloudFormation stack, this solution is configured to retain the created Amazon S3 bucket (for deploying in an opt-in Region) to prevent accidental data loss. You must manually empty all the S3 buckets before deleting the stack completely. Follow these steps to empty the Amazon S3 bucket.

1. Sign in to the Amazon S3 console.
2. Choose **Buckets** from the left navigation pane.
3. Locate the `[.replaceable]`<application name>`-<environment name>-<AWS account ID>\*` S3 buckets.
4. Select each S3 bucket and choose **Empty**.

To delete the S3 bucket using AWS CLI, run the following command:

```
aws s3 rm s3://<bucket-name> --recursive
```

(Migration Tracker only) Delete Amazon Athena workgroup

If you deployed the solution with the Migration Tracker, you must delete the Amazon Athena workgroup.

1. Sign in to the Amazon Athena console.
2. Select **Administration** from the left navigation pane, then select **Workgroups**.
3. Locate the <application name>-<environment name>-workgroup` from the workgroups.
4. From **Actions**, choose **Delete**.
5. Confirm that you want to delete the workgroup.

6. Choose **Delete**.

Using the AWS Management Console to delete the stack

1. Sign in to the AWS CloudFormation console.
2. On the **Stacks** page, select this solution's installation stack.
3. Choose **Delete**.

Using AWS Command Line Interface to delete the stack

Determine whether the AWS Command Line Interface (AWS CLI) is available in your environment. For installation instructions, refer to What Is the AWS Command Line Interface in the *AWS CLI User Guide*. After confirming that the AWS CLI is available, run the following command:

```
aws cloudformation delete-stack --stack-name <installation-stack-name>
```

User guide

The following sections provide guidance on how to use the various features available in a deployed Cloud Migration Factory on AWS instance with a large-scale migration to AWS.

Metadata management

The Cloud Migration Factory on AWS solution provides an extensible datastore that allows records to be added, edited, and deleted from within the user interface. All updates to the data stored in the datastore are audited with record level audit stamps, which provide creation and update timestamps along with user details. All update access to records is controlled by the groups and associated policies that the logged in user is assigned. For more details about granting user permissions, refer to **Permission management.**

Viewing data

Through the **Migration Management** navigation pane, you can select the record types (application, wave, database, server) held in the datastore. After you select a view, a table of the existing records for the chosen record type is shown. Each record type's table shows a default set of columns which can be changed by the user. Changes are persistent between sessions and are stored in the browser and computer used for making the changes.

Changing the default columns displayed in tables

To change the default columns, select the settings icon located on the upper-right corner of any data table, and then select the columns to display. From this screen, you can also change the default number of rows to be displayed and activate line wrapping for columns with large amounts of data.

Viewing a record

To view a specific record in a table, you can click anywhere on the row, or select the check box next to the row. Selecting multiple rows will result in no record being displayed. This will then display the record in read-only mode under the data table at the bottom of the screen. The displayed record will have the following default tables available.

Details - This is a summary view of the required attributes and values for the record type.

All Attributes - This displays a complete list of all the attributes and their values.

Other tabs may be present depending on the record type selected that provide related data and information. For example, **Application** records will have a **Servers** tab showing a table of the servers related to the **Application** selected.

Adding or editing a record

Operations are controlled by record type through user permissions. If a user does not have the required permission to add or edit a specific type of record then the **Add** and/or **Edit** buttons are greyed out and deactivated.

To add a new record:

1. Choose **Add** from the upper-right corner of the table for the record type you want to create.

By default, the **Add application** screen displays the **Details** and **Audit** sections, but depending on the type and any customizations to the schema, other sections might display too.

1. Once you have completed the form and resolved all errors, choose **Save**.

To edit an existing record:

1. Select a record from the table you want to edit, then choose **Edit**.
2. Edit the record and ensure no validation errors exist, then choose **Save**.

Deleting a record

If a user does not have the permission to delete a specific type of record then the **Delete** button is grayed out and deactivated.

> **Important**
>
> Records deleted from the datastore are not recoverable. We recommend making regular backups of the DynamoDB table, or exporting the data to ensure there is a recovery point in the event of an issue.

To delete one or more records:

1. Select one or more records from the table.
2. Choose **Delete** and confirm the action.

Exporting data

The majority of data stored within the Cloud Migration Factory on AWS solution can be exported into Excel (.xlsx) files. You can export data at the record type level or a complete output of all data and types.

To export a specific record type:

1. Go to the table to export.
2. *Optional*: Select the record(s) to export to an excel sheet. If none are selected, then all records will be exported.
3. Choose the **Export** icon in the upper-right corner of the data table screen.

An excel file with the name of the record type (for example, `servers.xlsx`) will be downloaded to the browser's default download location.

To export all data:

1. Go to **Migration Management**, and select **Export.**
2. Check **Download All Data**.

An excel file with the name `all-data.xlsx` will be downloaded to the browser's default download location. This excel file contains a tab per record type, and all records for each type will be exported.

> **Note**
>
> Exported files might contain new columns due to Excel having a cell text limit of 32767 characters. Hence, the export truncates the text for any fields that have more data than supported by Excel. For any truncated fields, a new column with the original name appended with the text `[truncated - Excel max chars 32767]` gets added to the export. Also, within the truncated cell, you will also see the text `[n characters truncated, first x provided]`. The truncation process protects against the scenario

where a user exports and then imports the same Excel, and as a result, overwriting data with the truncated values.

Importing data

The Cloud Migration Factory on AWS solution provides a data import capability that can import simple record structures into the data store, for instance a list of servers. It can also import more complex relational data, for instance it could create a new application record and multiple servers contained in the same file and relate them to one another in a single import task. This allows a single import process to be used for any data type needed to be imported. The import process validates the data using the same validation rules used when the user edits data in the user interface.

Downloading a template

To download template intake forms from the import screen, select the required template from the **Actions list**. The following two default templates are available.

Template with only required attributes - This contains only the attributes marked as required. It provides the minimum set of attributes required to import data for all record types.

Template with all attributes - This contains all the attributes in the schema. This template contains additional schema helper information for each attribute to identify the schema that it was found in. These helper prefixes to the column headers can be removed if required. If left in place during an import, the values within the column will only be loaded into the specific record type and not used for relational values. Refer to **Import header schema helpers** for more details.

Importing a file

Import files can be created in either .xlsx or .csv format. For CSV, it must be saved using UTF8 encoding, otherwise the file will appear to be empty when viewing the pre-upload validation table.

To import a file:

1. Go to **Migration Management**, and select **Import**.
2. Choose **Select file**. By default, you can only select files with either the `0csv` or `1xlsx` extensions. If the file is successfully read, then the file name and size of the file will be displayed.

3. Choose **Next**.
4. The **Pre-upload validation** screen shows the outcome of the mapping of the headers within the file to attributes within the schema, and validation of the values provided.
   - The mappings of the file column headers are shown on the on-screen table column names. To check which file column header was mapped, select the expandable name in the header for more information about the mapping, including the original file header and the schema name it has been mapped to. You will see a warning in the **Validation** column for any unmapped file headers, or where there are duplicate names in multiple schemas.
   - All headers validate the values for each row of the file against the requirements for the mapped attribute. Any warnings or errors in the file content are displayed in the **Validation column.**
5. Once no validation errors are present, choose **Next**.
6. The **Upload data** step shows an overview of the changes that will be made once this file is uploaded. For any item where a change will be performed on upload, you can select **Details** under the specific update type to view the changes that will be performed.
7. Once the review has been completed, choose **Upload** to commit these changes to the live data.

A message appears at the top of the form if the upload is successful. Any errors that occur during the upload are displayed under **Upload Overview**.

Import header schema helpers

By default, the column headers in the intake file should be set to the name of an attribute from any schema, the import process searches all schemas and attempts to match the header name with an attribute. If an attribute is found in multiple schemas you will see a warning, especially for relationship attributes which can be ignored in most cases. However, if the intention is to map a specific column to a specific schema attribute then you can override this behavior by prefixing the column header with a schema helper prefix. This prefix is in the format `{attribute name}`, where `{schema name}` is the name of the schema based on its system name (wave, application, server, database) and the `{attribute name}` is the system name of the attribute in the schema. If this prefix is present then all values will only be populated into records for this specific schema, even if the attribute name is present in other schemas.

As shown in the following figure, the header in column C has been prefixed with `[database]`, forcing the attribute to map to the `database_type` attribute in the database schema.

Import header schema helper

	B	C	D	E	F	G	H	I
1	database_name	[database]database_type	wave_name	aws_accountid	server_name	server_os_family	server_os_version	server_fqdn
2	importdb1	mssql	importwave1	123456789012	importserver1	linux	RH	importserver1

Attribute import format

The following table provides a guide to formatting the values in an import file to import correctly into the Cloud Migration Factory attributes.

Type	Supported import format	Example
String	Accepts alphanumeric and special characters.	`123456AbCd.!`
Multivalue String	A list of string type, delimited by a semicolon.	`Item1;Item2;Item3`
Password	Accepts alphanumeric and special characters.	`123456AbCd.!`
Date	MM/DD/YYYY HH:mm	`01/30/2023 10:00`
Checkbox	Boolean value, in the form of a string, `TRUE` for selected, and `FALSE` for not selected.	`TRUE` or `FALSE`
Textarea	String type with support for line feeds and carriage returns.	`Test line1` or `Testline 2`
Tag	Tags must be formatted as `key=value;` multiple tags must be delimited by a semicolon.	`TagKey1=Tagvalue1; TagKey2=tagvalue2;`
List	If setting a single value list attribute use the same formatting as String type, if multiple selection list then, as per Multivalue String type.	`Selection1;Selecti on2;`

Type	Supported import format	Example
Relationship	Accepts alphanumeric and special characters that need to match with a value based on the key defined in the attribute definition.	`Application1`

Credentials management

The Cloud Migration Factory on AWS solution features a Credentials Manager which integrates with AWS Secrets Manager within the account in which the instance is deployed. The feature allows administrators to save system credentials to AWS Secrets Manager for use in automation scripts without providing users access to retrieve the credentials directly, or needing to provide users access to AWS Secrets Manager. Users can select stored credentials based on their name and description when providing them to an automation job. The automation job will then only retrieve the credentials requested when running on the automation server, and at this point the IAM Role allocated to the EC2 instance will be used to access the required secrets.

The Credentials Manager administration area is only visible to users that are members of the **admin** group within Amazon Cognito. Non-admin users will only be able to view credential names and descriptions when referenced through an automation, or other records relationship.

The following three secret types can be stored in AWS Secrets Manager via Credentials Manager.

OS Credentials - In the form of a ,`username` and `password`.

Secret key/value - In the form of a `key` and `value`.

Plaintext - In the form of a single plain text string.

Add a secret

1. Choose **Add** from the **Credential Manager Secrets** list.
2. Select the **Secret Type** to add.
3. Enter a **Secret Name**. This will be the same name that will be displayed inside AWS Secrets Manager for the secret name.

4. Enter a **Secret Description**. This will be the same description that will be displayed inside AWS Secrets Manager for the secret description.
5. Enter the credential information for the secret type.

> **Note**
>
> For **OS Credentials** secret type, there is an option to select the **OS Type** which can be referenced in custom scripts.

Edit a secret

Except the secret name and type, you can edit all properties of the secret using the Credentials Manager user interface.

Delete a secret

From the Credentials Manager view, select the secret you want to delete and choose **Delete**. The secret will be scheduled for deletion within AWS Secrets Manager which may take a few minutes to complete. Any attempt to add a new secret with the same name during this time will fail.

Run automation from console

The Cloud Migration Factory on AWS solution provides an automation engine allowing users to run jobs in the form of scripts against the inventory within the datastore. With this feature, you can manage, customize, and deploy all automations required to complete the end-to-end migration activities.

Jobs initiated from AWS CMF can be run either via SSM Automation Document or an automation server that can be hosted in the AWS Cloud or on-premise. These servers need to run Windows with the AWS SSM agent installed, along with Python and Microsoft PowerShell. You can also install other frameworks as required for custom automations. Refer to Step 6. Build a migration automation server for details of the automation server build. At least one automation server is required to run jobs from the AWS CMF console.

When to Use Each Platform

Use Traditional Automation Server when:

- Scripts require direct network connectivity to on-premises systems
- Custom software installations or dependencies are needed
- Consistent Windows-based execution environment is required
- Complex authentication mechanisms with on-premises systems are involved

Use SSM Automation Document when:

- Performing AWS-native operations
- No special software dependencies are required
- Scalability and parallel execution are important
- Minimal maintenance overhead is desired

On deployment, you can use scripts for the most common tasks needed to rehost workloads using AWS MGN. Download the scripts from the web interface and use it as a starting point for custom scripts. For details on creating custom automation script, refer to Scripts management.

To initiate a job from the console, select a wave to run the automation against, then select **Actions**, and choose **Run Automation**. Or, you can select a job to run the automation against, then select **Actions**, and choose **Run Automation**.

From the **Run Automation**:

1. Enter the **Job Name**. This will be used to identify the job in the log.

> **Note**
>
> Job names do not have to be unique, as all jobs are also allocated a unique ID and timestamps to further identify them.

1. Select the **Script Name** from the list. This is a list of all scripts that have been loaded into the AWS CMF instance. When the job is submitted, the default version of the script selected will

be run. To check the details of the script, including the current default version, choose **Related details** under the script name. Refer to **Change default version of script package** for details about updating the default version of scripts. When you select the script to run, the required parameters are shown under **Script Arguments**.

2. From the **Instance ID**, select the automation server for the job from the list.

> **Note**
>
> The list will only show instances that have the SSM agent installed and where either the EC2 instance, or for non-EC2 hosted automation servers, the Managed Instance tag of `role` is set to `mf_automation`.

1. In **Script Arguments**, enter the required input arguments for the script.
2. Once you have entered all the required parameters and verified them, choose **Submit Automation Job**.

When you submit the automation job, the following process is initiated:

1. A job record will be created with the AWS Cloud Migration Factory **Jobs** view containing the details of the job and current status.
2. An AWS Systems Manager automation job will be created, and will start to run the AWS Cloud Migration Factory SSM automation document against the automation server provided via the **Instance ID**. The automation document:
   a. Downloads the current default version of the script package from the AWS Cloud Migration Factory S3 bucket to the automation server into the `C:\migration\scripts` directory*.*
   b. Unzips and verifies the package.
   c. Launches the master file python script specified in the `package-structure.yml` included in the zip.
3. Once the master file python script has been launched, any output from the script is captured by the SSM agent and fed into CloudWatch. It is then captured regularly and stored in the AWS Cloud Migration Factory datastore with the original job record, providing a complete audit of the job run.

a. If the script requires credentials to AWS Cloud Migration Factory then the script will contact AWS Secrets Manager to obtain the service account credentials. If the credentials are incorrect or not present then the script will return a failure.

b. If the script has a requirement to access other secrets stored using the AWS Cloud Migration Factory Credentials Manager feature, then it will contact AWS Secrets Manager to access those credentials. If this is not possible then the script will return a failure.

4. Once the master file python script exits, the outcome of this script will determine the status provided to the AWS Cloud Migration Factory job record. A non-zero return will set `Job Status` to `Failed`.

Script Execution Platforms

The Cloud Migration Factory supports two compute platforms for executing automation scripts:

Traditional Automation Server

The default execution method using a Windows-based automation server. This requires maintaining a dedicated server with the required software installations and configurations as detailed in the "Build a Migration Automation Server" section.

SSM Automation Document

Scripts can be executed directly through AWS Systems Manager Automation Documents by specifying "SSM Automation Document" as the Compute Platform in the Package-Structure.yaml file. This option:

- Eliminates the need for a dedicated automation server
- Leverages AWS Systems Manager's native automation capabilities
- Reduces maintenance overhead
- Provides better scalability and reliability

To use the SSM Automation Document platform:

1. In your script package's Package-Structure.yaml file, set: `yaml ComputePlatform: "SSM Automation Document"`

> **Note**
>
> Currently, if a failure occurs in the initial run of the AWS SSM document, it is not shown in the web interface. Failures are only logged once the master file python is launched.
> All jobs initiated from the console will timeout after 12 hours if they have not returned a success or failure status.

Run automations from command prompt

Although we recommend running automation jobs through the web interface, you can run automation scripts manually from a command line on the automation server. This provides additional options where organizations cannot or do not want to use the combination of AWS CMF Credentials Manager, AWS Secrets Manager and AWS Systems Manager in the environment, or if Cloud Migration Factory on AWS users need to provide multi-factor authentication (MFA) one-time access codes to logon to Cloud Migration Factory on AWS.

When scripts are run from the command line, job history and logs are not available from within the **Jobs** view in the web interface. Log output will only be directed to the command-line output only. The scripts can still access the Cloud Migration Factory on AWS APIs to read and update records, and other functions available through the APIs.

We recommend storing scripts in the scripts library or another central location to ensure you are accessing and using the latest version of the script, or the version that is currently approved for use.

Manually running an automation package

This section describes the steps to download a package from Cloud Migration Factory on AWS and manually run it on the automation server. You can also follow the process for other script source locations by replacing steps 1 and 2 with the source specific download steps.

1. If scripts are stored in Cloud Migration Factory on AWS, follow the steps covered in Download script packages to obtain the automation package zip file.
2. Copy the zip file to a location on the automation server, such as `c:\migrations\scripts`, and unzip the contents.
3. Copy the `FactoryEndpoints.json` file to each of the unzipped script folder. Configure the file with the specific API endpoints for the Cloud Migration Factory instance that contains

the servers, or other records this automation job will reference. Refer to Creation of the FactoryEndpoints.json for more information on how to create this file.

4. From the command line, ensure that you are within the root directory of the unzipped package, and run the following command:

```
python [package master script file] [script arguments]
```

package master script file - this can be obtained from the `Package-Structure.yml` under the `MasterFileName` key.

script arguments - information about the arguments is provided in the `Package-Structure.yml` under the `Arguments` key.

1. The scripts will request credentials required for Cloud Migration Factory on AWS APIs and the remote server. Any credentials manually entered are cached in memory for the duration of this process to avoid entering the same credentials again. If you enter script arguments to access secrets stored using the Credentials Manager feature, then access to AWS Secrets Manager and associated secrets is required. If secret retrieval fails for any reason, the script will prompt for user credentials.

Creation of the FactoryEndpoints.json

We recommended creating this file once when deploying Cloud Migration Factory on AWS solution, as the content does not change after initial deployment, and stored in a central location on the automation server. This file provides the automation scripts with the Cloud Migration Factory on AWS API endpoints and other key parameters. An example of the default contents of the file is shown here:

```
{
 "UserApi": "cmfuserapi",
 "VpceId": "",
 "ToolsApi": "cmftoolsapi",
 "Region": "us-east-1",
 "UserPoolId": "us-east-1_AbCdEfG",
 "UserPoolClientId": "123456abcdef7890ghijk",
 "LoginApi": "cmfloginapi"
}
```

> **Note**
>
> Most information required to compose this file for a deployed AWS Cloud Migration Factory instance is available from the AWS CloudFormation **Outputs** tab of the deployed stack, except the `UserPoolClientId`. Obtain this value by completing the following steps:

1. Navigate to the Amazon Cognito console.
2. Open the **User pool configuration**.
3. Select **App integration**, which will provide the **App client configuration**.

```
{
 "UserApi": <UserApi-value>,
 "Region": <Region-value>,
 "UserPoolId": <UserPoolId-value>,
 "UserPoolClientId": <Amazon-Cognito-user-pool-app-clients-console>,
 "LoginApi": <LoginApi-value>
}
```

Replace *<LoginApi-value>*, *<UserApi-value>*, *<Region-value>*, and *<UserPoolId-value>* with the corresponding values you retrieved from the AWS CloudFormation Outputs console. Do not add a forward slash (/) to the end of the URLs.

The file has an optional `DefaultUser` key. You can set the value for this key to the default user ID to be used to access the Cloud Migration Factory on AWS instance to avoid having to enter it every time. When prompted for the Cloud Migration Factory user ID, you can either enter a user ID or use the default value by pressing the enter key. You can only do this when the scripts are run manually.

Launch AWS MGN jobs from Cloud Migration Factory

The Cloud Migration Factory on AWS solution has built in automation to initiate and manage Rehost migration using AWS MGN. These automations allow migration teams to manage all aspects of their migration from a single user interface, combining the key actions available within the AWS MGN service console, with the AWS Cloud Migration Factory automation library that extends the functionality with prebuilt scripts for mass migrations, which helps to increase the speed of the migration activities. Refer to List of automated migration activities for AWS Application Migration Service (AWS MGN) for a full list of AWS MGN automation jobs available.

Using AWS Cloud Migration Factory also provides seamless multi account migrations using AWS MGN as the Cloud Migration Factory has the ability to assume roles in different target accounts automatically based on the Cloud Migration Factory application and server definitions being migrated.

Prerequisite activities

1. Target account AWS CMF CloudFormation deployed into each target account. For more information, review the AWS CloudFormation templates section in this document.
2. AWS MGN is initialized in each target account.

Initial definition

Definition of the on-premises inventory is performed through the creation of wave, application and server items using either the user interface, or through the import of a CSV intake form. These definitions are used to provide the on-premise server identities and also the target EC2 parameters and well as other required data to manage the migration activity.

User interface definition

In order to use the AWS MGN functionality, you need to create a wave record, with associated application records, and finally one or more server records associated to the applications. The wave record is used to group the applications, and does not provide parameters to the automation, whereas the application record defines the target AWS account ID and AWS Region that the application will be migrated to. The server records provide the automations actions and AWS MGN integration the target parameters for the EC2 instances, such as instance type, subnets, security groups, etc.

When defining a server in the AWS CMF datastore for use with the AWS MGN functionality the server needs to be configured with a **Migration Strategy** of **Rehost**. Once Rehost is selected then the additional attributes required for this functionality will be shown on the screen. The following attributes are required to be populated in order to successfully initiate an AWS MGN migration job:

Required

Server OS Family - Set to either linux or windows depending on the OS family.

Server OS Version - Set to the detailed OS version running on the server.

Instance Type - EC2 instance type to be used.

Tenancy - Shared hosting, dedicated host.

Security Group Ids - List of security groups that will be assigned to the instance when the final cutover is initiated.

Security Group Ids - Test - List of security groups that will be assigned to the instance when the testing is initiated.

Conditional

Subnet Ids - Subnet ID to assign this EC2 instance to when the final cutover is initiated. (not applicable when **Network Interface ID** specified)

Subnet Ids - Test - Subnet ID to assign this EC2 instance to when testing is initiated. (not applicable when **Network Interface ID -Test** specified)

Network Interface ID - ENI ID to be used when the final cutover is initiated.

Network Interface ID - Test - ENI ID to be used when testing is initiated.

Dedicated Host ID - Dedicated host ID that the instance will be launched on. (only applicable when **Tenancy** is set to **Dedicated host**).

Optional

Tags - EC2 Instance tags to be applied to instance.

All other attributes not listed here do not have any bearing on the AWS MGN Jobs initiated from within the AWS CMF solution.

Intake form definition

Intake forms can contain the details to create or update multiple types of record with the datastore in a single row of the csv file, this enables the import of related data. In the example below, the wave, application and server records will be created and related to each other automatically during the import.

To import the intake form, follow the same process as other data imports into the Cloud Migration Factory on AWS solution covered in Importing data.

Initiating a job

Initiating an AWS MGN job from AWS CMF is performed against a wave, from the wave list view select the wave, and then from the **Actions** select **Rehost**>**MGN**.

This screen requires the user to make the following choices before they can **Submit** the job.

1. Select the AWS MGN **Action** to perform against the applications and servers in the wave. These actions mostly replicate those available in the AWS MGN service console and API, with the exception of **Validate Launch Template** (see below for details on this action). For details of the effects of each action, refer to AWS MGN user guide.
2. Select the **Wave** to run the action against.
3. Select the **Applications** from the wave that the action will be run against. This list will only show applications that are associated to the Wave selected.
4. Once all options are correct, choose **Submit**.

The automation will now initiate the selected action against each selected application's target AWS account, as specified in the Application record. The results of the action will be displayed in the notification message, including any errors.

Validate launch template

This action is used to validate the configuration data stored in CMF for each server is valid before attempting cutover activities. In order to run this action, you must have successfully deployed the AWS MGN agents onto the source server.

The validations performed for each server are:

- Verify instance type is valid.
- Verify IAM instance profile exists.
- Security groups exist for both test and live.
- Subnets exist for both test and live (if ENI not specified).
- Dedicated host exists (if specified).
  - If dedicated host is specified then the following checks are made:
    - Does the dedicated host support the instance type specified?
    - Does the dedicated host have free capacity for all the requirements of this wave, based on instance types required?

- ENI exists (if specified).

The results of the action will be displayed in the notification message, including any errors.

Replatform to EC2

The Cloud Migration Factory on AWS solution allows groups of EC2 instances to be launched automatically from configurations defined in its datastore; deploying EC2 instances with EBS volumes attached. This provides the ability to provision new EC2 instances, allowing Replatform through AWS CloudFormation, and Rehost of on-premise servers with AWS MGN within a single CMF user interface. Before you can use this functionality the datastore must contain the definition of the servers. Once this has been addressed the servers should be linked to a wave. When the decision is taken to launch the EC2 instances, the user can initiate the following actions against the wave:

- EC2 Input Validation
- EC2 Generate CF Template
- EC2 Deployment

Prerequisites

Permissions to add the Replatform attribute access.

Script Execution Platform Selection

Before deploying automation scripts, determine which compute platform best suits your needs:

- **Traditional Automation Server**: Best for scenarios requiring complex dependencies, multiple programming languages, or specific OS requirements
- **SSM Automation Document**: Recommended for standard Python-based automation scripts where access to on-premises environment is not needed

Initial configuration

Configuration of the new EC2 instances is performed through the creation of new server items using either the user interface or through the import of a CSV intake form containing the server

items. These definitions are converted to AWS CloudFormation templates stored in an S3 bucket within the same AWS account that the AWS CMF instance is deployed.

User interface definition

When defining a server in the AWS Cloud Migration Factory datastore for use with the Replatform to EC2 functionality the server needs to be configured with a **Migration Strategy** of **Replatform**. Once **Replatform** is selected then the additional attributes required for this functionality will be shown on the screen. The following attributes are required to be populated for the functionality to work:

Required attributes

AMI Id - ID of the Amazon Machine Image used to launch the EC2 instance.

Availability Zone - AZ that the EC2 instance will be deployed to.

Root Volume Size - Size in GB of the root volume for the instance.

Instance Type - EC2 instance type to be used.

Security Group Ids - List of security groups assigned to the instance.

Subnet Ids - Subnet ID to assign this EC2 instance to.

Tenancy - Currently the only supported option for the Replatform to EC2 integration is **Shared** any other option will be replaced with **Shared** when the template is generated.

Optional Attributes

Enable Detailed Monitoring - Check to enable detailed monitoring.

Additional Volume Names - List of Additional EBS volume names. Each item in the list needs to map to the same line as the **Size** and **Type** lists.

Additional Volume Sizes - List of additional EBS volume sizes. Each item in the list needs to map to the same line as the **Names** and **Type** lists.

Additional Volume Types - List of additional EBS volume types. Each item in the list must map to the same line as the **Names** and **Size** lists, if not specified then defaults to **gp2** for all volumes.

EBS KMS Key Id for Volume Encryption - If EBS volumes will be encrypted then specify the **Key ID**, **Key ARN**, **Key Alias**, or **Alias ARN**.

Enable EBS Optimized - Select to turn on **EBS Optimized**.

Root Volume Name - Select from the options provided, if not specified then the ID will be used.

Root Volume Type - Provide the EBS type of the volume to be created, if not specified then defaults to **gp2**.

Intake form definition

Intake forms can contain the details to create or update multiple types of record with the datastore in a single row of the csv file, this enables the import of related data. In the following example, the wave, application and server records will be created and related to each other automatically during the import.

Example: Intake form

Column name	Example data	Required	Notes
wave_name	`wave1`	Yes	
app_name	`app1`	Yes	
aws_accountid	`1234567890`	Yes	
server_name	`Server1`	Yes	
server_fqdn	`Server1`	Yes	
server_os_family	`linux`	Yes	
server_os_version	`Amazon`	Yes	
server_tier	`Web`	No	
server_environment	`Dev`	No	
subnet_IDs	`subnet-xxxxxxx`	Yes	
securitygroup_ID	`sg-yyyyyyyyyy`	Yes	
instanceType	`m5.large`	Yes	

Column name	Example data	Required	Notes
iamRole	ec2customrole	No	
tenancy	Shared	Yes	
r_type	Replatform	Yes	
root_vol_size	50	Yes	
ami_id	ami-zzzzzzzzzz	Yes	
availabilityzone	us-west-2a	Yes	
root_vol_type	gp2	No	
add_vols_size	40:100	No	
add_vols_type	gp2:gp3	No	
ebs_optimized	false	No	
ebs_kmskey_id	1111-1111 -1111-1111	No	
detailed_monitoring	true	No	
root_vol_name	Server1_r oot_volume	No	
add_vols_name	Server1_r oot_volum eA: Server1_r oot_volumeB	No	

To import the intake form, follow the same process as any other data imports into the Cloud Migration Factory on AWS solution.

Deployment actions

EC2 input validation

After defining the instance parameters, you must first run the wave action: **Replatform**>**EC2**>**EC2 Input Validation**. This action verifies that all the correct parameters have been provided for each server in order to create a valid CloudFormation template.

> **Note**
>
> This validation does not currently verify that the input parameters are valid, only that they are present in each server definition. You must verify the correct values before creating the template otherwise the deployment of the template will fail.

EC2 generate CloudFormation template

Once the definitions for all servers included in a wave have been verified the CloudFormation template can be generated. To do this, run the wave action: **Replatform**>**EC2**>**EC2 Generate CF Template**. This action creates a CloudFormation template for each application in the wave, where the servers in the application have a **Migration Strategy** of **Replatform**; any servers with other migration strategies defined will not be included in the template.

Once run, the templates for each application will be stored in the S3 bucket: **-gfbuild-cftemplates** , which was automatically created when the Cloud Migration Factory on AWS solution was deployed. The folder structure of this bucket is as follows:

- [Target AWS Account ID]
- [Wave Name]
  - **CFN_Template_ _ 0yaml**

Each time the generate action is run a new version of the template is stored in the S3 bucket. The S3 URIs for the templates will be provided in the notification, these templates can be reviewed or edited as required before deployment.

The CloudFormation templates generate the following CloudFormation resource types currently:

- AWS::EC2::Instance

- AWS::EC2::Volume
- AWS::EC2::VolumeAttachment

EC2 deployment

Once you're ready to deploy the new EC2 instances, you can initiate the **EC2 Deployment** action can be initiated through the wave action **Replatform**>**EC2**>**EC2 Deployment**. This action will use the latest version of the CloudFormation template for each application in the wave, and deploy these templates into the target accounts selected, through AWS CloudFormation.

Scripts management

The Cloud Migration Factory on AWS solution allows users to fully manage the library of automation scripts or packages within the user interface. You can upload new custom scripts as well as new versions of the script using the scripts management interface. When multiple versions are available, an administrator can switch between these versions allowing the ability to test updates before making them default. The script management interface also allows administrators to download script packages to update or review the content.

A supported script package is a compressed zip archive containing the following mandatory files in the root:

- **Package-Structure.yml** - Used to define the script's arguments and other metadata, such as description and default name. Refer to Composing a new script package for more details.
- **[custom python script].py** - This is the initial script that will be run when a job is submitted. This script can call other scripts and modules and if so these should be included in the archive. The name of this script must match the value specified in the `MasterFileName` key in the `Package-Structure.yml`.

Compute Platform Configuration

Two compute platforms are available for executing automation scripts: * "SSM Automation Document" - Executes the script directly as an AWS Systems Manager Automation Document without requiring an automation server * "Automation Server" - Executes the script on a dedicated automation server instance (this is the default platform if not specified)

The compute platform for script execution is defined in the `Package-Structure.yml` file, for direct SSM based autmations, add the following line after `MasterFileName`: `ComputePlatform: "SSM Automation Document"`

Upload new script package

> **Note**
>
> A script package must conform to the supported format. Refer to Composing a new script package for more details.

1. Choose **Add** on the **Automation Scripts** table.
2. Select the package archive file you want to upload.
3. Enter a unique name for the script. Users will reference the script by this name for initiating jobs.

Download script packages

You can download script packages from the console to activate updates and content verification.

1. Select **Automation**, then **Scripts**.
2. Select the script you want to download from the table, then select **Actions** and choose **Download default version** or **Download latest version**.

You can download specific versions of a script. To do so, select the script, then **Actions** and choose **Change default version.** From the **Script Default Version** list, choose **Download selected version**.

Add new version of a script package

Updates to AWS Cloud Migration Factory script packages can be uploaded in the **Automation** > **Scripts** section by following these steps:

1. Select **Automation,** then **Scripts.**
2. Select the existing script to add a new version, then select **Actions** and choose **Add new version**.
3. Select the updated package archive file you want to upload, and choose **Next**. The new script version will keep the existing name by default. Enter a unique script name. Any name change will only be applied to this version of the script.

4. You can make the new version of the script the default version by selecting **Make default version**.
5. Choose **Upload**.

Deleting script packages and versions

You cannot delete scripts or versions of a script for auditing purposes. This allows reviewing the exact script that was run against a system at a point in time. Every script version has a unique signature and ID when uploaded which is recorded against the job history that the script and version was used in.

Composing a new script package

Cloud Migration Factory on AWS script packages support Python as the primary scripting language. You can initiate other shell scripting languages as required from within a Python main program or wrapper. To create a new script package quickly, we recommend downloading a copy of one of the prepackaged scripts and updating it to perform the required task. You must first create a master Python script that will perform the core functionality of the script. Then, create a `Package-Structure.yml` file to define the arguments and other metadata the script requires. Refer to `Package-Structure.yml` options for more details.

Main Python script

This is the initial main script that runs when a job is initiated. Once the script completes running, the task is finished and the final return code determines the status of the job. All output from this script is captured when run remotely and passed into the output audit log of the job for reference. This log is also stored in Amazon CloudWatch.

Accessing Cloud Migration Factory on AWS data and APIs from a script

To provide access to the Cloud Migration Factory on AWS APIs and data, you can use the included python helper module. The module provides the main functions below are some key functions to get started:

`factory_login`

Returns an access token that can be used to call Cloud Migration Factory on AWS APIs. This function will attempt login to CMF using a number of attempts for credentials:

1. By attempting to access the default secret containing the service account userid and password if it exists and access is allowed. This secret name **MFServiceAccount-`userpool id`]** will be checked.
2. If Step 1 is unsuccessful, and the user is running the script from the command line, then the user will be prompted to supply an AWS Cloud Migration factory userid and password. If run from a remote automation job, the job will fail.

`get_server_credentials`

Returns the login credentials for a server stored in AWS Cloud Migration Factory in either Credentials Manager, or through user input. This function will check a number of different sources to determine the credentials for a specific server, the order of the sources is:

1. If local_username and local_password is set and valid then these will be returned.
2. If secret_overide is set then this will be used to retrieve the secret specified from AWS Secret Manager, otherwise, checks if the server record contains the key **secret_name** and this is not empty then this secret name will be used.
3. If there is a failure locating or accessing the secrets specified then the function will fall back to prompting the user for the credentials, but only if the **no_user_prompts** is set to **False**, otherwise it will return a failure.

Parameters

local_username - If passed, then will be returned.

local_password - If passed, then will be returned.

server - CMF Server dict, as returned by get_factory_servers. in AWS Cloud Migration Factory.

Secret_overide - Is passed this will set the secret name to retrieve from Secrets Manager for this server.

No_user_prompts - Tells the function not to prompt a user for a userid and password if not stored, this should be True for any remote automation script.

`get_credentials`

Gets the credentials stored using AWS Cloud Migration Factory Credentials Manager from Secrets Manager.

Parameters

secret_name - name of the secret to retrieve.

get_factory_servers

Returns an array of servers from the AWS Cloud Migration Factory datastore based on the waveid provided.

Parameters

waveid - Wave record ID of the servers that will be returned.

token - Authentication token obtained from the FactoryLogin Lambda function.

app_ids - Optional list of application Ids within the wave to include.

server_ids - Optional list of server Ids within the wave and applications to include.

os_split - If set to `true`, then two lists will be returned one for Linux and one windows servers, if False, then a single combined list will be returned.

rtype - Optional string to filter only for a specific Migration Strategy of servers, i.e. passing the value "Rehost" will return only servers with Rehost.

Final message summary

It is recommended to provide a summary message of the script's outcome as the final output to the screen or sysout. This will be shown on the console in the **Last Message** property, which provides a quick status of the script outcome without the user having to read the full output log.

Return code

The main python script should return a non-zero return code on exit if the function of the script was not completely successful. On receiving a non-zero return code the job status will be shown as **Failed** in the jobs log indicating to the user that they should review the output log for details of the failure.

YAML Package-Structure.yml options

Example YAML file

```
Name: "0-Check MGN Prerequisites"
```

```
Description: "This script will verify the source servers meet the basic requirements
 for AWS MGN agent installation."
MasterFileName: "0-Prerequisites-checks.py"
UpdateUrl: ""
Arguments:
-
name: "ReplicationServerIP"
description: "Replication Server IP."
long_desc: "IP Address of an AWS MGN Replication EC2 Instance."
type: "standard"
required: true
-
name: "SecretWindows"
long_desc: "Windows Secret to use for credentials."
description: "Windows Secret"
type: "relationship"
rel_display_attribute: "Name"
rel_entity: "secret"
rel_key: "Name"
-
name: "SecretLinux"
long_desc: "Linux Secret to use for credentials."
description: "Linux Secret"
type: "relationship"
rel_display_attribute: "Name"
rel_entity: "secret"
rel_key: "Name"
-
name: "Waveid"
description: "Wave Name"
type: "relationship"
rel_display_attribute: "wave_name"
rel_entity: "wave"
rel_key: "wave_id"
validation_regex: "^(?!\\s*$).+"
validation_regex_msg: "Wave must be provided."
required: true
SchemaExtensions:
-
schema: "server"
name: "server_pre_reqs_output"
description: "Pre-Req Output"
type: "string"
```

YAML key descriptions

Required

Name - Default name that the script will use on import.

Description - Description of the usage of the script.

MasterFileName - This is the starting point for the script to run, it has to be a python file name that is included within the script package archive.

Arguments - A list of arguments that the MasterFileName Python script accepts. Each argument needs specified is in the AWS Cloud Migration Factory Attribute definition format. Required properties for each argument are **Name** and **Type**, all other properties are optional.

Optional

ComputePlatform - This key defines where the script will execute. Set to "SSM Automation Document" to run directly in AWS Systems Manager without an automation server. If omitted, defaults to executing on the automation server.

UpdateUrl - Provide a URL where the script package's source is available for providing updates. Currently this is for reference only.

SchemaExtensions - A list of attributes that the Python script requires to be in the schema to store output or retrieve additional data. Each attribute must be specified in the AWS CMF Attribute definition format. Required properties for each attribute are **Schema**, **Name, Description** and **Type**. All other properties are optional. Any new attributes will be automatically added to the schema when the script is initially loaded, and changes to SchemaExtensions will not be processed for new versions of the script. If this is required for a new script to be added, manual updates to the schema must be made.

Pipeline management

The pipeline manager is a component within Cloud Migration Factory on AWS to support the creation and running of a sequence of tasks automatically. The pipeline manager provides a way for users to do the following:

- Run a template of predefined tasks for migration and modernization
- Fully manage the pipelines within the user interface, such as completing manual tasks, retrying a task, or skipping a task as needed

- View the status of a running pipeline
- Check the inputs and logs for any tasks for the pipeline

Add a new pipeline

This section provides instructions for adding a new pipeline.

1. Select **Automation**, then select **Pipelines**.
2. In the **Pipelines** table, choose **Add**.
3. Enter **Pipeline Name** and **Pipeline Description**.
4. Select a template from the **Pipeline Template**.
5. Enter **Task Arguments** for the selected pipeline template.
6. Choose **Save** to run the pipeline.

Delete a pipeline

This section provides instructions for deleting a pipeline.

1. Select **Automation**, then select **Pipelines**.
2. In the **Pipelines** table, select one or more pipelines.
3. Choose **Delete**.

View pipeline status

This section provides instructions for viewing the pipeline status.

1. Select **Automation**, then select **Pipelines**.
2. In the **Pipelines** table, select one pipeline.
3. Select **Details**, then **Pipeline template**, and then the **Pipeline template tasks** tab to view the template information.
4. Select the **Manage** tab to view the visual representation of the pipeline to where you can manage the tasks and view detailed status.
5. Select the **Tasks** tab to view and manage the execution status of individual the pipeline tasks.

Manage pipeline tasks

This section provides instructions for managing pipeline tasks from the web interface. You can view tasks inputs and logs as well as update the status of each task.

1. Select **Automation**, then select **Pipelines**.
2. In the **Pipelines** table, select one pipeline.
3. Select the **Tasks** tab.

   From the task list, you can see the high-level status of each task such as task execution status and last modified time.

To manage an individual task, complete the following steps:

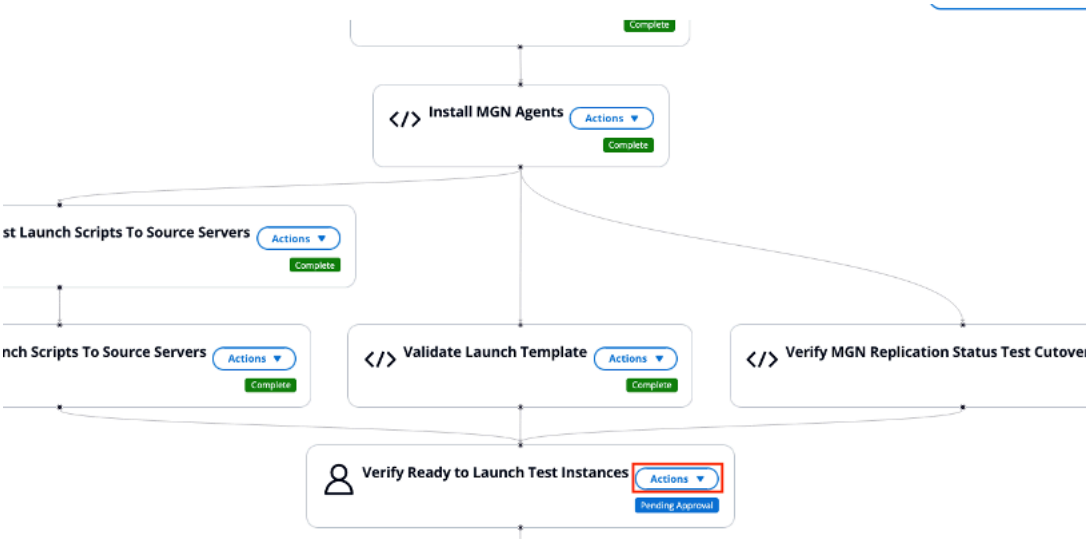
1. Select one of the tasks from the list.
2. Select **Actions**, then select **View Inputs and logs** to verify the inputs and view logs of that task.

To change the status of the task, such as **retry** or **skip**, complete the following steps:

1. Select **Actions**, then select **Update Status**.
2. Select one of the statuses from the list to change the status. For example, select **Complete** to complete a manual task.

You can also manage pipeline tasks in the visual representation of the pipeline under the **Manage** tab. As shown in the following diagram, each task is represented by a node on the graph, and on each task you can initiate the actions.

Pipeline showing tasks for Install MGN Agents Validate Launch Template, and Verify Reading to Launch Test Instances.



Conditional Branching

The Conditional Branching feature in Cloud Migration Factory on AWS allows users to control which parts of their migration pipeline to execute. This feature enables skipping pipeline paths that are not required for specific migration waves.

Conditional Branching allows you to:

1. Choose which parts of your pipeline to execute during a migration
2. Skip steps that are not required for a specific migration wave
3. Have more control over your migration pipelines

How It Works

Manual Decision Points

1. To enable conditional branching, you need to add manual approval steps at the start of each potential branch in your pipeline.
2. These steps act as decision points where you can choose which path to take.

Complete or Abandoned

When your pipeline reaches a manual approval step, you have two options:

1. **Complete**: The branch will continue executing as normal.

2. **Abandoned**: The branch will not execute, and all tasks in that branch will be skipped.

Automatic Propagation

1. If you abandon a task, all tasks that exclusively depend on it will also be automatically abandoned.
2. This allows you to effectively abandon an entire branch with just one action.

Joining Branches

1. If abandoned and approved branches join later in the pipeline, the joined tasks will still run as long as at least one incoming branch was successful.
2. This ensures that necessary tasks are not skipped unintentionally.
3. A task will only be automatically abandoned when all its predecessors are abandoned.

Using Conditional Branching

1. **Prepare Your Pipeline**: When creating your pipeline, add manual approval steps at the beginning of each potential branch.
2. **Start the Pipeline**: Begin your migration pipeline as usual.
3. **Make Decisions**: When the pipeline reaches a manual approval step:
   a. Review the upcoming branch.
   b. Decide whether this branch is necessary for your current migration.
   c. Choose to either approve or abandon the task.
4. **Monitor Progress**: As the pipeline progresses, you'll see some branches executing and others marked as abandoned based on your choices.
5. **Review Results**: At the end of the pipeline, review which branches were executed and which were abandoned to ensure the migration proceeded as intended.

Best Practices

1. Use clear naming conventions for your manual approval steps to easily identify what each branch does.
2. Regularly review your pipeline structure to ensure it allows for efficient decision-making.

Important Notes

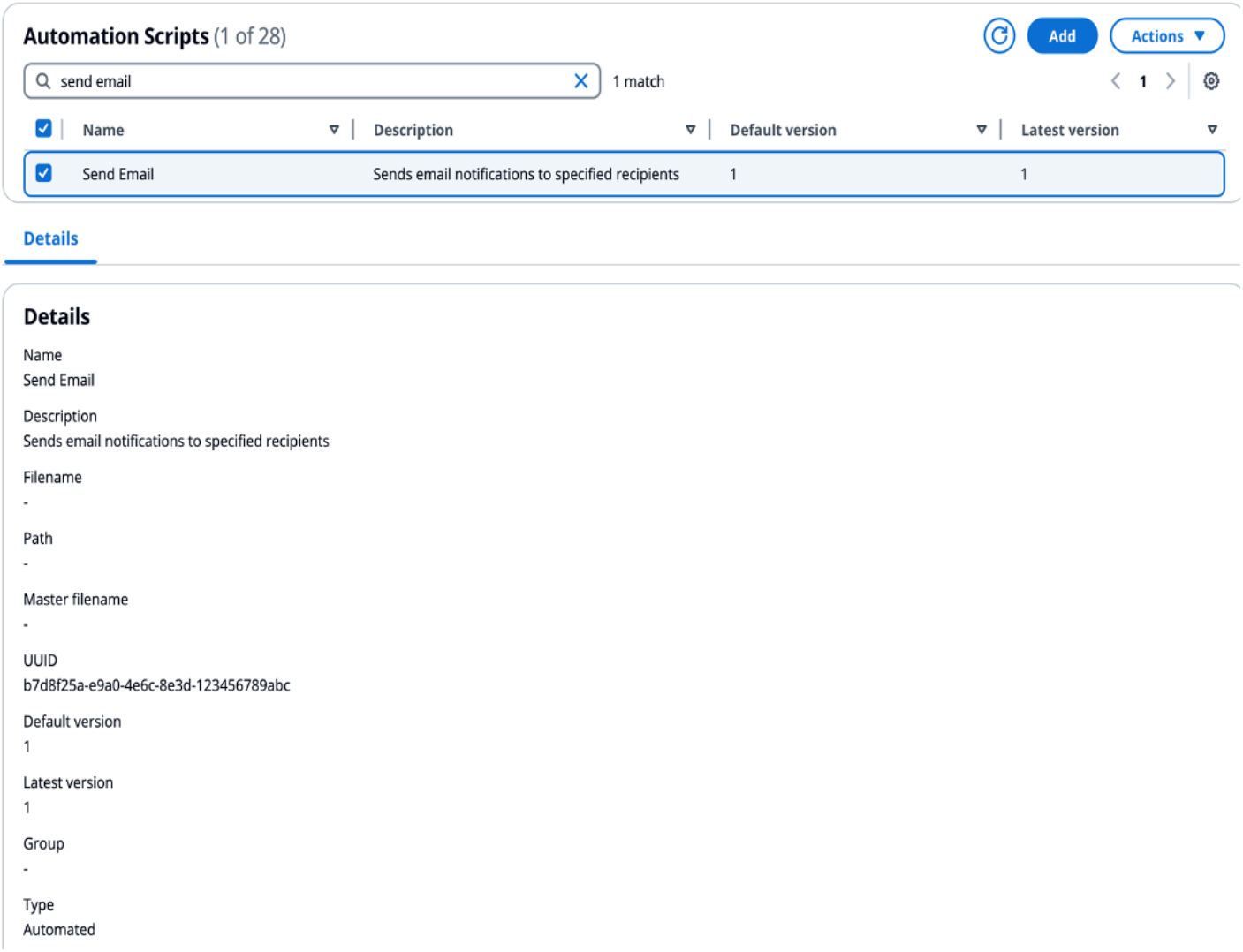
1. You can only abandon tasks that are in "Pending Approval" or "Not Started" status.
2. Once a task has started executing, it cannot be abandoned.
3. Abandoned tasks are considered neither successful nor failed - they are simply skipped.
4. You cannot directly abandon automated tasks as they do not wait for approval and immediately go to the In-progress state. Automated tasks are only abandoned through propagation if all their predecessors are abandoned. Also manage pipeline tasks in the visual representation of the pipeline under the **Manage** tab. As shown in the following diagram, each task is represented by a node on the graph, and on each task you can initiate the actions.

Email notifications

Email notifications are triggered in three scenarios during pipeline execution:

- When a task fails
- When a manual task requires user approval
- For "Send Email" automation tasks ("Send Email" is a new type of automation that serves the sole purpose of sending an email with a custom body). A "Send Email" task might show a "Complete" status in the UI but this does not guarantee the delivery of the actual email notification. For the user to actually receive email from a email automation task they need to confirm SNS subscription. This is explained further in Email Recipient User Management.

  Send Email Automation Task Details



Configuring email notification settings

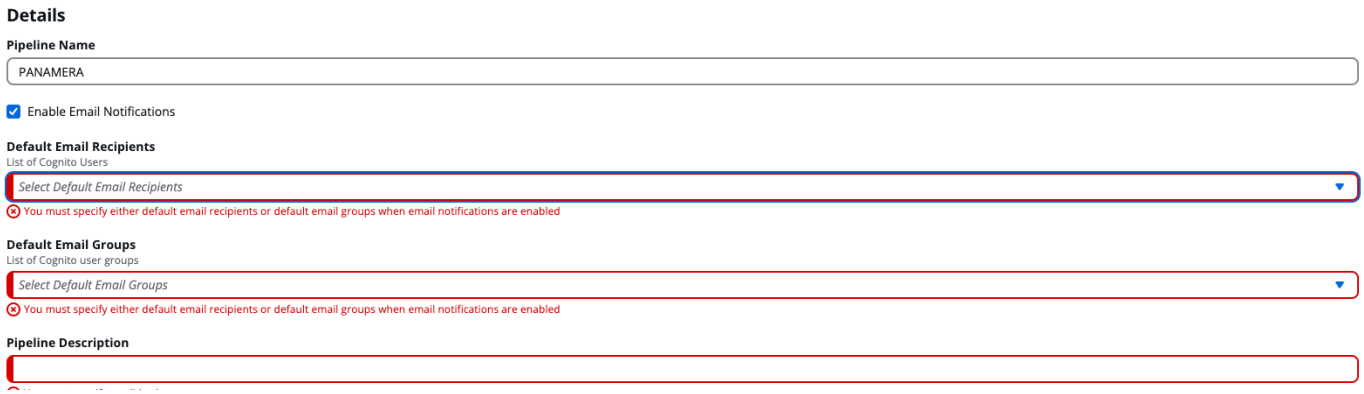
Email notifications can only be configured during pipeline creation by:

- Enabling email notifications (checkbox). If disabled, no emails will be received from this pipeline and no email settings are visible.

Enable Email Notifications Toggle during Pipeline Creation

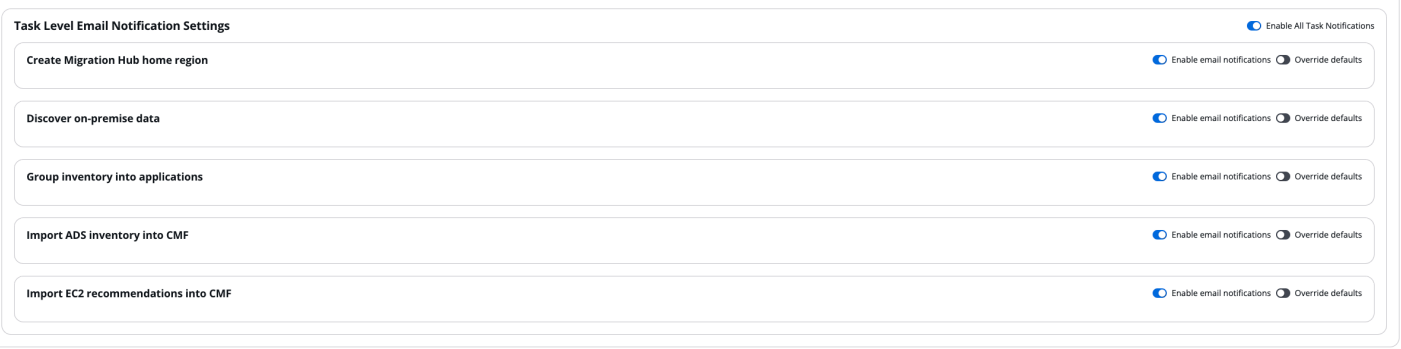
- If Enable Email Notifications is set to true, you have to populate at least one of the following default email settings:
  - Default email recipients
  - Default email groups

Email Notification Recipients Configuration



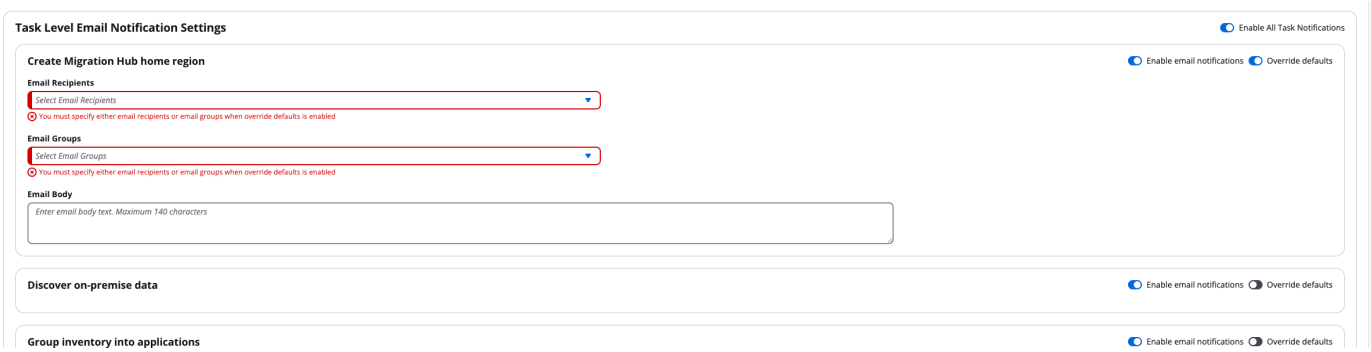
- Once email notifications are enabled using the Enable Email Notifications, and a pipeline template is selected, you can enable email notifications for each task individually or all tasks at once. If emails are disabled for all tasks, users will not receive any emails for any tasks despite pipeline level Enable Email Notifications being set to true.

Task Level Email Notification Toggle



- Once task level email notifications are enabled, you can optionally enable Override Defaults. If Override Defaults is enabled, at least one of the following needs to be populated, and these task level email settings are used, else the default email settings are used:
  - Email recipients
  - Email groups

Task Level Email Recipients Configuration



If a custom email body is not provided by the customer, Cloud Migration Factory sends a default email message based on the event that triggered the email. If custom email body is provided, it appears in addition to this default email message.

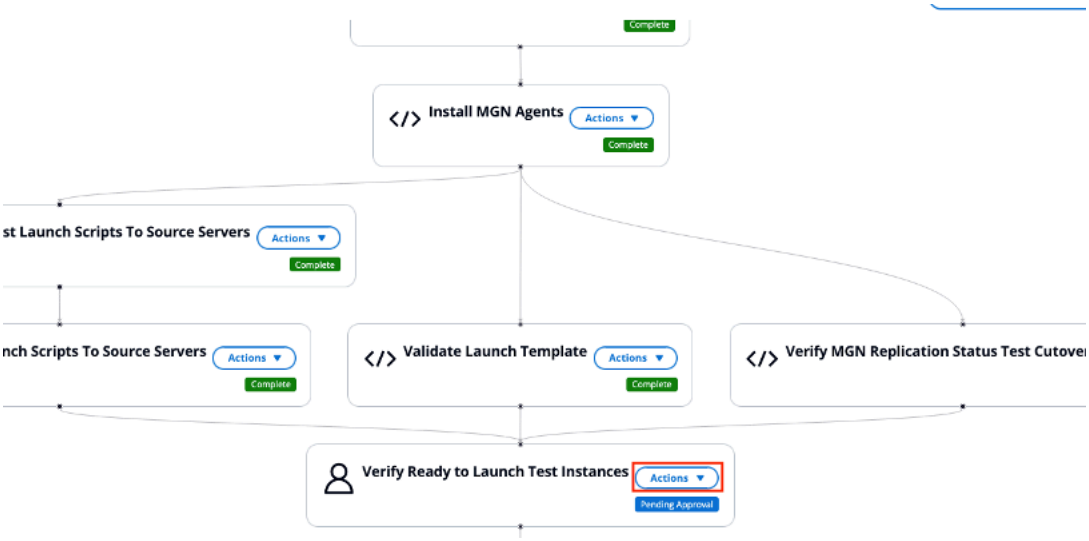
Example: Task "Create Migration Hub home region" uses task-level email settings. Task "Discover on-premise data" uses default email settings.

Email recipient user management

- Users are automatically added to the Email SNS topic upon addition to Cognito users list. Users will only receive email notifications if:
  - They are part of the email recipient list
  - They have a valid email address
  - They have confirmed SNS subscription (via email confirmation link).
- When a user's email address is updated in the Cognito user pool, they have to sign in to Cloud Migration Factory with the new email address to start receiving email notifications to their updated email address.

You can also manage pipeline tasks in the visual representation of the pipeline under the **Manage** tab. As shown in the following diagram, each task is represented by a node on the graph, and on each task you can initiate the actions.

Pipeline showing tasks for Install MGN Agents Validate Launch Template, and Verify Reading to Launch Test Instances.



Pipeline Template Creation Using Visual Tools

This section describes how to create Cloud Migration Factory pipeline templates using visual diagramming tools. The solution supports template creation using either DrawIO or Lucid Chart.

Check Prerequisites

- Access to either DrawIO or Lucid Chart diagramming tool
- Access to your Cloud Migration Factory environment
- List of valid automation script IDs from your CMF instance

Template Components

A pipeline template consists of the following core components:

Element Type	Shape	Use When...
Start Node	Circle	Indicating the start of a flow and when indicating the start of a branch
Automated Task	Rectangle	Indicating that the automation exists already as part of the automation library of CMF
Manual Task	Rectangle	Indicating that the task at hand is manual
Connection	Line/Arrow	Shows task sequence

Data Attributes

Each shape requires specific attributes for CMF conversion:

Element Type	Required Attribute	Example
Start Circle	Start	"Start": "Wave 1 Migration"
Automated Task	TaskType, AutomationID	"TaskType": "Automated", "AutomationID": "<VALID_CMF_SCRIPT_NAME>"
Manual Task	TaskType	"TaskType": "Manual"

Important Concepts

Before creating your diagram, understand these key elements that enable successful conversion to CMF templates:

1. Template Naming
   a. Your diagram's tab/sheet name becomes your CMF template name.
   b. Names must be unique across CMF.

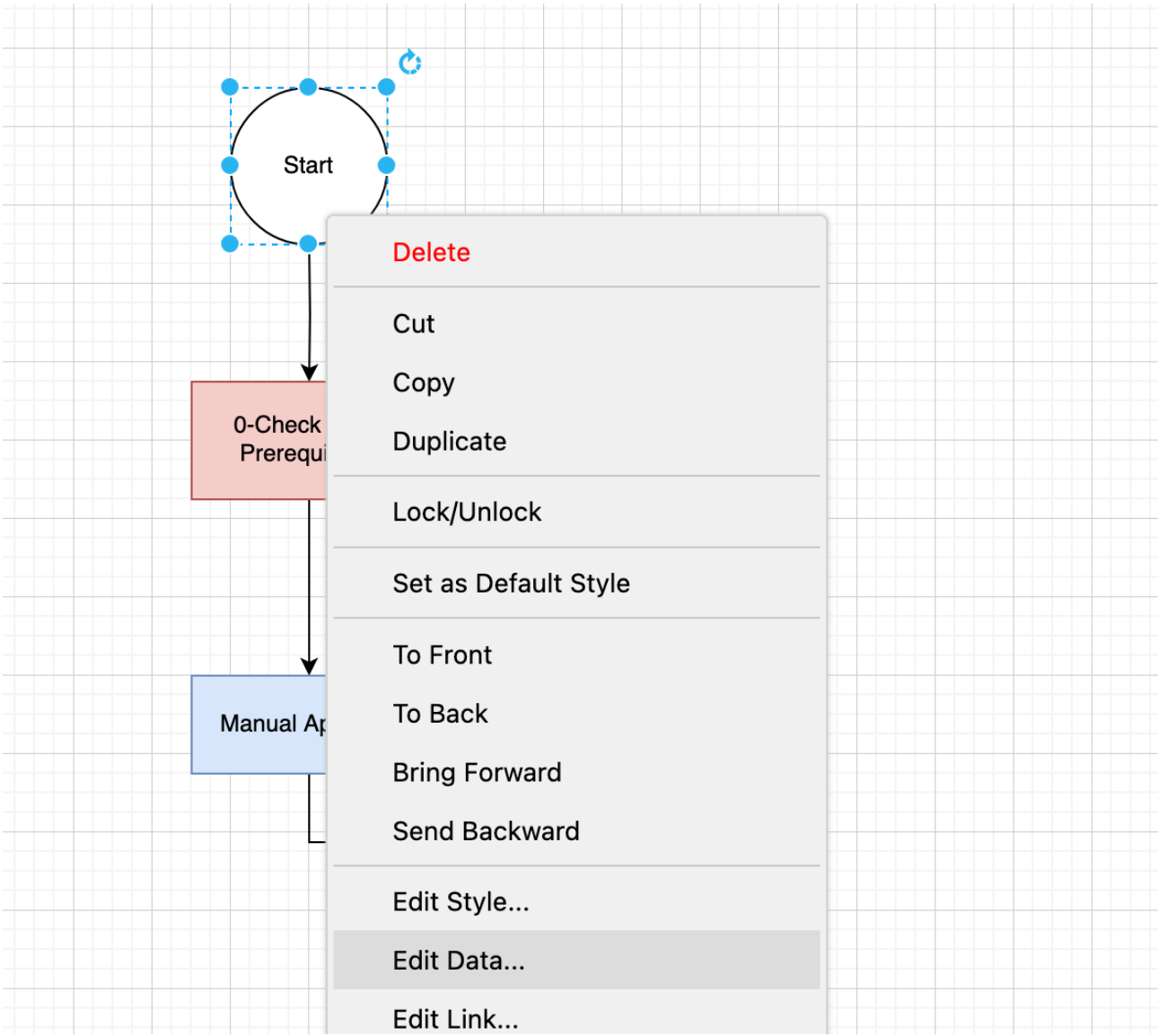
c. Each tab creates a separate CMF template, allowing you to design multiple templates in a single file.

2. Task Naming
   a. The task name will be identical to the text/label you give to each shape in your diagram.
   b. Ensure each task has a unique and descriptive label for clear identification.
3. Attribute Requirements
   a. TaskType must be exactly "manual" or "automated"
   b. AutomationID must match existing CMF scripts name
   c. Start circle's "Start" property defines template description

Creating templates in DrawIO

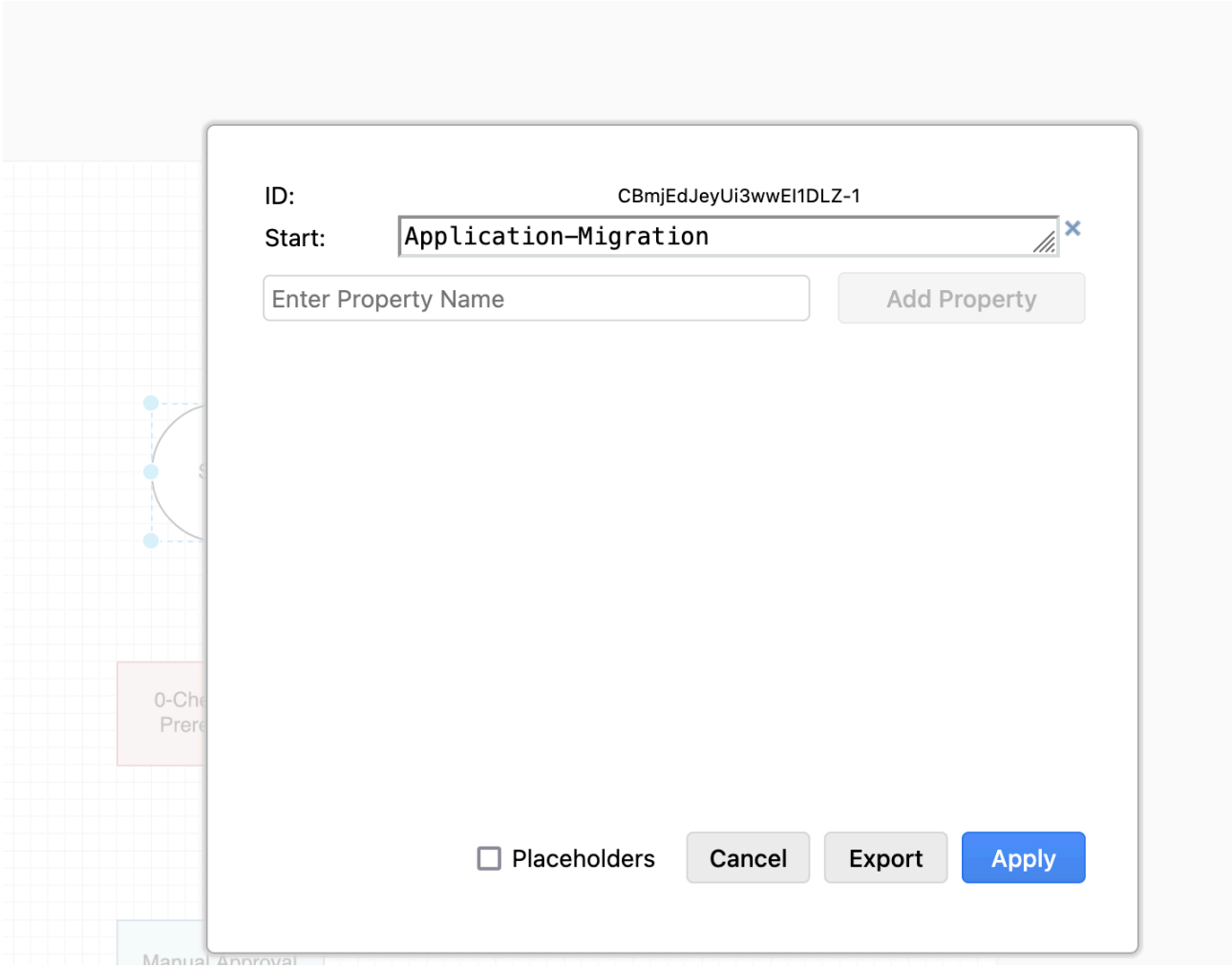
1. Create Start Node:
   a. Drag a Circle shape onto the canvas
   b. Double-click and label it "Start"
      i. Add Start attribute:
         A. Right-click circle → Edit Data

DrawIO Shape Right-click panel



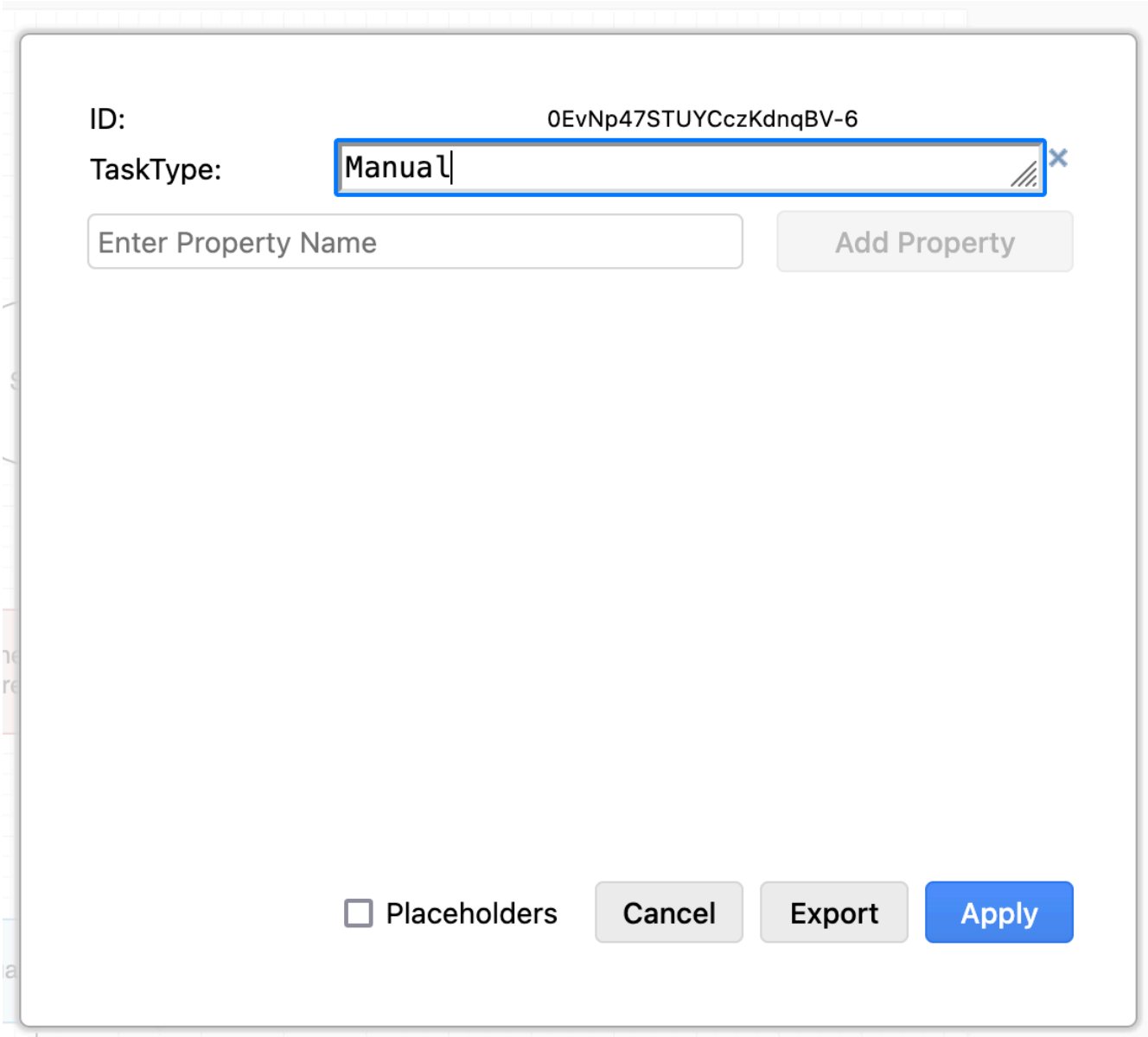
B. Add Data Attribute key "Start" and value (e.g., "Wave 1 Migration")

DrawIO Shape Data



2. Manual Task:
   a. Drag a Rectangle shape onto the canvas
   b. Double-click and add a descriptive label
   c. Add attributes:
      i. Right-click rectangle → Edit Data
      ii. Add Data Attribute key "TaskType" with value "Manual"

DrawIO Manual Task Configuration

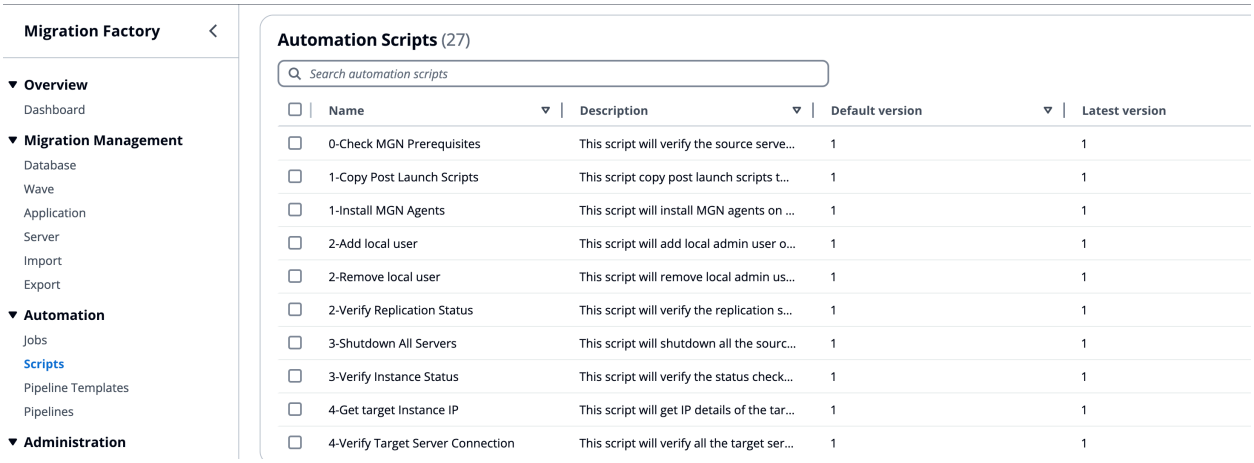


3. Automated task:
   a. Drag a Rectangle shape onto the canvas
   b. Double-click and add a descriptive label, this will be Task Name in CMF
   c. Add attributes:
      i. Right-click rectangle → Edit Data
      ii. Add Data Attribute key "TaskType" with value "Automated"
      iii. Add Data Attribute key "AutomationID" with a valid CMF script name.
         A. To find valid AutomationID:
            I. Log into CMF portal

II. Navigate to "Scripts" under Automation in the left navigation bar

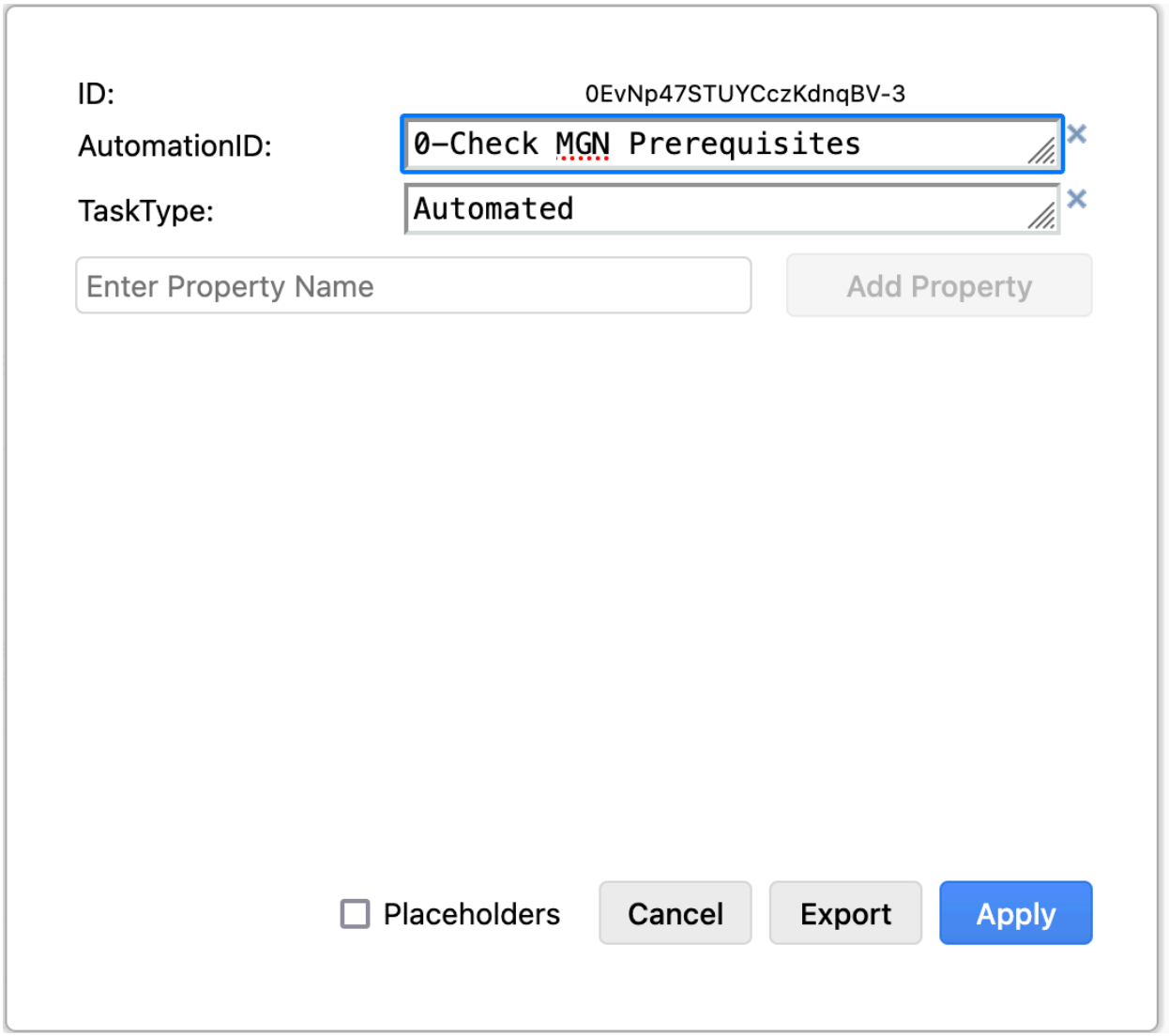
III. Browse or search for your desired script

CMF Scripts List



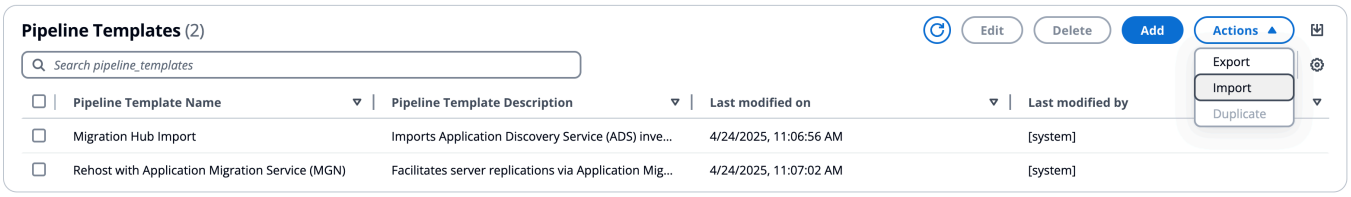
IV. Use the script name as your AutomationID in your diagram

DrawIO Automated Task Configuration



4. Set template name
   a. Rename the diagram tab to your desired template name
5. Saving & Exporting
   a. File → Save As → Format: .drawio
6. Uploading to CMF
   a. Log into CMF portal
   b. Navigate to "Pipeline Templates" in the left navigation bar
   c. Click on "Actions" and select "Import"

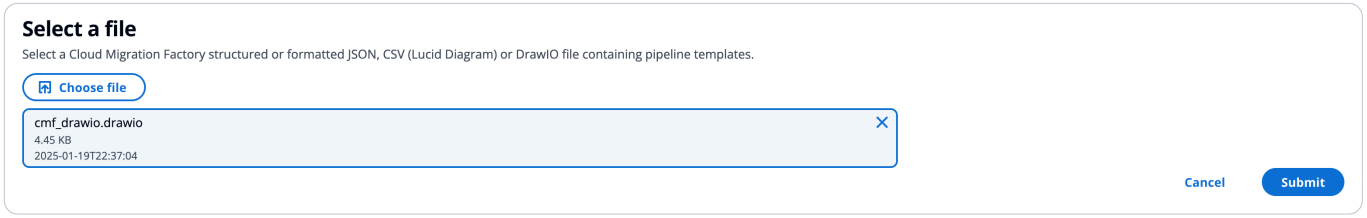
Pipeline Templates Action→Import



d. Choose your saved .drawio file

e. Click "Submit" to complete the import

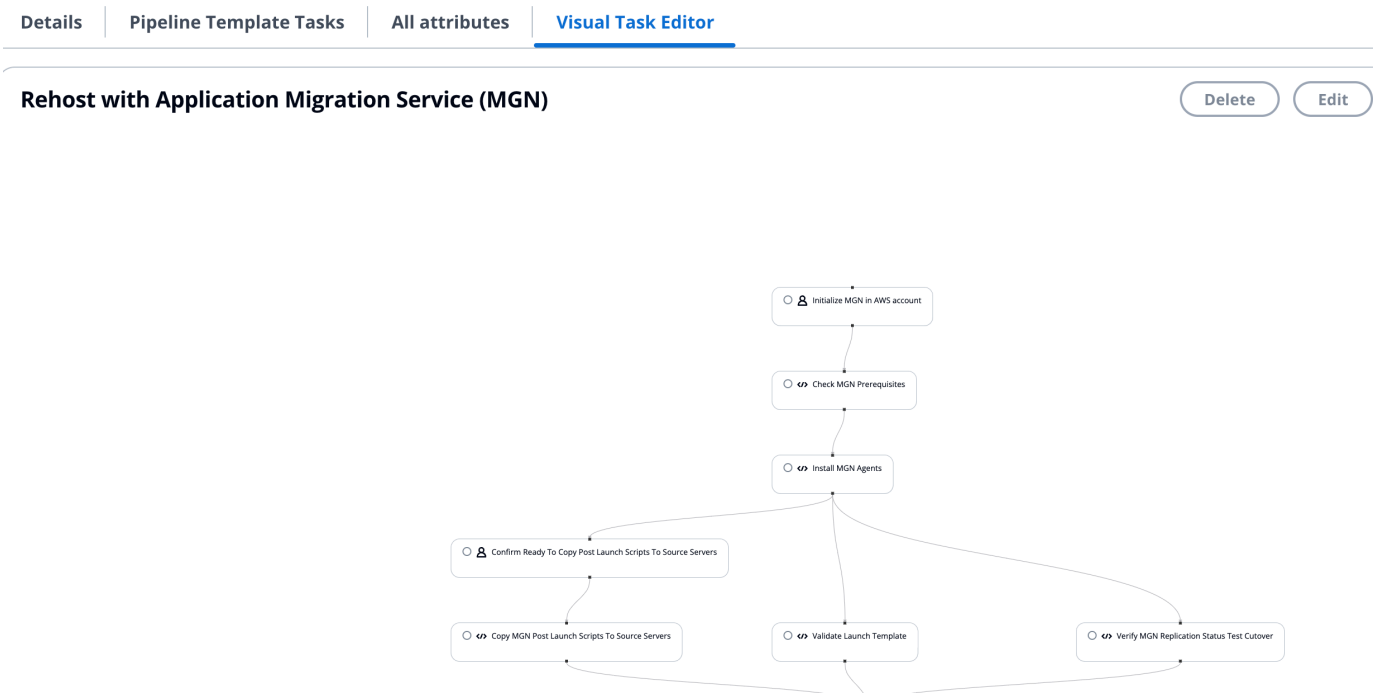
Template Import Submit



After drawIO import is complete

1. A new template will be created under Pipeline Templates
2. To see how your diagram attributes are converted in CMF:
   - Locate your newly created template in the Pipeline Templates list
   - Click on the template to open it
   - You'll see a visual representation of your workflow under Visual task Editor

Pipeline Template Visual Task Editor



- Each shape from your diagram is now a task in CMF
- Click on a task to view its details:
  - Task names correspond to the labels you gave shapes
  - For automated tasks, you'll see the assigned AutomationID under Scripts dropdown.

Pipeline Template Task Edit

Edit pipeline Template Task

Details

Template Task Name

MGN Prerequisites

Script

0-Check MGN Prerequisites

Related details

Clear

Script Version

1

Task Successors

1 Task Successors selected

Manual Approval

Audit

Created by
serviceaccount@yourdomain.com

Created on
2025-04-25T21:06:09.618549+00:00

Last modified by
serviceaccount@yourdomain.com

Last updated on
2025-04-25T21:08:31.983969+00:00

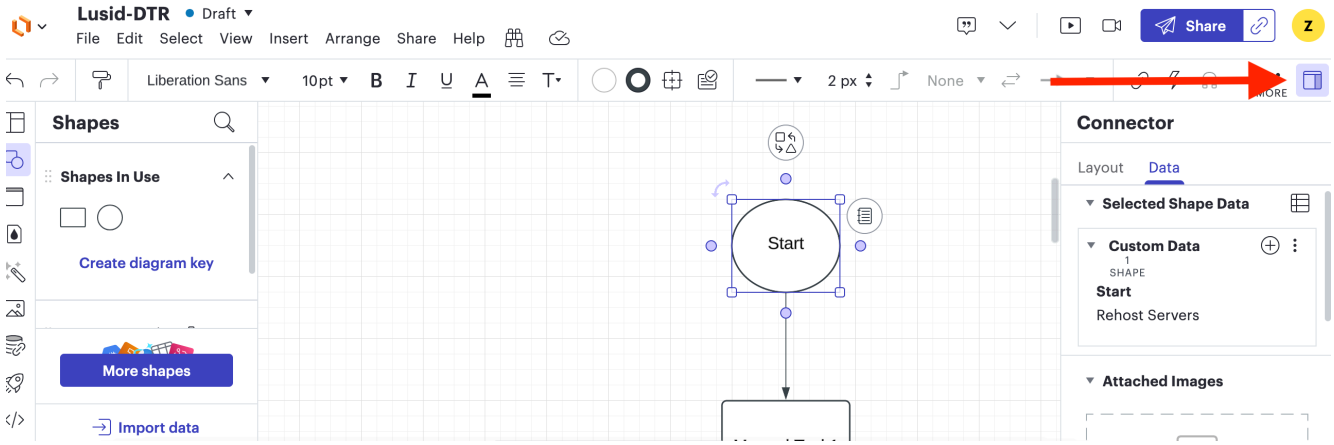
Cancel Save

Creating Templates in Lucid Chart

Follow these steps to create pipeline templates using Lucid Chart:

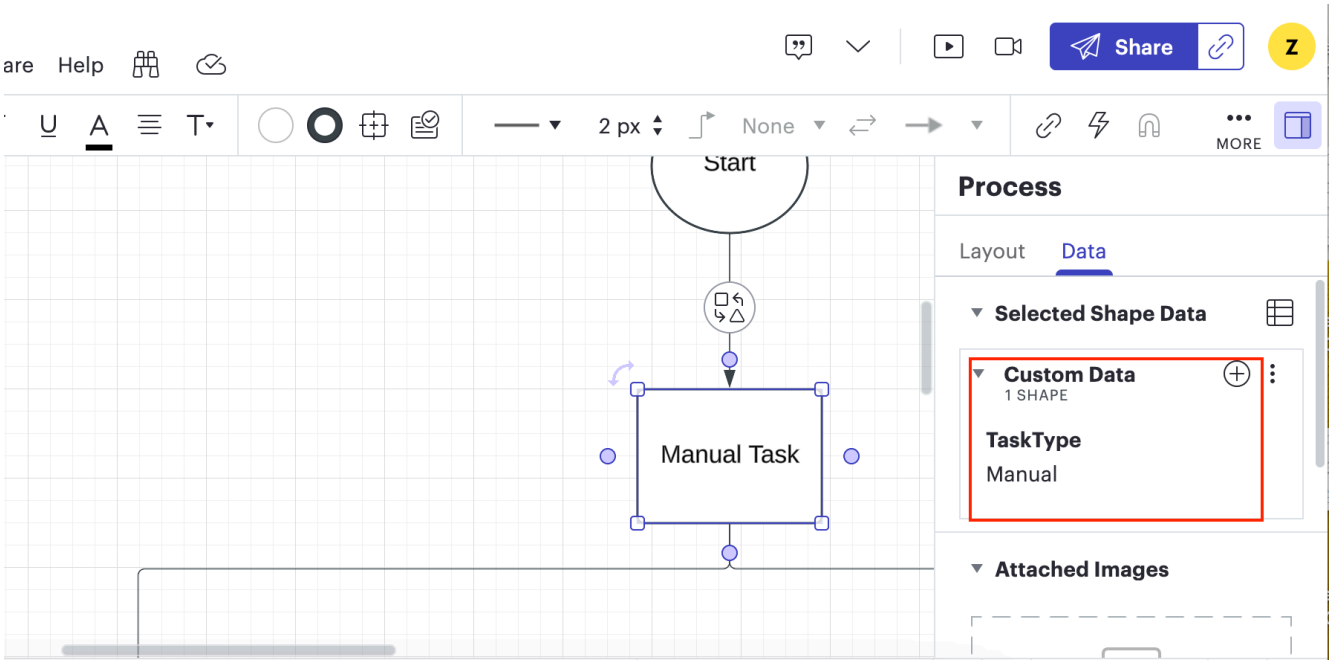
1. Create Start Node
   a. Drag a Circle shape onto the canvas
   b. Double-click and label it "Start"
   c. Add Start attribute:
      i. Click the data icon (marked by red arrow in UI)
      ii. Select the "Data" tab
      iii. Add Data Attribute key "Start" and value (e.g., "Rehost Servers")

Lucid Chart Start Node Configuration



2. Add Manual Tasks
   a. Drag a Rectangle shape onto the canvas
   b. Double-click and add a descriptive label
   c. Add attributes:
      i. Click the data icon
      ii. Select the "Data" tab
      iii. Add Data Attribute key "TaskType" with value "Manual"

Lucid Chart Manual Task Configuration

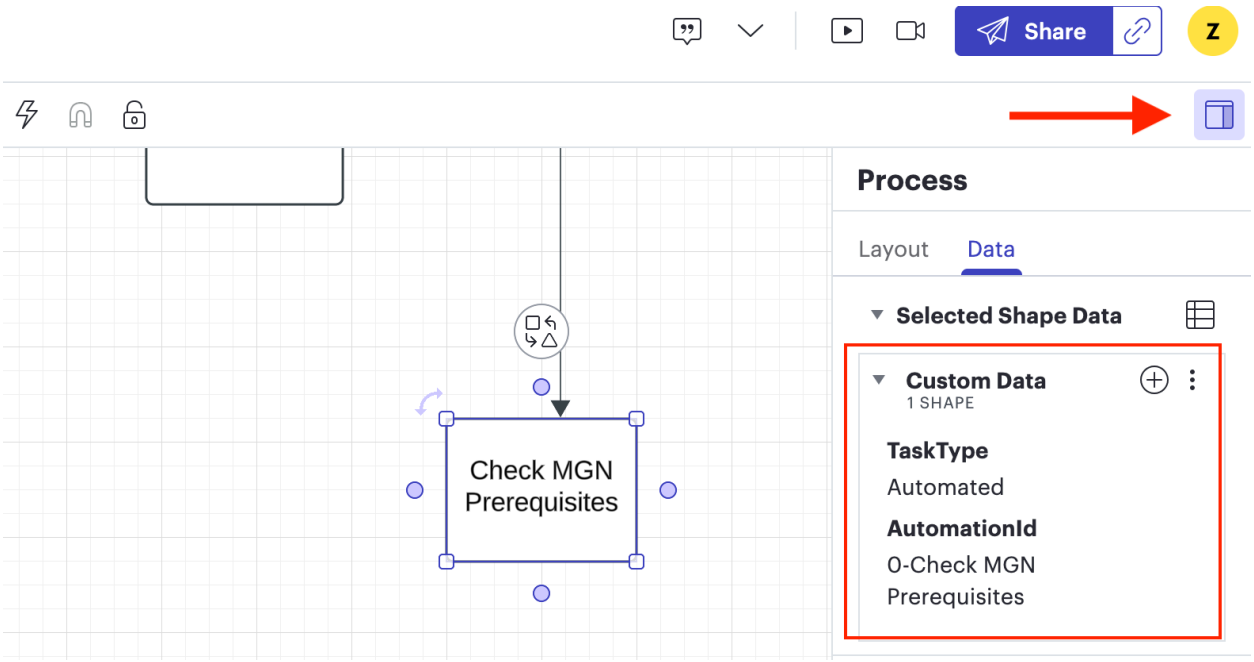


3. Add Automated Tasks
   a. Drag a Rectangle shape onto the canvas
   b. Double-click and add a descriptive label
   c. Add attributes:
      i. Click the data icon
      ii. Select the "Data" tab
      iii. Add Data Attribute key "TaskType" with value "Automated"
      iv. Add Data Attribute key "AutomationID" with a valid CMF script name
         A. To find valid AutomationID:
            I. Log into CMF portal
            II. Navigate to "Scripts" under Automation in the left navigation bar
            III. Browse or search for your desired script

CMF Scripts List

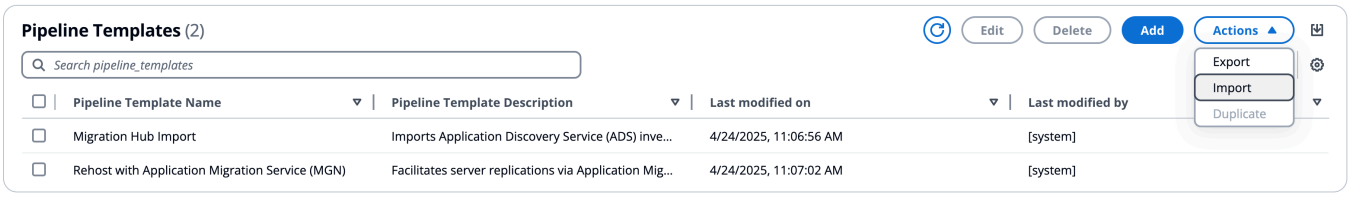
            IV. Use the script name as your AutomationID in your diagram

Lucid Chart Automated Task Configuration



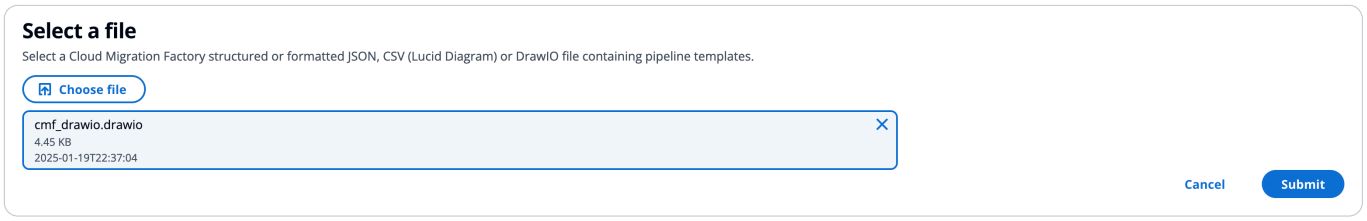
4. Set template name
   a. Rename the diagram tab to your desired template name
5. Saving & Exporting
   a. File → Export → CSV of Shape Data
6. Uploading to CMF
   a. Log into CMF portal
   b. Navigate to "Pipeline Templates" in the left navigation bar
   c. Click on "Actions" and select "Import"

Pipeline Templates Action→Import



   d. Choose your saved lucid file
   e. Click "Submit" to complete the import

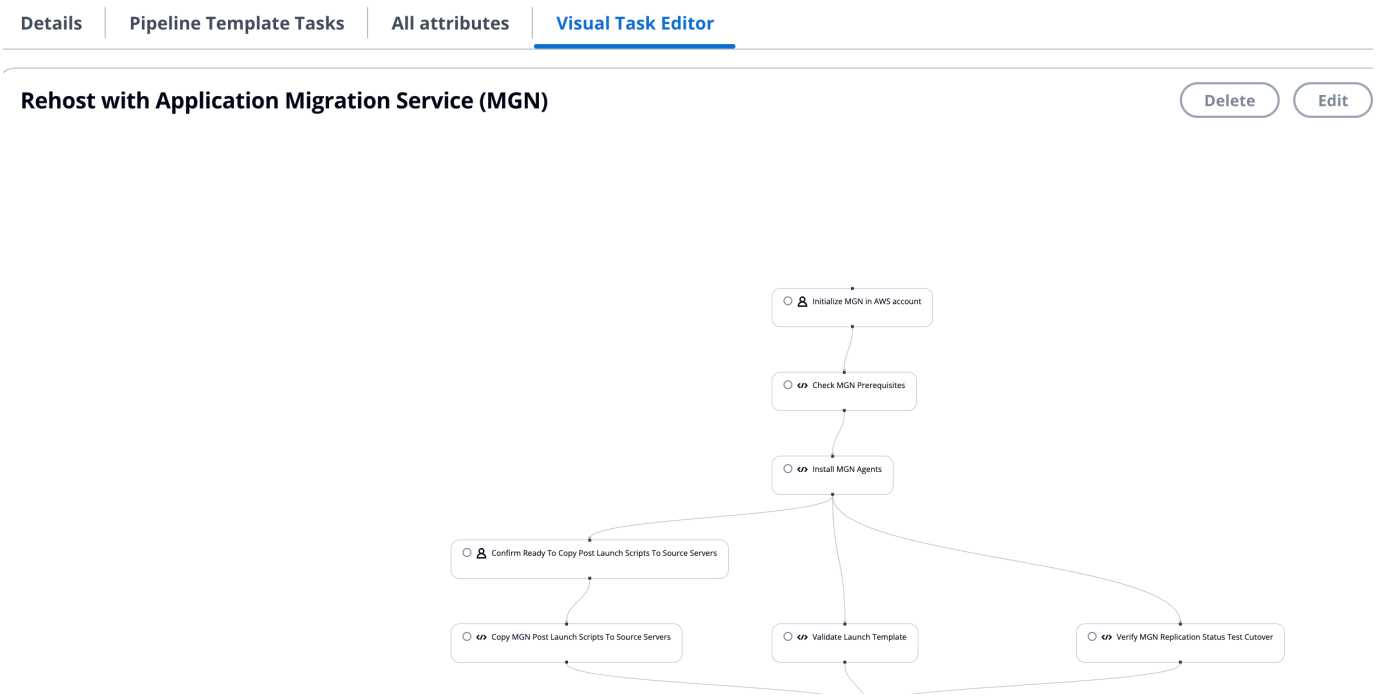
Template Import Submit



After Lucid import is complete

1. A new template will be created under Pipeline Templates
2. To see how your diagram attributes are converted in CMF:
   - Locate your newly created template in the Pipeline Templates list
   - Click on the template to open it
   - You'll see a visual representation of your workflow under Visual task Editor

Pipeline Template Visual Task Editor



   - Each shape from your diagram is now a task in CMF
   - Click on a task to view its details:
     - Task names correspond to the labels you gave shapes
     - For automated tasks, you'll see the assigned AutomationID under Scripts dropdown.

Pipeline Template Task Edit

Edit pipeline Template Task

Details

Template Task Name

MGN Prerequisites

Script

0-Check MGN Prerequisites

Related details

Clear

Script Version

1

Task Successors

1 Task Successors selected

Manual Approval

Audit

Created by
serviceaccount@yourdomain.com

Created on
2025-04-25T21:06:09.618549+00:00

Last modified by
serviceaccount@yourdomain.com

Last updated on
2025-04-25T21:08:31.983969+00:00

Cancel Save

Pipeline templates management

The pipeline templates provide a way for users to define a list of tasks in a given order to automate migration and modernization activities. You can upload new templates or change existing templates using the pipeline templates management interface. When Cloud Migration Factory on AWS deploys, the solution loads system-managed default pipeline templates automatically.

A template task is the smallest executable unit in a template. There are three types of tasks:

- **Script package runs on the automation server** - This type of task is a script that runs on the automation server using an AWS Systems Manager agent. The script package is often used to connect to the source environment, such as installing an AWS MGN agent on the source server to initiate data replication.
- **Lambda function** - This type of task is a Lambda function that runs inside the solution's AWS account. For example, a Lambda function to connect to the AWS MGN API to initiate instance cutover activities. You can use this type of task to perform actions inside a Lambda function, such as connecting to a remote API, or using other AWS services.
- **Manual task** - This type of task is managed by the user, not executed by the system. For example, if a user needs to submit a request for change in their environment to change a firewall port or a task to get approval. The user would complete the task outside of the solution and change the status to **complete** to continue the pipeline execution.

Add a new pipeline template

This section provides instructions for adding a new pipeline template.

1. Select **Automation**, then select **Pipeline templates**.
2. Select **Add**.
3. Enter the **Pipeline template description** and **Pipeline template name**.
4. Choose **Save** to create a new template.

Duplicate an existing template

This section provides instructions for duplicating a pipeline template from an existing template and making changes to the tasks based on your requirements. By default, the solution loads system templates, which can't be deleted.

1. Select **Automation**, then select **Pipeline templates**.
2. Select the template that you want to duplicate from the pipeline template table.
3. Select **Actions**, then select **Duplicate**.
4. Update the **Pipeline Template Description** and **Pipeline Template Name**.
5. Choose **Save** to create a template.

Delete a pipeline template

This section provides instructions for deleting a user managed template. You can't delete a system default template.

1. Select **Automation**, then select **Pipeline templates**.
2. Select the template that you want to delete from the pipeline template table.
3. Choose **Delete**.

Export a pipeline template

This section provides instructions for exporting one or more templates to JSON format.

1. Select **Automation**, then select **Pipeline templates**.
2. Select the template that you want to export.
3. Select **Actions**, then select **Export**.

Import a pipeline template

This section provides instructions for importing a template from a JSON format. You can download an existing template, make changes, and import it to the pipeline templates as a new template.

1. Select **Automation**, then select **Pipeline templates**.
2. Select **Actions**, then select **Import**.
3. On the **Import template** page, select **Choose File** to choose the new template in JSON format. The file name for the JSON template appears on the page.
4. Choose **Next**.
5. The **Step-2 Upload data** page appears. Review the template content.

6. Choose **Submit** to import the template.
7. After a few seconds, a **Pipeline templates imported successfully** message appears.
8. Select the newly imported template, then select the **Pipeline Templates tasks** tab.
9. Verify the task list for the template to ensure that all the tasks are imported correctly from the template.

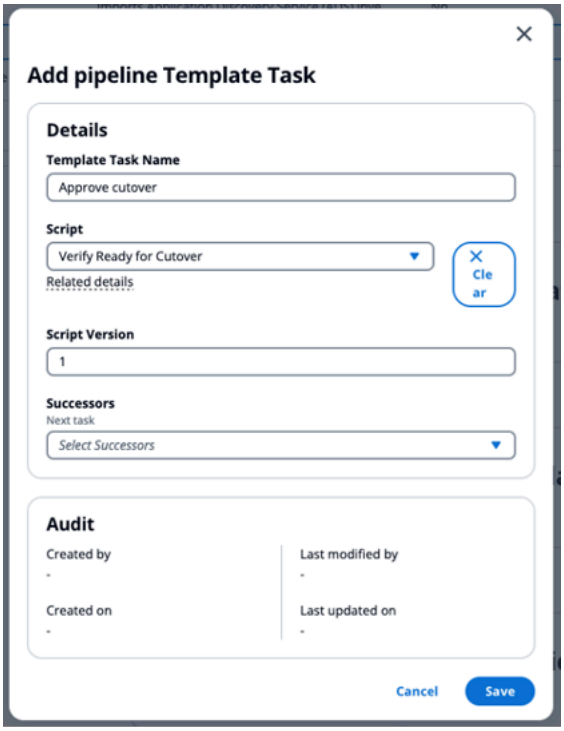
Add a new pipeline template task

This section provides instructions for adding a new pipeline template task.

1. Select **Automation**, then **Pipeline templates**.
2. Select one of the templates on the list, then select the **Visual Task Editor** tab.
3. Select **Add** to add a new task.
4. Enter a template task name. Select the script for this task and successors to this task.
5. Choose **Save**.

The following image shows an example of adding a pipeline template task.

Add pipeline task screen with Details and Audit menus.



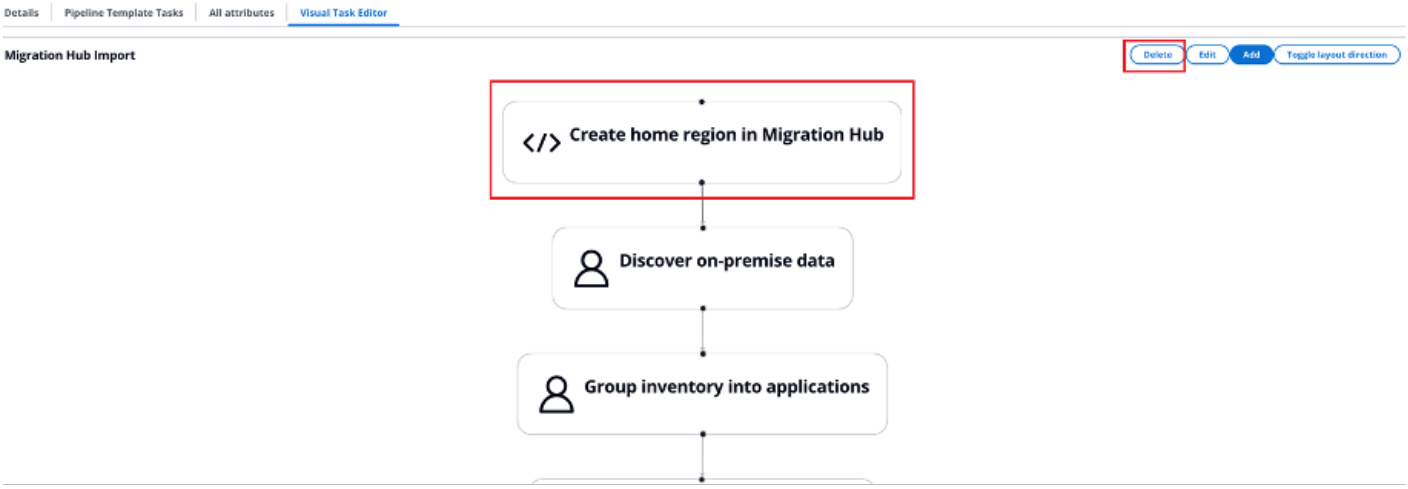
Delete a pipeline template task

This section provides instructions for deleting a pipeline template.

1. Select **Automation**, then **Pipeline templates**.
2. Select one of the templates on the list, then select the **Visual Task Editor** tab.
3. From the task list map, select the task that you want to delete.
4. Choose **Delete**.

The following image shows an example of deleting a pipeline template task.

Add pipeline task screen with Delete button.

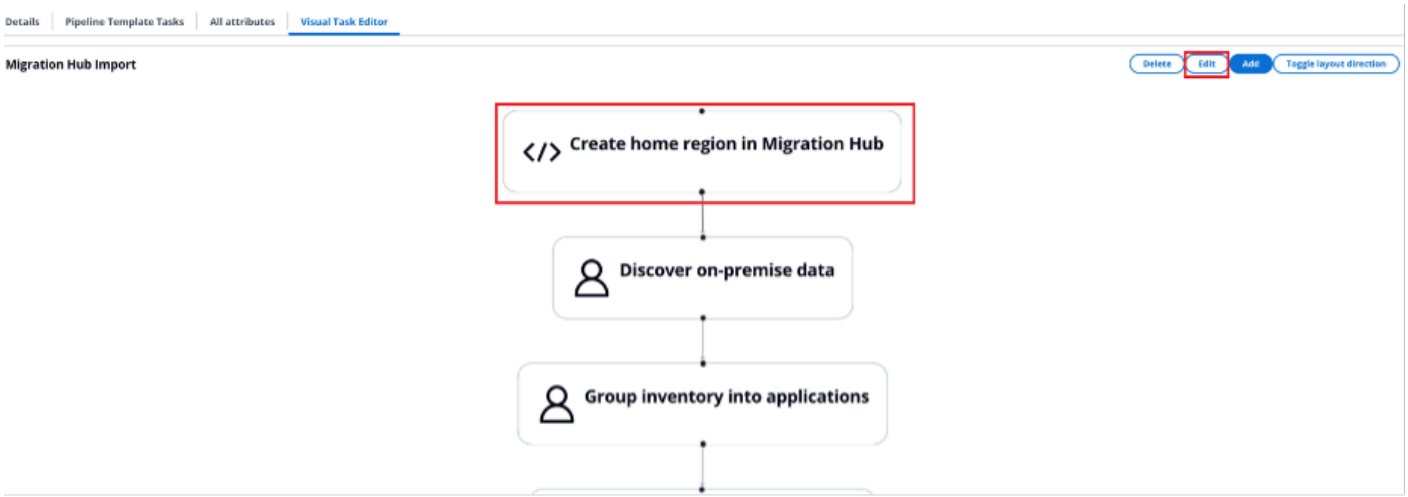


Editing a pipeline template

This section provides instructions for editing a pipeline template.

1. Select **Automation**, then **Pipeline templates**.
2. Select one of the templates on the list, then select the **Visual Task Editor** tab.
3. From the task list map, select the task that you want to edit.
4. Choose **Edit**.

Add pipeline task screen with Delete button.



5. On the task page, change the details of the task.
6. Choose **Save**.

Schema management

The Cloud Migration Factory on AWS solution provides a fully extensible metadata repository, allowing data for automation, auditing and status tracking to be stored in a single tool. The repository provides a default set of entities (Waves, Applications, Servers, and Databases) and attributes at deployment time to get you started with capturing and using the most frequently used data, and from here you can customize the schema as required.

Only Cognito admin group users have permissions to manage the schema. To make a user a member of the admin or other groups, refer to User management.

Go to **Administration**, and select **Attributes** for the default entity tabs. The following tabs are available to support management of the entity.

Attributes - Allows for adding, editing and deleting attributes.

Info Panel - Allows for editing of the Info panel help content, this is shown on the right of the entities' screen in the Migration Management section.

Schema Settings - Currently this tab only provides the ability to change the friendly name of the entity, this is the name that is shown on the user interface. If not defined, then the user interface uses the programmatic name of the entity.

Adding/editing an attribute

Attributes can be amended dynamically through the **Attributes** administration section of the Cloud Migration Factory on AWS solution. When attributes are added, edited or deleted the updates will be applied in real-time for the administrator making the change. Any other user that is currently logged into the same instance will have their session updated automatically within a minute of the changes being saved by the administrator.

Some attributes are defined as system attributes, which means that the attribute is key to the core functionality of Cloud Migration Factory on AWS and so only some properties are available for administrators to amend. Any attribute that is a system attribute will be shown with a warning on the top of the **Amend attribute** screen.

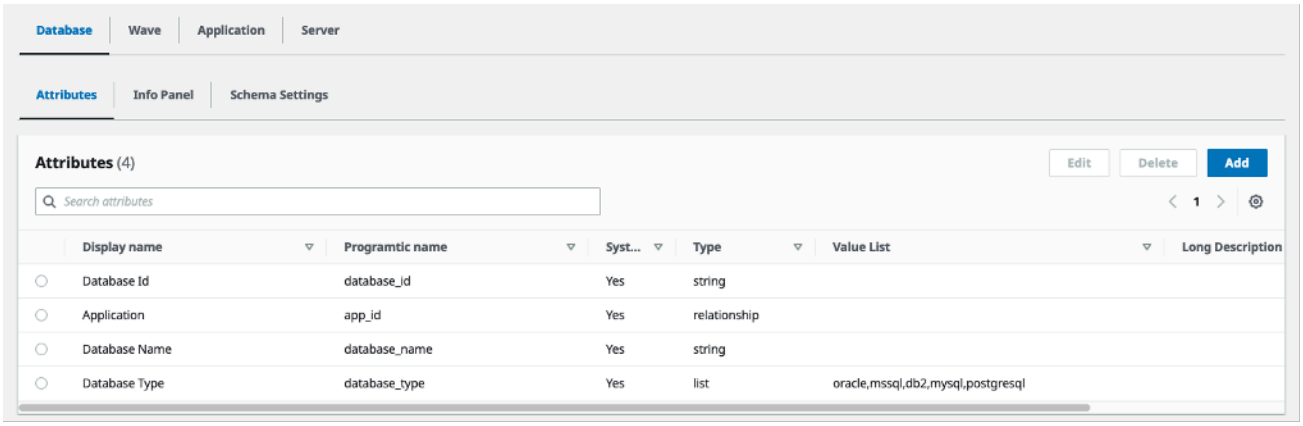
For system defined attributes only the following can be edited:

- Info Panel
- Advanced Options
  - Attribute Grouping & Positioning
  - Input Validation

All other properties of the system defined attribute are read-only.

Adding an attribute:

Attribute management



You can add new attributes by choosing the **Add** button on the attributes tab of the entity you wish to add the attribute to. In the example above, choosing **Add** will add a new attribute to the database entity.

On the **Amend attribute** dialog, you must to provide the following required properties:

Programmatic name - This is the key that will be used to store data for the attribute against items in the DynamoDB table. It is also referenced when using the Migration Factory APIs, and in automation scripts.

Display name - This is the label that will be displayed on the web interface against the data entry field.

Type - This drop-down selection defines the type of data that the user will be allowed to store against the attribute. The following options are available:

Type	Usage
String	Users can enter any single line of text carriage returns are not permitted.
Multivalue String	Similar to a **String** the only difference being that the user can enter multiple values on separate lines within the field, these are then stored as an array/list.
Password	Provides the user with a way to securely enter data that should not be displayed on the screen by default. **Note** Data is not stored encrypted when using this attribute type, and is shown in clear text when viewed in API payloads, thus should not be used to store sensitive data. Any passwords or secrets should be stored in the Migration Factory Credential Manager (covered in this document) which utilizes AWS Secrets Manager to

Type	Usage
	securely store and provide access to credentials.
Date	Provides a field with a date picker for the user to select a date, or they can manually enter the date required.
Checkbox	Provides a standard checkbox, when checked the key value will store '`true' if not checked then it will be '`false' or the key will not exist in the record.
TextArea	Unlike the **String** type **TextAreas** provide the ability to store multi line text, it supports basic text characters only.
Tag	Allows users to store a list of key/value pairs.
List	Provides the user a list of predefined options to select from, these options are defined in the schema attribute definition in the Value List property of the attribute.

Type	Usage
Relationship	This attribute type provides the ability to store relationships between any two entities or records. When defining a relationship attribute you select the entity that the relationship will be to, and then the key value used to relate the items and select the attribute from the related item that you wish to display to the user. The user is presented with a drop-down list based on the entity and display values available for the relationship. Under each relationship field the user has a quick link to show the summary of the related item.
JSON	Provides a JSON editor field where JSON data can be stored and edited. This could be used for storing script input/output parameters or other data needed for automation of tasks, or any other use.

When adding a new attribute, you must grant users access to the new attribute through a policy. See the Permission management section for details on how to grant attribute access.

Info panel

Provides the facility to specify contextual help and guidance for the attribute's usage. When specified, the attribute's label on the UI will have an **Info** link displayed to the right. Clicking this link provides the user with the **Help content** and **Help links** specified in this section to the right of the screen.

The Info panel section provides two views of the data, the **Edit** view where you can define the content, and the **Preview** view to provide a quick preview of what the user will see when updates to the attribute are saved.

The **Help title** supports only plain text values. The **Help content** supports a subset of html tags that allow text formatting. For example, adding start and end tags around the text will make the enclosed text bold (i.e. Network Interface ID would result in **Network Interface ID**). The supported tags are as follows:

Tag	Usage	UI Example
	Defines a paragraph.	My first paragraph My second paragraph
<a>	Defines a hyperlink.	Visit AWS!
<h3>, <h4> and <h5>	Defines headings h3 to h5	My heading 3
	Defines a section of text, allowing additional formatting to be applied, such as text color, size, font.	blue
	Defines a block of the document, allowing additional formatting to be applied, such as text color, size, font.	 This is a blue heading This is some blue text in a div.
+	Defines an unordered bulleted list.	 - Rehost - Replatform - Retire

Tag	Usage	UI Example
,	Defines an ordered/numbered list.	 - Rehost - Replatform - Retire
<code>	Defines a block or section of text containing code.	<code>background-color</code>

<pre>	Defines a block of preformatted text, all line breaks, tabs, and spaces are output.	<pre>
		My preformatted text.
		This is displayed in a fixed width font and will display as typed <<these spaces will be shown.
		</pre>

<dl>, <dt> and <dd>	Defines a description list.	<dl> <dt>Rehost</dt> <dd>Lift and shift migration </dd> <dt>Retire</dt> <dd>Decommission the instance or service </dd> </dl>

Tag	Usage	UI Example
<hr>	Defines a horizontal rule across the page to show a switch in topic or section.	<hr>
 	Defines a line break in text. These are supported but not required as any carriage returns in the editor will be replaced with when saved.	
and	Defined the enclosed text in *Italic* or alternative localized format.	This is in Italic or This is also Italic
and	Defines the enclosed text in **bold** font.	I'm in bold or This is different

Another option available to provide help is links to external content and guidance. To add an external link to the attribute's contextual help click **Add new URL** and provide a **Label** and URL. You can add multiple links to the same attribute type as required.

Advanced options

Attribute grouping and positioning

This section provides the administrator with the ability to set where on the Add/Edit UI the attribute will be positioned and also allows for grouping of attributes providing the user with a simple way to locate related attributes.

UI Group is a text value that defines the name of the group that the attribute should be shown in, all attributes with the same UI Group value will be placed in the same group, any attribute with no UI Group specified will be placed in the default group at the top of the form entitled **Details**. When UI Group is specified the user interface will display the text shown here as the title of the group.

The second property in this section is **Order in group**, this can be set to any positive or negative number, and when specified the attributes will be listed based on a sort of lowest to highest based on this value. Any attributes that do not have an **Order in group** specified will be lower priority and sorted alphabetically.

Input validation

This section allows the administrator to define validation criteria that ensures that the user has entered valid data before they are able to save an item. The validation uses a regular expression or regex string which is a series of characters that specify a search pattern for a text value. For example, the pattern **^(subnet-([a-z0-9]{17})**)$* will search for the text **subnet-** followed by any combination of the characters a to z (lowercase) and digits 0 to 9 with an exact number of characters of **17**, if it finds anything else it will return false indicating that the validation has failed. Within this guide we cannot cover all the possible combinations and patterns available, but there are many resources on the internet that can provide help on creating the prefect on for your use case. Here are some common examples to get you started:

Regex Pattern	Usage
^(?!\s*$).+	Ensures that the value is set.
^(subnet-([a-z0-9]{17})*)$	Checks that the value is a valid subnet ID. [Starts with the text **subnet-** followed by 17 characters made up of letters and numbers only]
^(ami-(([a-z0-9]{8,17})+)$)	Check that the value is a valid AMI ID. [Starts with the text **ami-** followed by between 8 and 17 characters made up of letters and numbers only]
^(sg-([a-z0-9]{17})*)$	Checks that the value is in a valid security group ID format. [Starts with the text **sg-** followed by 17 characters made up of letters and numbers only]

Regex Pattern	Usage
^(([a-zA-Z0-9]|[a-zA-Z0-9] **[a-zA-Z0-9])\.)** ([A-Za-z0-9]|[A-Za-z0-9][A-Za-z0-9\-]*[A-Za-z0-9])$	Ensures that server names are valid and only contain alphanumeric characters, hyphens and periods.
^([1-9]|[1-9][0-9]|[1-9][0-9][0-9]|[1-9][0-9][0-9][0-9]|[1][0-6][0-3][0-8][0-4])$	Ensures that a number is entered that is between 1 and 1634.
^(standard|io1|io2|gp2|gp3)$	Ensures that the string enter matches either standard, io1, io2, gp2 or gp3.

Once you have created your regex search pattern, you can specify the specific error message that will be shown to the user under the field, enter this into the **Validation help message** property.

Once these two properties are set then in the same screen you will see below a **Validation simulator**, here you can test that your search pattern is working as expected and that the error message is displayed correctly. Just type some test text into the **Test validation** field to verify the pattern is matched correctly.

Example data

The example data section provides the administrator with the ability to show the user an example of data format required for an attribute, this can be specified for the format of data required when provided in an intake form upload, through the user interface and/or through the API directly.

Example data shown in the **Intake form example data** property will be output in any intake template created where the attribute is included, when using the **Download, a template intake form** function, under **Migration Management > Import**.

User interface example data and API example data are stored in the attribute, but not currently exposed in the web interface. These can be used in integrations and scripts.

Permission management

The Cloud Migration Factory on AWS solution provides granular role-based access control to the data and automation functions available in the solution, underlying this is Amazon Cognito, providing the user directory and authentication engine.

The following table shows the various elements that make up the access control framework within the Cloud Migration Factory on AWS solution and where each element is managed from.

Access control element	Management interface	Description
User	Amazon Cognito and Cloud Migration Factory on AWS	Users are created, deleted, and updated in Amazon Cognito, where the users' profile can be established as well as multi-factor authentic ation (MFA) if required. Within the AWS CMF user interface, you can add and remove users from groups only.
Group	Cloud Migration Factory on AWS	You can create or delete groups from within the AWS CMF user interface.
Role	Cloud Migration Factory on AWS	A Role is mapped to one or many Groups, changing the groups a Role is assigned to is performed in the AWS CMF administration section. Any user that is a member of a group assigned to a role will be assigned all policies that are mapped to the role. One or many policies can be assigned to a role.
Policy	Cloud Migration Factory on AWS	A policy contains the detailed rights that are assigned to any user to which the policy applies (via group membershi p). A single policy can include data access rights for multiple

Access control element	Management interface	Description
		entities or a single entity, along with access rights to run automation jobs and other actions within the AWS CMF user interface. These policies also apply when a user is interacting with the AWS CMF APIs.

Policies

A policy provides the most granular permissions possible in Cloud Migration Factory on AWS, it holds the tasks level definition of what rights are provided to a user. Within a policy there are two main permission types that can be granted to a user group, **Metadata Permissions** and **Automation Action Permissions**. Metadata permissions allow an administrator to control the level of access a group has to individual schemas and their attributes, specifying rights to create, read, update and/or delete as required. Automation Action permissions grant users access to run specific automation actions, such as the AWS MGN integration action.

Metadata permissions

For each schema or entity within AWS CMF an administrator can define a policy that allows users access to specific attributes and also define the level of access they have to those attributes. On creation of a new policy, the default rights for all schemas are no access. The first thing that should be set is the level of access required for this policy at the item/record level. Below is a table describing the record level access permissions available.

Access level	Description
Create	When selected, a user where this policy applies will have the ability to Add new records/items of this type to the metadata store. When create is selected but no other rights are allowed the user will have the ability to create records and set only required

Access level	Description
	attributes to a value regardless of the selected attributes.
Read	**Not yet implemented** When selected, a user will have read rights to all records/items for this entity type, when not selected they will not see the data items in the UI or the API.
Update	When selected, a user where this policy applies will have the ability to update records/items of this type to the metadata store, but only for the attributes specified in the Attribute level access list. When update is selected at least one Attribute has to be selected or an error will be show on saving.
Delete	When selected, a user where this policy applies will have the ability to delete records/items of this type from the metadata store.

Roles

Roles allow one or more policies to be assigned to one or more groups. The combination of all policies assigned to a role provides access permissions. Roles can be created based on job roles or functions within the project or organization.

Developer guide

Source code

You can visit our GitHub repository to download the templates and scripts for this solution, and to share your customizations with others. If you require an earlier version of the CloudFormation template or have a technical issue to report, you can do so from the GitHub issues page. Report technical issues with the solution on the Issues page of the GitHub repository.

Supplemental topics

List of automated migration activities using Migration Factory web console

The Cloud Migration Factory on AWS solution deploys automated migration activities that you can leverage for your migration projects. You can follow the migration activities listed below and customize them based on your business needs.

Before starting any of the activities, make sure you read User Guide - Run Automation from console to understand how this works. Also, you must Build an Automation server and create Windows and Linux users to run automation from the console.

Use the following procedures in the same order to conduct a complete test run of the solution using the sample automation script and activities.

Check prerequisites

Connect with the in-scope source servers to verify the necessary prerequisites such as TCP 1500, TCP 443, root volume free space, .Net framework version, and other parameters. These prerequisites are required for replication.

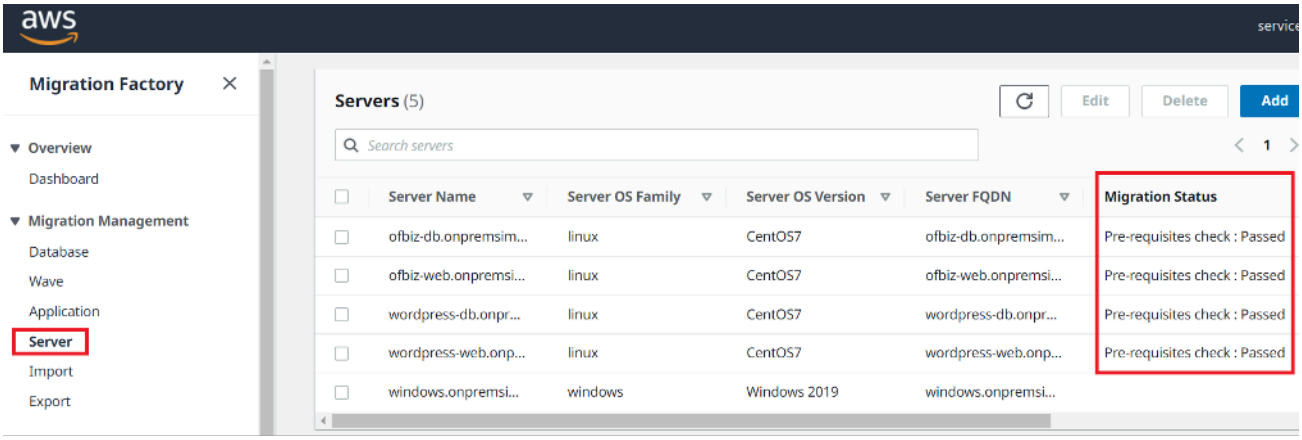
Before you can conduct the prerequisites check, you must install the first manually on one source server, so this will create a replication server in EC2. We will connect to this server for port 1500 testing. After installation, AWS Application Migration Service (AWS MGN) creates the replication server in Amazon Elastic Compute Cloud (Amazon EC2). You must verify the TCP port 1500 from the source server to the replication server in this activity. For information about installing the AWS MGN agent on your source servers, refer to Installation instructions in the *AWS Application Migration Service User Guide*.

Use the following procedure while signed in to the migration factory web console.

1. On the Migration Factory console, select **Jobs** on the left-hand side menu, and select **Actions**, and then **Run Automation** on the right-hand side.
2. Enter **Job Name**, select **0-Check MGN Prerequisites** script and your automation server to run the script. If automation server does not exist, make sure you complete Build a migration automation server.

3. Select **Linux Secrets** and/or **Windows Secrets** depends on what OSs you have for this wave. Enter MGN replication server IP, choose the wave you want to run automation on and choose **Submit Automation Job.**
4. You will be redirected to the **Jobs** list page. The job status should be RUNNING. Choose **Refresh** to see the status. It should change to Complete after a few minutes.
5. The script will also update the solution's **migration status** in the Migration Factory web interface as shown in the following screenshot of an example project.

Migration status



Install the replication agents

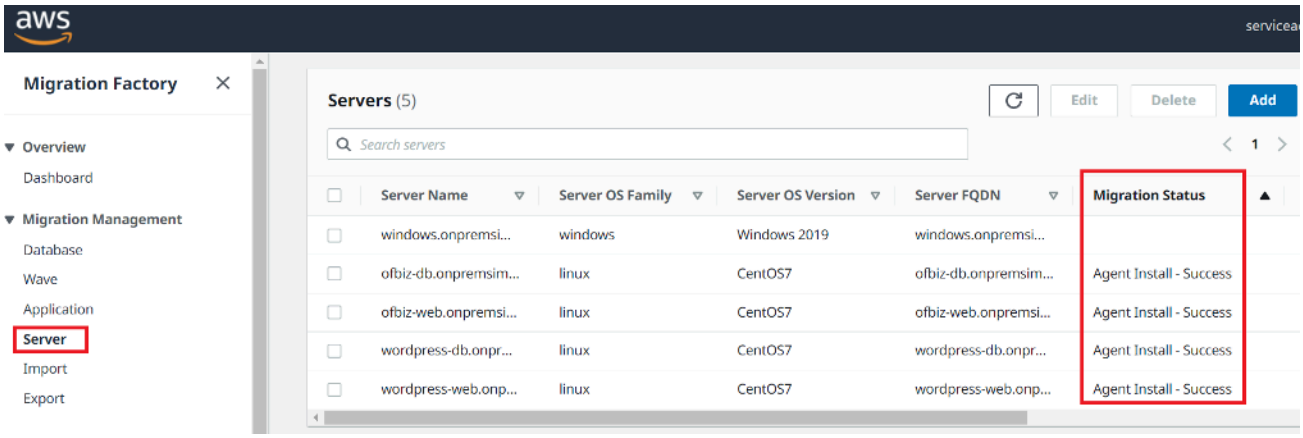
> **Note**
>
> Before you install the agent, make sure AWS MGN is initialized in each target account and region.

Use the following procedure to automatically install the Replication agents in the in-scope source servers.

1. On the Migration Factory console, select **Jobs** on the left-hand side menu, and select **Actions**, and then **Run Automation** on the right-hand side.
2. Enter **Job Name**, select **1-Install MGN Agents** script and your automation server to run the script. If automation server does not exist, make sure you complete Build a migration automation server.

3. Select **Linux Secrets** and/or **Windows Secrets** depends on what OSs you have for this wave. Choose the wave you want to run automation, and choose **Submit Automation Job**.
4. You will be redirected to the **Jobs** list page. The job status should be running. Choose **Refresh** to see the status. It should change to **Complete** after a few minutes.
5. The script also provides the migration status in the Migration Factory web interface as shown in the following example screenshot.

Migration status



Push the post-launch scripts

AWS Application Migration Service (MGN) supports post-launch scripts to help you automate OS-level activities, such as installing/uninstalling the software after launching target instances. This activity pushes the post-launch scripts to Windows and/or Linux machines, depending on the servers identified for migration.

> **Note**
>
> Before you push the post-launch scripts, you must copy the files to a folder on the migration automation server.

Use the following procedure to push the post-launch scripts to Windows machines.

1. On the Migration Factory console, select **Jobs** on the left-hand side menu, and select **Actions**, and then **Run Automation** on the right-hand side.

2. Enter Job Name, select **1-Copy Post Launch Scripts** script and your automation server to run the script. If automation server does not exist, make sure you complete Build a migration automation server.
3. Select **Linux Secrets** and/or **Windows Secrets** depends on what OSs you have for this wave. Provide a **Linux source location** and/or **Windows source location**.
4. Choose the wave you want to run automaton and choose **Submit Automation Job**.
5. You will be redirected to the **Jobs** list page, the job status should be running, and you can choose **Refresh** to see the status. It should change to **Complete** after a few minutes.

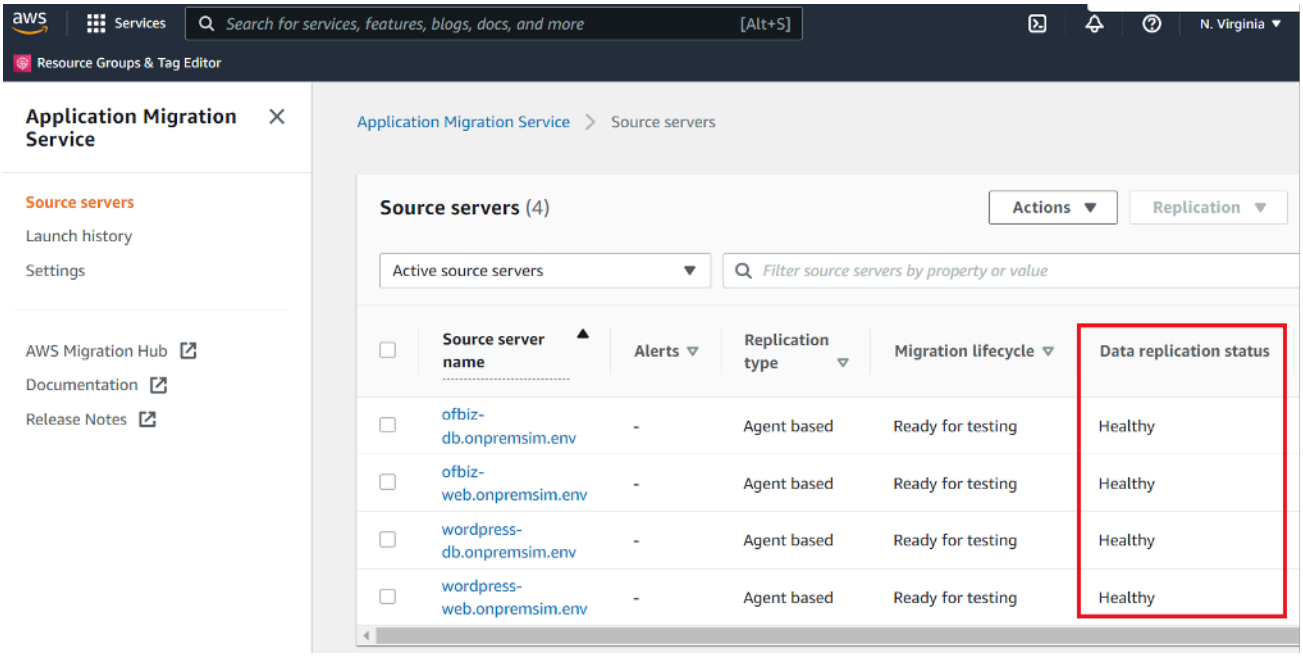
Verify the replication status

This activity verifies the replication status for the in-scope source servers automatically. The script repeats every five minutes until the status of all source servers in the given wave changes to a *Healthy* status.

Use the following procedure to verify the replication status.

1. On the Migration Factory console, select **Jobs** on the left-hand side menu, and select **Actions**, and then **Run Automation** on the right-hand side.
2. Enter Job Name, select **2-Verify Replication Status** script and your automation server to run the script. If automation server does not exist, make sure you complete Build a migration automation server.
3. Choose the wave you want to run automaton and choose **Submit Automation Job**.
4. You will be redirected to the **Jobs** list page, the job status should be running, and you can click **refresh** button to see the status. It should change to **Complete** after a few minutes.

Data replication status



Note

Replication can take a while. You might not see the status update from the factory console for a few minutes. Optionally, you can also check the status in MGN service.

Validate launch template

This activity validates the server metadata in the migration factory and makes sure it works with EC2 template and no typos. It will validate both test and cutover metadata.

Use the following procedure to validate EC2 launch template.

1. Navigate to the Migration Factory console, and select **Wave** in the menu pane.
2. Select the target wave, and choose **Actions**. Select **Rehost**, and then select **MGN**.
3. Select **Validate Launch Template *for the *Action**, then select All* applications.*
4. Choose **Submit** to initiate the validation.

After some time, the validation will return a successful result.

Note

If validation is not successful, you will receive a specific error message:

The errors may be due to invalid data in the server attribute such as an invalid **subnet_IDs**, **securitygroup_IDs**, or **instanceType**.
You can switch to the Pipeline page from the Migration Factory web interface and select the problematic server to fix the errors.

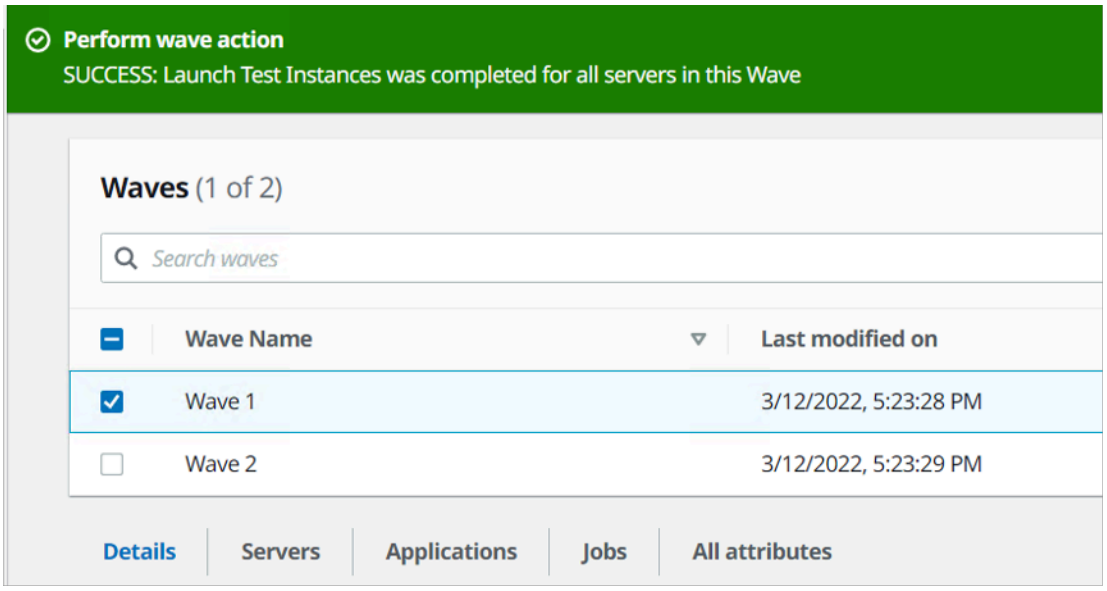
Launch instances for testing

This activity launches all target machines for a given wave in AWS Application Migration Service (MGN) in test mode.

Use the following procedure to launch test instances.

1. On the Migration Factory console, select **Wave** on the navigation menu.
2. Select target wave, and choose **Actions**. Select **Rehost**, and then select **MGN**.
3. Select **Launch Test Instances** Action, select **All applications.**
4. Choose **Submit** to launch test instances.
5. After some time, the validation will return a successful result.

Wave action success



Note

This action will also update the migration status for the server launched.

Verify the target instance status

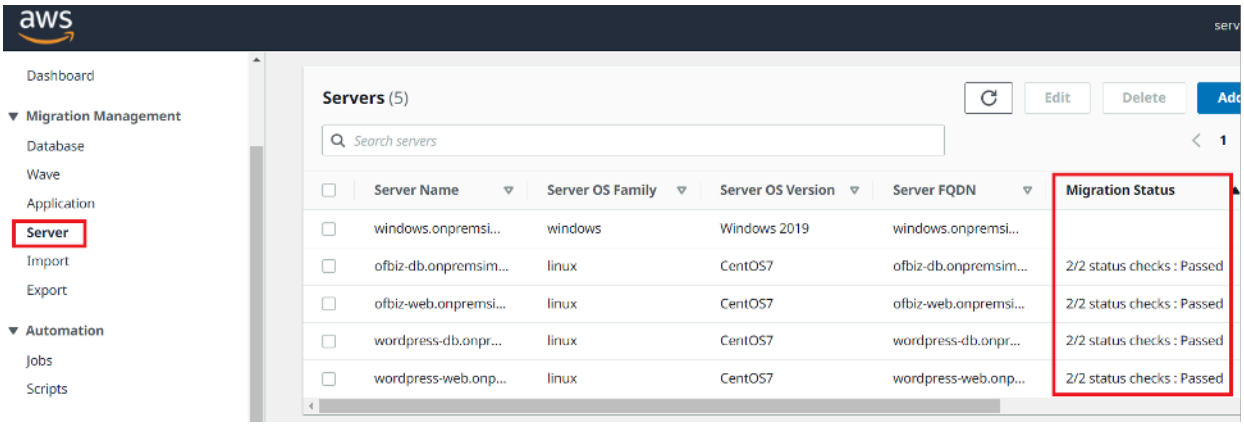
This activity verifies the status of the target instance by checking the boot up process for all in-scope source servers in the same wave. It may take up to 30 minutes for the target instances to boot up. You can check the status manually by logging into the Amazon EC2 console, searching for the source server name, and checking the status. You will receive a health check message stating *2/2 checks passed*, which indicates that the instance is healthy from an infrastructure perspective.

However, for a large-scale migration, it's time consuming to check the status of each instance, so you can run this automated script to verify the *2/2 checks passed* status for all source servers in a given wave.

Use the following procedure to verify the status of the target instance.

1. Navigate to the Migration Factory console, and select **Jobs** on the left-hand side menu.
2. Select **Actions**, then **Run Automation** on the right-hand side.
3. Enter **Job Name**, select **3-Verify Instance Status** script and your automation server to run the script. If automation server does not exist, ensure you complete Build a migration automation server.
4. Choose the wave you want to run automaton, and choose **Submit Automation Job**.
5. You will be redirected to the **Jobs** list page, the job status should be running, and you can choose **Refresh** to see the status. It should change to **Complete** after a few minutes.

AWS Migration Management dashboard showing server list with migration status for 5 servers.



Note

Instance boot up can take a while and you might not see the status update from the factory console for a few minutes. Migration factory also receives a status update from the script. Refresh the screen if necessary.

Note

If your target instances fail the 2/2 health checks the first time, it may be due to the boot up process taking longer to complete. We recommend running the health checks a second time about an hour after the first health check. This ensures that the boot up process completes. If the health checks fail this second time, go to the AWS support center to log a support case.

Mark as ready for cutover

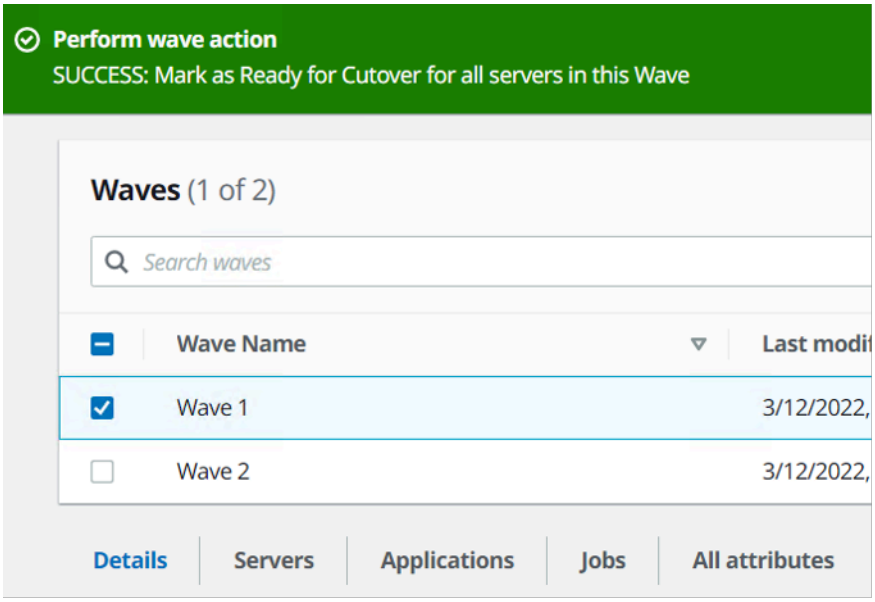
Once testing is finished, this activity changes the status of the source server to mark as ready for cutover, so that user is able to launch a cutover instance.

Use the following procedure to validate EC2 launch template.

1. On the Migration Factory console, and select **Wave** on the left-hand side.
2. Select target wave, and click **Actions** button. Select **Rehost**, and then select **MGN**.
3. Select **Mark as Ready for Cutover** Action, select **All applications.**
4. Choose **Submit** to launch live instances.

After some time, the validation will return a successful result.

Wave action ready for cutover



Shut down the in-scope source servers

This activity shuts down the in-scope source servers involved with the migration. After you verify the source servers' replication status, you are ready to shut down the source servers to stop transactions from the client applications to the servers. You can shut down the source servers in the cutover window. Shutting down the source servers manually could take five minutes per server, and, for large waves, it could take a few hours in total. Instead, you can run this automation script to shut down all your servers in the given wave.

Use the following procedure to shut down all the source servers involved with the migration.

1. On the Migration Factory console, select **Jobs** on the left-hand side menu, and select **Actions**, and then **Run Automation** on the right-hand side.
2. Enter Job Name, select **3-Shutdown All Servers** script and your automation server to run the script. If automation server does not exist, make sure you complete Build a migration automation server.
3. Select **Linux Secrets** and/or **Windows Secrets** depends on what OSs you have for this wave.
4. Choose the wave you want to run automaton and choose **Submit Automation Job**.
5. You will be redirected to the **Jobs** list page, the job status should be running, and you can click **refresh** button to see the status. It should change to **Complete** after a few minutes.

Launch instances for Cutover

This activity launches all target machines for a given wave in AWS Application Migration Service (MGN) in Cutover mode.

Use the following procedure to launch test instances.

1. On the Migration Factory console, and select **Wave** on the left-hand side.
2. Select target wave, and choose **Actions**. Select **Rehost**, and then select **MGN**.
3. Select **Launch Cutover Instances** Action, select **All applications.**
4. Choose **Submit** to launch test instances.

After some time, the validation will return a successful result.

> **Note**
>
> This action will also update the migration status for the server launched.

List of automated migration activities using command prompt

> **Note**
>
> We recommend running automation from the Cloud Migration Factory on AWS console. You can use the following steps to run automation scripts. Make sure you download the automation scripts from the GitHub repo and configure the automation server with steps in Run Automations from Command prompt, and following the instructions to configure permissions in Configure AWS permissions for the migration automation server.

The Cloud Migration Factory on AWS solution deploys automated migration activities that you can leverage for your migration projects. You can follow the migration activities listed below and customize them based on your business needs.

Before starting any of the activities, verify that you are logged on to your migration automation server as a domain user with local administrator permission on the in-scope source servers.

Important

You must log in as an administrator user to complete the activities listed in this section.

Use the following procedures in the same order to conduct a complete test run of the solution using the sample automation script and activities.

Check prerequisites

Connect with the in-scope source servers to verify the necessary prerequisites such as TCP 1500, TCP 443, root volume free space, .Net framework version, and other parameters. These prerequisites are required for replication.

Before you can conduct the prerequisite check, you must install the first agent manually on one source server, so this will create a replication server in EC2, we will be connecting to this server for port 1500 testing. After installation, AWS Application Migration Service (AWS MGN) creates the replication server in Amazon Elastic Compute Cloud (Amazon EC2). You will need to verify the TCP port 1500 from the source server to the replication server in this activity. For information about installing the AWS MGN agent on your source servers, refer to Installation instructions in the *Application Migration Service User Guide*.

Use the following procedure while signed in to the migration automation server to check for the prerequisites.

1. Signed in as an administrator, open a command prompt (`CMD.exe`).
2. Navigate to the `c:\migrations\scripts\script_mgn_0-Prerequisites-checks` folder and run the following Python command:

```
python 0-Prerequisites-checks.py --Waveid <wave-id> --ReplicationServerIP <rep-server-ip>
```

Replace *<wave-id>* and *<rep-server-ip>* with the appropriate values:

- The `Waveid` is a unique integer value to identify your migration waves.
- The `ReplicationServerIP` value identifies the replication server IP address. Change this value to the Amazon EC2 IP address. To locate this address, sign in to the AWS Management Console,

search for **Replication**, select one of the replication servers, and copy the private IP address. If the replication occurs over the public internet, use the public IP address instead.

1. The script automatically retrieves a server list for the specified wave.

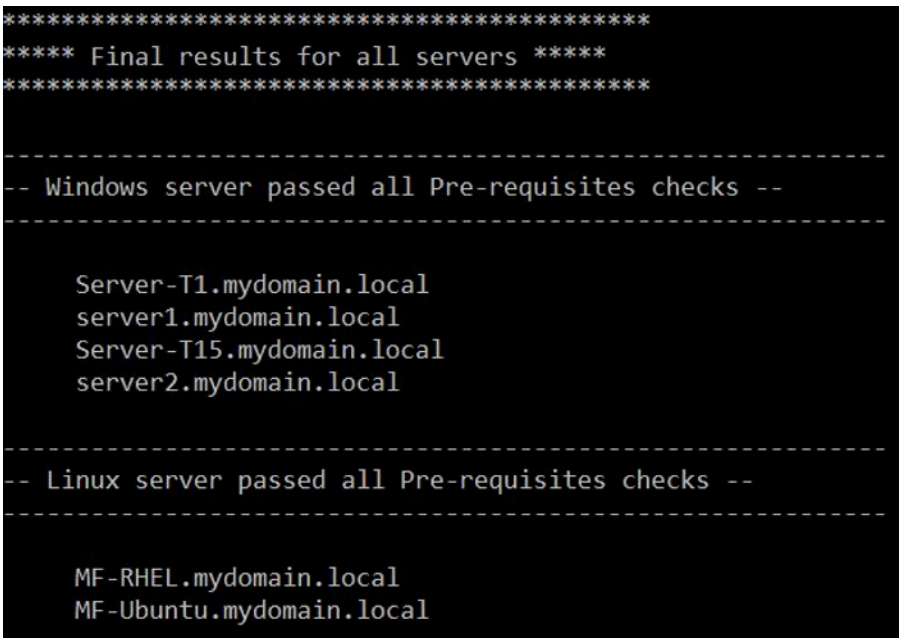
The script then checks the prerequisites for Windows servers and returns a state of either `pass` or `fail` for each check.

> **Note**
>
> You might get a security warning like the following when the PowerShell script is not trusted. Run the following command in PowerShell to resolve the issue:
>
> ```
> Unblock-File C:\migrations\scripts\script_mgn_0-Prerequisites-checks\0-Prerequisites-Windows.ps1
> ```

Next, the script checks the Linux servers.

Once the checks are completed, the script will return a final result for each server.

Script final result



If the server failed one or more prerequisites checks, you can identify the faulty server by either reviewing the detailed error message provided at the completion of the check or by scrolling through the log details.

The script will also update the solution's **Migration Status** in the Migration Factory web interface as shown in the following screenshot of an example project.

Install the replication agents

> **Note**
>
> Before you install the agent, make sure AWS MGN is initialized in each target account.

Use the following procedure to automatically install the Replication agents in the in-scope source servers.

1. In the migration automation server, signed is as an administrator, open a command prompt (`CMD.exe`).
2. Navigate to the `c:\migrations\scripts\script_mgn_1-AgentInstall` folder and run the following Python command:

```
python 1-AgentInstall.py --Waveid <wave-id>
```

Replace <*wave-id*> with the appropriate Wave ID value to install the Replication agent on all servers in the identified wave. The script will install the agent on all source servers in the same wave one by one.

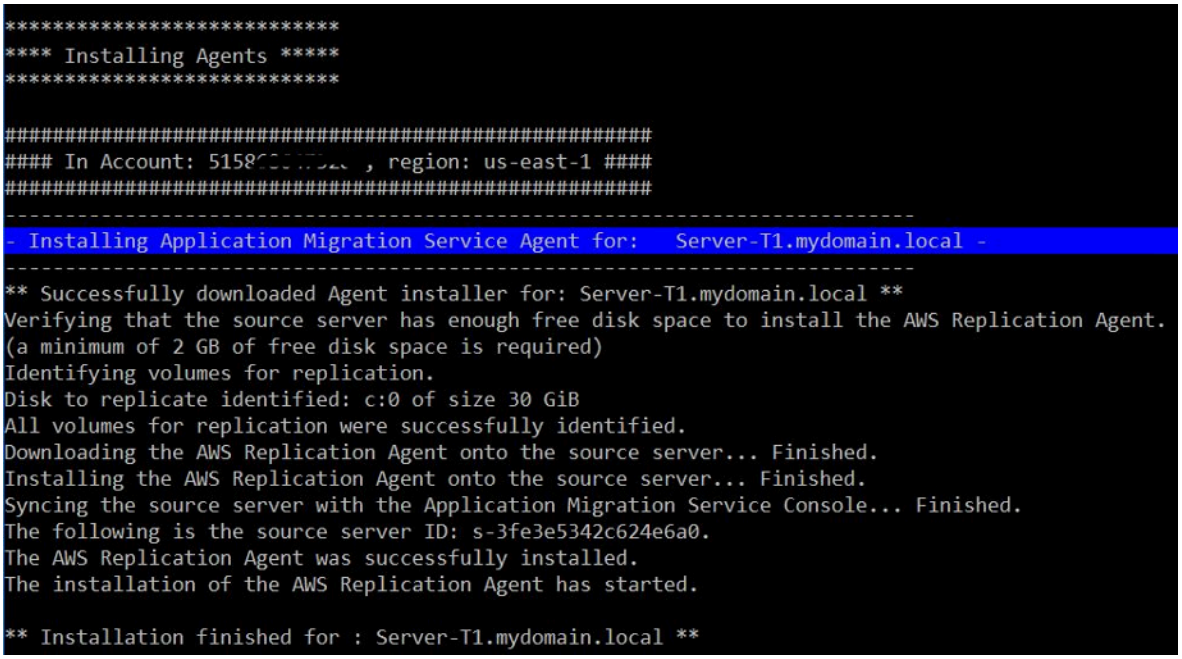
> **Note**
>
> To reinstall the agent, you can add `--force` argument.

1. The script generates a list identifying the source servers included for the specified wave. In addition, servers that are identified in multiple accounts and for different OS versions may also be provided.

If there are Linux machines included in this wave, you must enter your Linux sudo sign-in credentials to sign in to those source servers.

The installation starts on the Windows, then proceeds to the Linux for each AWS account.

Install replication agents



> **Note**
>
> You might get a security warning like the following when the PowerShell script is not trusted. Run the following command in PowerShell to resolve the issue:
>
> ```
> Unblock-File C:\migrations\scripts\script_mgn_1-AgentInstall\1-Install-Windows.ps1
> ```

Results are displayed after the script finishes installing the replication agents. Review the results for error messages to identify servers that failed to install the agents. You will need to manually install the agents on the failed servers. If manual installation does not succeed, go to the AWS support center and log a support case.

Agent install result

```
******************************
*Checking Agent install results*
******************************

-- SUCCESS: Agent installed on server: Server-T1.mydomain.local
-- SUCCESS: Agent installed on server: server1.mydomain.local
-- FAILED: Agent install failed on server: MF-RHEL.mydomain.local
-- SUCCESS: Agent installed on server: Server-T15.mydomain.local
-- SUCCESS: Agent installed on server: server2.mydomain.local
-- SUCCESS: Agent installed on server: MF-Ubuntu.mydomain.local
```

The script also provides the migration status in the Migration Factory web interface as shown in the following screenshot of an example project.

Push the post-launch scripts

AWS Application Migration Service supports post-launch scripts to help you automate OS-level activities such as the install/uninstall of software after launching target instances. This activity pushes the post-launch scripts to Windows and/or Linux machines, depending on the servers identified for migration.

Use the following procedure from the migration automation server to push the post-launch scripts to Windows machines.

1. Logged in as an administrator, open a command prompt (`CMD.exe`).
2. Navigate to the `c:\migrations\scripts\script_mgn_1-FileCopy` folder and run the following Python command:

```
python 1-FileCopy.py --Waveid <wave-id> --WindowsSource <file-path> --LinuxSource
 <file-path>
```

Replace *<wave-id>* with the appropriate Wave ID value and *<file-path>* with the full file path for Source, where the script is located. For example, `c:\migrations\scripts\script_mgn_1-FileCopy`. This command copies all files from the source folder to the destination folder.

> **Note**
>
> At least one of these two arguments must be provided: WindowsSource, LinuxSource. If you provide WindowsSource path, this script will only push files to Windows servers in

this wave, same as LinuxSource, which only pushes files to the Linux Servers in this wave. Provide both will push files to both Windows and Linux servers.

1. The script generates a list identifying the source servers included for the specified wave. In addition, servers that are identified in multiple accounts and for different OS versions may also be provided.

If there are Linux machines included in this wave, you must enter your Linux sudo sign-in credentials to sign in to those source servers.

1. The script copies the files to the destination folder. If the destination folder does not exist, the solution creates a directory and notifies you of this action.

Verify the replication status

This activity verifies the replication status for the in-scope source servers automatically. The script repeats every five minutes until the status of all source servers in the given wave changes to a *Healthy* status.

Use the following procedure from the migration automation server to verify the replication status.

1. Signed in as an administrator, open a command prompt (`CMD.exe`).
2. Navigate to the `\migrations\scripts\script_mgn_2-Verify-replication` folder and run the following Python command:

```
python 2-Verify-replication.py --Waveid <wave-id>
```

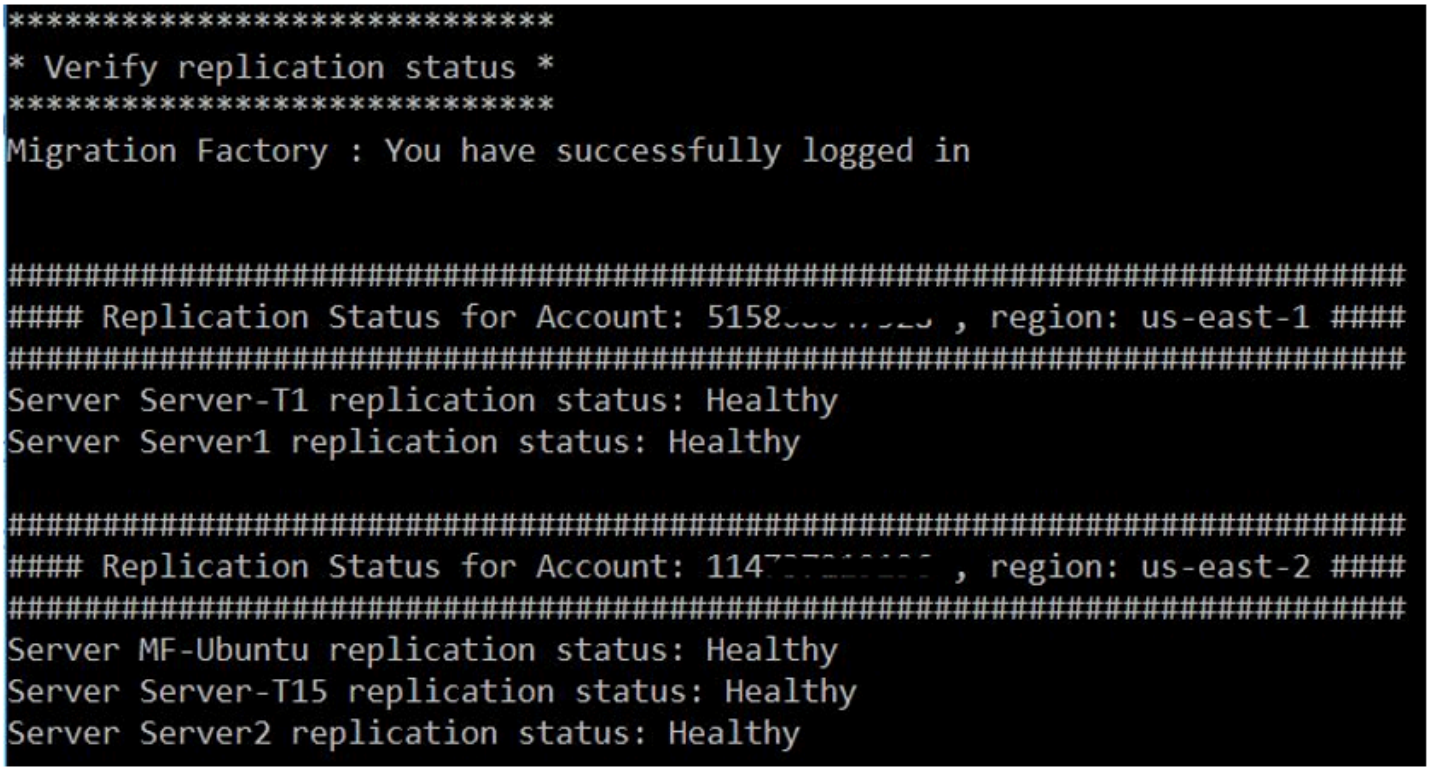
Replace *<wave-id>* with the appropriate Wave ID value to verify the replication status. The script verifies the replication details for the all servers in the specific wave and updates the **replication status** attribute for the source server identified in the solution.

1. The script generates a list identifying the servers included for the specified wave.

The expected status for the in-scope source servers that is ready to launch is **Healthy**. If you receive a different status for a server, then it is not ready for launch yet.

The following screenshot of an example wave shows that all servers in the current wave have finished replication and are ready for testing or cutover.

Agent install result



Optionally, you can verify status in the **Migration Factory** web interface.

Verify the target instance status

This activity verifies the status of the target instance by checking the boot up process for all in-scope source servers in the same wave. It may take up to 30 minutes for the target instances to boot up. You can check the status manually by logging into the Amazon EC2 console, searching for the source server name, and checking the status. You will receive a health check message stating *2/2 checks passed*, which indicates that the instance is healthy from an infrastructure perspective.

However, for a large-scale migration, it's time-consuming to check the status of each instance, so you can run this automated script to verify the *2/2 checks passed* status for all source servers in a given wave.

Use the following procedure from the migration automation server to verify the status of the target instance.

1. Signed in as an administrator, open a command prompt (`CMD.exe`).

2. Navigate to the `c:\migrations\scripts\script_mgn_3-Verify-instance-status` folder and run the following Python command:

```
python 3-Verify-instance-status.py --Waveid <wave-id>
```

Replace *<wave-id>* with the appropriate Wave ID value to verify instance status. This script verifies the instance boot up process for all source servers in this wave.

1. The script returns a listing of the server list and Instance IDs for the specified wave.
2. The script will then return a list of target instance IDs.

> **Note**
>
> If you get an error message that the target instance Id does not exist, the launch job might still be running. Wait a few minutes before continuing.

3. You will receive instance status checks that indicates whether your target instances passed the 2/2 health checks.

> **Note**
>
> If your target instances fail the 2/2 health checks the first time, it may be due to the boot up process taking longer to complete. We recommend running the health checks a second time about an hour after the first health check. This ensures that the boot up process completes. If the health checks fail this second time, go to the AWS support center to log a support case.

Shut down the in-scope source servers

This activity shuts down the in-scope source servers involved with the migration. After you verify the source servers' replication status, you are ready to shut down the source servers to stop transactions from the client applications to the servers. You can shut down the source servers in the cutover window. Shutting down the source servers manually could take five minutes per server, and, for large waves, it could take a few hours in total. Instead, you can run this automation script to shut down all your servers in the given wave.

Use the following procedure from the migration automation server to shut down all the source servers involved with the migration.

1. Signed in as an administrator, open a command prompt (`CMD.exe`).
2. Navigate to the `c:\migrations\scripts\script_mgn_3-Shutdown-all-servers` folder and run the following Python command:

```
Python 3-Shutdown-all-servers.py -Waveid <wave-id>
```

3. Replace *<wave-id>* with the appropriate Wave ID value to shut down the source servers.
4. The script returns a listing of the server list and Instance IDs for the specified wave.
5. The script first shuts down Windows servers in the specified wave. After the Windows servers are shut down, the script proceeds to the Linux environment and prompts for the login credentials. After successful login, the script shuts down the Linux servers.

Retrieve the target instance IP

This activity retrieves the target instance IP. If the DNS update is a manual process in your environment, you would need to get the new IP addresses for all the target instances. However, you can use the automation script to export the new IP addresses for all the instances in the given wave to a CSV file.

Use the following procedure from the migration automation server to retrieve the target instance Ips.

1. Signed in as an administrator, open a command prompt (`CMD.exe`).
2. Navigate to the `c:\migrations\scripts\script_mgn_4-Get-instance-IP` folder and run the following Python command:

```
Python 4-Get-instance-IP.py --Waveid <wave-id>
```

Replace *<wave-id>* with the appropriate Wave ID value to get the new IP addresses for the target instances.

1. The script returns a server list and the target instance ID information.
2. The script will then return the target server IP.

The script exports the server name and IP addresses information to a CSV file (*<wave-id>*-*<project-name>*-Ips.csv) and places it in the same directory as your migration script (`c:\migrations\scripts\script_mgn_4-Get-instance-IP`).

The CSV file provides **instance_name** and **instance_Ips** details. If the instance contains more than one NIC or IP, they will all be listed and separated by commas.

Verify the target server connections

This activity verifies the connections for the target server. After you update the DNS records, you can connect to the target instances with the host name. In this activity, you check to determine if you can log in to the operating system by using Remote Desktop Protocol (RDP) or through Secure Shell (SSH) access. You can manually log in to each server individually, but it is more efficient to test the server connection by using the automation script.

Use the following procedure from the migration automation server to verify the connections for the target server.

1. Logged in as an administrator, open a command prompt (`CMD.exe`).
2. Navigate to the `c:\migrations\scripts\script_mgn_4-Verify-server-connection` folder and run the following Python command:

```
Python 4-Verify-server-connection.py --Waveid <wave-id>
```

Replace *<wave-id>* with the appropriate Wave ID value to get the new IP addresses for the target instances.

> **Note**
>
> This script uses the default RDP port 3389 and SSH port 22. If needed, you can add the following arguments to reset to the default ports: --RDPPort *<rdp-port>* --SSHPort *<ssh-port>*.

1. The script returns a server list.
2. The script returns the test results for both RDP and SSH access.

Reference

This section provides references for deploying the Cloud Migration Factory on AWS solution.

Anonymized data collection

This solution includes an option to send anonymized operational metrics to AWS. We use this data to better understand how customers use this solution and related services and products. When activated, the following information is collected and sent to AWS:

- **Solution ID:** The AWS solution identifier
- **Unique ID (UUID):** Randomly generated, unique identifier for each Cloud Migration Factory on AWS solution deployment
- **Timestamp:** Data-collection timestamp
- **Status:** Status is migrated once a server is launched in AWS MGN with this solution
- **Region:** The AWS Region where the solution is deployed

> **Note**
>
> AWS will own the data gathered via this survey. Data collection will be subject to the AWS Privacy Policy. To opt out of this feature, complete the following steps before launching the AWS CloudFormation template.

1. Download the AWS CloudFormation template to your local hard drive.
2. Open the AWS CloudFormation template with a text editor.
3. Modify the AWS CloudFormation template mapping section from:

```
Send:
 AnonymousUsage:
 Data: 'Yes'
```

to:

```
Send:
```

```
AnonymousUsage:
Data: 'No'
```

4. Sign in to the AWS CloudFormation console.
5. Select **Create stack**.
6. On the **Create stack** page, **Specify template** section, select **Upload a template file**.
7. Under **Upload a template file**, choose **Choose file** and select the edited template from your local drive.
8. Choose **Next** and follow the steps in Launch the stack in the Automated deployment section of this guide.

Related resources

AWS training

- Using AWS Solutions: Cloud Migration Factory Skill Builder course - you will learn about the features, benefits, and technical implementation of the solution.
- AWS Partners Only: Advanced Migrating to AWS (Technical, classroom based) - you will learn how to migrate workloads at scale, and covers common migration patterns, including a hands-on workshop for Cloud Migration Factory on AWS.

AWS services

- AWS CloudFormation
- AWS Lambda
- Amazon API Gateway
- Amazon CloudFront
- Amazon Cognito
- Amazon DynamoDB
- Amazon Simple Storage Service
- AWS Systems Manager
- AWS Secrets Manager

AWS resources

- Automating large-scale server migrations with Cloud Migration Factory

Contributors

The following individuals contributed to this document:

- Abe Wubshet
- Ahmad Mahmoudi
- Aijun Peng
- Asif Mithawala
- Avinash Seelam
- Balamurugan K
- Chris Baker
- Dev Kar
- Dilshad Hussain
- Frank Aloia
- Gnanasekaran Kailasam
- Jijo James
- Lakshmi Sudhakar Nekkanti
- Lyka Segura
- Phi Nguyen
- Sapeksh Madan
- Shyam Kumar
- Simon Champion
- Suman Rajotia
- Thiemo Belmega
- Vijesh Vijayakumaran Nair
- Wally Lu

Revisions

Publication date: *June 2020 (last update: November 2024)*

Visit the CHANGELOG.md in our GitHub repository to track version-specific improvements and fixes.

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.