AWS Migration Hub Orchestrator

User Guide

AWS Migration Hub Orchestrator: User Guide

Copyright © 2023 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

What is AWS Migration Hub Orchestrator?

AWS Migration Hub Orchestrator simplifies and automates the migration of servers and enterprise applications to AWS. It provides a single location to run and track your migrations.

With Migration Hub Orchestrator, you can migrate SAP NetWeaver based applications, such as S/4HANA, BW4HANA, ECC on HANA, and others to AWS and rehost supported custom applications to Amazon EC2. Migration Hub Orchestrator offers templates to create a migration workflow that can be customized to fit your unique migration requirements. Migration Hub Orchestrator automates the steps in your chosen workflow and displays the status of migration.

You can access Migration Hub Orchestrator from https://console.aws.amazon.com/migrationhub/orchestrator/ or from the AWS Command Line Interface.

Related services

If you are new to Migration Hub, you can refer to the following guides.

- Application Discovery Service
- AWS Application Migration Service
- AWS Launch Wizard for SAP

Pricing

AWS Migration Hub Orchestrator is available to you at no additional cost. You only pay for the AWS resources that you provision for migrations.

Setting up

Sign up for AWS

When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all AWS services, including AWS Migration Hub Orchestrator. You are charged only for the services that you use.

If you already have an AWS account, skip this step.

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

1. Open https://portal.aws.amazon.com/billing/signup.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

   When you sign up for an AWS account, an *AWS account root user* is created. The root user has access to all AWS services and resources in the account. As a security best practice, assign administrative access to an administrative user, and use only the root user to perform tasks that require root user access.

Create an IAM user

By default, an administrator account inherits all of the policies that are required to access Migration Hub Orchestrator. To create an **administrative user**, follow the steps in Create an administrative user.

To create a **non-administrative** IAM user for use with Migration Hub Orchestrator, we recommend that you create these IAM users:

- To access the console, create a user with both the `AWSMigrationHubFullAccess` and the `AWSMigrationHubOrchestratorConsoleFullAccess` managed policies attached.
- To enable the Migration Hub Orchestrator plugin to communicate with your servers, create a user with the `AWSMigrationHubOrchestratorPlugin` managed policy attached.
- To enable the instances to communicate with the Migration Hub Orchestrator plugin, create a user with the `AWSMigrationHubOrchestratorInstanceRolePolicy` managed policy attached.

Alternatively, you can create one user with all the managed policies attached. For more information, see AWS managed policies for Migration Hub Orchestrator.

When creating non-administrative IAM users, follow the Grant least privilege security best practice and grant users minimum permissions.

To create a non-administrator IAM user to use with Migration Hub Orchestrator

1. In AWS Management Console, navigate to the IAM console.
2. Follow the instructions in Creating an IAM user in your AWS account.

While following the instructions, ensure that you:

- Select both **Programmatic access** and **AWS Management Console access** as the type of access.
- Choose the option to **Attach existing policies to user directly** on the **Set permission** page. Then, choose the managed IAM policy **AWSMigrationHubFullAccess**, **AWSMigrationHubOrchestratorConsoleFullAccess**, or **AWSMigrationHubOrchestratorPlugin** from the list of policies.
- Follow the guidance in the **Important** note about saving the new access key ID and secret access key in a safe and secure place.

Home Region

The data stored in the AWS Migration Hub (Migration Hub) home Region provides a single repository of discovery and migration planning information for your entire migration portfolio. The data stored in the home Region from the discovery and migration tools is used to track the progress of your migrations regardless of the migrating application's target Region. For more information, see Migration Hub home Region.

How AWS Migration Hub Orchestrator works

You can simplify and automate the migration of your on-premises servers and applications to AWS Cloud using AWS Migration Hub Orchestrator.

Topics

Select a template

Based on your migration requirements, select a template to begin your migration journey with Migration Hub Orchestrator. You can see the steps of a template by selecting a template card, and then choosing **Preview**.

For more information about the different templates offered by Migration Hub Orchestrator, see Templates.

Create a workflow

After selecting your template, you can start configuring your migration workflow. Ensure that you meet the prerequisites of your selected template, and that you have defined the applications you want to migrate in AWS Application Discovery Service.

Run the workflow

Once you have configured your workflow, you can run the workflow. You can now track the progress of your migration and customize your workflow. For more information, see Migration workflows.

> **Note**
> Before you can run the workflow, some templates require the Migration Hub Orchestrator plugin to be configured on-premises. The following table denotes which templates require the plugin setup.

Template	Plugin setup required
Migrate SAP NetWeaver applications to AWS	Yes
Rehost applications on Amazon EC2	Yes
Rehost SQL server on Amazon EC2	Yes
Replatform SQL server on Amazon RDS	Yes

Template	Plugin setup required
Import virtual machine images to AWS	Optional

The plugin communicates with the source and target environments to orchestrate and automate migrations. To download and setup the Migration Hub Orchestrator plugin, see Configure Migration Hub Orchestrator plugin.

Templates

Migration Hub Orchestrator offers the following templates to configure your migration workflows.

- Migrate SAP NetWeaver applications to AWS
- Rehost applications on Amazon EC2
- Rehost SQL server on Amazon EC2
- Replatform SQL server on Amazon RDS
- Import virtual machine images to AWS

Migrate SAP NetWeaver based applications and SAP HANA databases to AWS

With this template, you can automate the migration of your SAP NetWeaver based applications along with SAP HANA databases, or SAP HANA databases only to AWS.

Topics

Migration types

The template offers the following migration types.

- SAP NetWeaver on SAP HANA – central system installation
- SAP NetWeaver on SAP HANA – distributed system installation
- SAP NetWeaver on SAP HANA – high availability installation
- SAP NetWeaver on SAP HANA – scale-out
- SAP HANA database – single node
- SAP HANA database – high availability
- SAP HANA database – scale-out

Prerequisites

You must meet the following requirements to create a migration workflow using this template.

- Verify that your servers and applications are on a supported operating system. For more information, see Version support for SAP deployments.
- Enable network connectivity between the source and target servers by opening the required ports on both servers.

- Provide credentials of SAP HANA database instance running on your source server. These credentials are used by the Migration Hub Orchestrator plugin to communicate with the source server.

  1. Sign in to https://console.aws.amazon.com/secretsmanager/.
  2. On the AWS Secrets Manager page, select **Store a new secret**.
  3. For Secret type, select **Other type of secret** and create the following key value pairs.

Key	Value
`hana_systemdb_username`	source SAP HANA system database username
`hana_systemdb_password`	source SAP HANA system database password
`hana_saptenantdb_username`	source SAP HANA tenant database username
`hana_saptenantdb_user_password`	source SAP HANA tenant database password

> **Note**
> The `hana_systemdb_username` and `hana_saptenantdb_username` must have admin permissions to enable the SAP HANA System Replication and perform database backups.

  4. Select **Next** and enter a name beginning with `migrationhub-orchestrator-`*`secretname123`* in Secret name.

> **Important**
> The Secret ID must begin with the prefix `migrationhub-orchestrator-` and must only be followed by an alphanumeric value.

  5. Select **Next** and then, select **Store**.

- The following parameters must be the same on the source and target environments.
  - SAP SID
  - SAP HANA SID
  - PAS instance number
  - ASCS instance number
  - SAP HANA instance number
  - SAP HANA database password
- You must disable SAP HANA system replication before migrating SAP environments with high availability setup.

Target environment setup

AWS Migration Hub Orchestrator guides you to create the target environment in AWS to host your SAP NetWeaver application using AWS Launch Wizard for SAP. For more information, see [Get started with AWS Launch Wizard for SAP](#).

Create an SAP deployment using AWS Launch Wizard for SAP. For more information, see [Deploy an SAP application with AWS Launch Wizard for SAP](#).

> **Note**
> Migration Hub Orchestrator supports single node or multi node SAP NetWeaver stack deployment for target. You must choose to deploy the SAP NetWeaver software as part of target environment setup with Launch Wizard.

- Create a private key in the Amazon EC2 console and store it in the AWS Secrets Manager. The plugin uses this private key associated with the target instance to perform migration tasks.

See the following steps to create a private key.

1. Sign in to the Amazon EC2 console.
2. In the left navigation pane, under Network & Security, select **Key Pairs**.
3. Select **Create key pair**.
4. Enter a name for the key pair beginning with `migrationhub-orchestrator-`*`keyname123`*.

   Important
   The Key Pair must begin with the prefix `migrationhub-orchestrator-` and must only be followed by an alphanumeric value.
5. Select **RSA** as the Key pair type.
6. Select **.pem** as the Private key file format.
7. Select **Create key pair** and save the file.

See the following steps to store the private key.

1. Sign in to https://console.aws.amazon.com/secretsmanager/.
2. On the AWS Secrets Manager page, select **Store a new secret**.
3. For Secret type, select **Other type of secret** and select **Plaintext** below.
4. Copy and paste the Private key created in Amazon EC2 console and select Next.
5. In Secret name, enter the same name (`migrationhub-orchestrator-`*`keyname123`*) that you used for creating the key pair.
6. Select **Next** and then, **Store**.

- To establish a connection between your source and target environments, we recommend creating a new security group with your source IP address while creating an SAP deployment with Launch Wizard.

  1. Under **Infrastructure - SAP landscape**, go to **Security groups**.
  2. Select **Create new security groups**.
  3. In Connection type, select **IP Address/CIDR**.
  4. In Value, enter your source IP address.
- Launch Wizard attaches the `AmazonEC2RoleForLaunchWizard` instanceRole by default when creating the target environment. After creating the target instance with Launch Wizard, attach the `AWSMigrationHubOrchestratorInstanceRolePolicy` managed policy to `AmazonEC2RoleForLaunchWizard`. For more information, see AWS managed policies for Migration Hub Orchestrator.
- Migration Hub Orchestrator uses the same secret to connect to databases on source and target servers for validation. For your target server, ensure that you provide the same SAP HANA database sign-in credentials that you stored in AWS Secrets Manager following the steps in the section called “Prerequisites” (p. 6).

Create a migration workflow

1. Go to https://console.aws.amazon.com/migrationhub/orchestrator/, and select **Create migration workflow**.
2. On Choose a workflow template page, select **Migrate SAP NetWeaver on HANA applications** template.
3. Configure and submit your workflow to begin migration.

   - the section called “Details” (p. 9)
   - the section called “Application” (p. 9)

- the section called “Source environment configuration” (p. 10)

Details

Enter a name for your workflow. Optionally, you can enter a description and add tags. If you intend to run multiple migrations, we recommend adding tags to enhance searchability. For more information, see Tagging AWS resources.

Application

Select the application you want to migrate. If you do not see the application in the list, you must define it in AWS Application Discovery Service.

Define applications

Define applications by adding a data source and grouping the servers as applications.

Topics

Add data source

Get metadata about the source servers and applications that you want to migrate to AWS. You can use one of the following methods to collect the data.

- **Migration Hub import** – Import information about your on-premises servers and applications into Migration Hub. For more information, see Migration Hub Import in the *Application Discovery Service User Guide*.
- **AWS Agentless Discovery Connector** – The Discovery Connector is a VMware appliance that collects information about VMware virtual machines (VMs). For more information, see AWS Agentless Discovery Connector in the *Application Discovery Service User Guide*.
- **AWS Application Discovery Agent** – The Discovery Agent is AWS software that you install on your on-premises servers and VMs to capture system information, as well as information about the network connections between systems. For more information, see AWS Application Discovery Agent in the *Application Discovery Service User Guide*.

Group servers

To use Migration Hub Orchestrator, you must group servers as applications.

1. In AWS Migration Hub console, select **Discover**, **Servers**.
2. In the servers list, select each server that you want to group into a new or existing application.
3. To create your application, or add to an existing one, choose **Group as application**.
4. In the **Group as application** dialog box, choose **Group as a new application** or **Add to an existing application**.
5. Select **Group**.

To view and edit your applications in the AWS Migration Hub console, go to **Discover** > **Servers**.

Source environment configuration

Enter the details of the SAP source environment that you want to migrate with the Migration Hub Orchestrator.

SAP application server configuration

- SAPSID: Enter the system ID of the SAP application that you want to migrate.
- SAP application hostname: Enter the hostname of the source SAP application.
- AWS Application Discovery Service server ID for SAP application server: Select the server ID where the central instance of your source SAP application is running. The IDs in the list are available based on the application configurations made in AWS Application Discovery Service. For more information, see Define applications.

SAP HANA database configuration

- SAP HANA replication mode: Select from *synchronous* or *asynchronous* mode for database replication.
- HANASID: Enter the system ID of your source SAP HANA database.
- Instance number: Enter the instance number of your source SAP HANA database.
- Database hostname: Enter the hostname of your source SAP HANA database. To find the hostname, run the `hostname` command on your database.
- AWS Application Discovery Service server ID for SAP HANA database: Select the server ID where your SAP HANA database is running. The IDs in the list are available based on the application configurations made in AWS Directory Service. For more information, see Define applications.
- Credentials: Select the credentials you created for your source HANA database in the section called “Prerequisites” (p. 6).
- Version: Migration Hub Orchestrator only supports migrations for SAP HANA database 2.0 versions. Verify that the version of your SAP HANA database is 2.0 or higher with `HDB version` command.
- Backup location: Enter the backup location of your SAP HANA database.

SSL encryption

- If you do not want to use SSL encryption for database replication, select the box next to *I want to disable SSL encryption for database replication*.
- If you want to use SSL encryption for database replication or leave the box unchecked, a manual step – *Enable SSL on source for replication* in step group 4, must be completed to proceed with your migration workflow.

  1. Open the `global.ini` file on your source SAP HANA system.
  2. Set the replication property as follows.

     ```
     [system_replication_communication]
     enable_ssl=on
     ```

  3. Restart the database.
- **Note**

  SSL encryption is required for SAP NetWeaver on SAP HANA – scale-out and SAP HANA database – scale-out migration types.

For more information, see SAP help portal – Configure Secure Communication (TLS/SSL) Between Primary and Secondary Sites.

Migration steps

Migration Hub Orchestrator automates the migration process after you create the migration workflow. Some tasks require additional inputs and user interactions.

- By default, Launch Wizard deploys the target SAP HANA database with baseline HANA components. If the source application that is being migrated has components that have been deployed after the initial installation, check and deploy those components on the target instance.
- An SAP HANA system has several configuration (`*.ini`) files that contain properties for configuring the system as a whole and individual tenant databases, hosts, and services. SAP HANA's configuration files contain parameters for global system configuration (`global.ini`) and for each service in the system. For instance, `indexserver.ini`. Based on your application requirement, if any of these configuration files have been adjusted on the source, you need to update them on the newly deployed target system before cutover.
- Before beginning cutover, verify that your source application has been migrated properly. Step group 7 of the **Migrate SAP NetWeaver to AWS** template guides you through the necessary steps.
  - **Stop source SAP production system**: Ensure that there are no end users logged in or accessing the application before stopping the source application.
  - **Stop source HANA production system**: Verify that the HANA System Replication has completed copying data to target and gracefully stopped the source HANA database.
  - **Cutover & Start SAP application**: Start the migrated SAP application servers on the target.
  - **Verify database records**: Verify database records to validate that the application has been migrated properly.
  - **Manual post processing**: Perform any manual post-migration tasks, such as attaching interface file systems or updating end user `SAPGUI`configuration to connect to the newly migrated applications on AWS.

Rehost applications on Amazon EC2

You can rehost your custom Windows and Linux applications on Amazon EC2 using the *Rehost applications on Amazon EC2* template.

Prerequisites

You must meet the following requirements to create a migration workflow using this template.

- Verify that your applications are on a supported operating system. For more information, see Supported operating systems.
- AWS Application Migration Service must be initialized by the IAM admin of the AWS account. For more information, see Application Migration Service initialization and permissions .
- Complete the replication settings for AWS Application Migration Service. For more information, see Replication settings.
- Provide credentials in the AWS Secrets Manager to install the AWS Replication Agent on your remote server.

  1. Sign in to https://console.aws.amazon.com/secretsmanager/.
  2. On the AWS Secrets Manager page, select **Store a new secret**.
  3. For Secret type, select **Other type of secret** and enter the following keys.
     - `access_key`
     - `secret_key`

4. Select **Next** and enter a name for the key pair beginning with `migrationhub-orchestrator-`*`secretname123`*.

   Important
   The Secret ID must begin with the prefix `migrationhub-orchestrator-` and must only be followed by an alphanumeric value.

5. Select **Next** and then, select **Store**.

- Create an IAM user and attach the **AWSApplicationMigrationAgentPolicy** policy.
- Create an IAM role with the Amazon EC2 use case to run test scripts on migrated instances. Attach the **AWSMigrationHubOrchestratorInstanceRolePolicy** and **AmazonSSMManagedInstanceCore** policies to this role. Once the role is created, update the trust policy to include SSM (`ssm.amazonaws.com`). For more information on updating a trust policy, see Modifying a role trust policy (console).
- The IAM user running the AWS Application Migration Service must have permissions to perform the `startTest` and `startCutoverInstance` tasks. Create an IAM user and attach the **AWSApplicationMigrationFullAccess**, **AWSApplicationMigrationEC2Access**, and **AmazonEC2FullAccess** policies along with the following inline policy.

```
{
     "Effect": "Allow",
     "Action": [
         "mgn:StartCutover",
         "mgn:StartTest"
     ],
     "Resource": "*"
 },
 {
     "Effect": "Allow",
     "Action": "iam:PassRole",
     "Resource": "*",
     "Condition": {
         "StringEquals": {
             "iam:PassedToService": "ec2.amazonaws.com"
         }
     }
 }
```

Create a migration workflow

1. Go to https://console.aws.amazon.com/migrationhub/orchestrator/, and select **Create migration workflow**.
2. On Choose a workflow template page, select **Rehost on Amazon EC2 using AWS Application Migration Service** template.
3. Configure and submit your workflow to begin migration.

   - the section called “Details” (p. 12)
   - the section called “Application” (p. 13)
   - the section called “Target environment configuration” (p. 13)

Details

Enter a name for your workflow. Optionally, you can enter a description and add tags. If you intend to run multiple migrations, we recommend adding tags to enhance searchability. For more information, see Tagging AWS resources.

Application

Select the application you want to migrate. If you do not see the application in the list, you must define it in AWS Application Discovery Service.

Define applications

Define applications by adding a data source and grouping the servers as applications.

Topics

Add data source

Get metadata about the source servers and applications that you want to migrate to AWS. You can use one of the following methods to collect the data.

- **Migration Hub import** – Import information about your on-premises servers and applications into Migration Hub. For more information, see Migration Hub Import in the *Application Discovery Service User Guide*.
- **AWS Agentless Discovery Connector** – The Discovery Connector is a VMware appliance that collects information about VMware virtual machines (VMs). For more information, see AWS Agentless Discovery Connector in the *Application Discovery Service User Guide*.
- **AWS Application Discovery Agent** – The Discovery Agent is AWS software that you install on your on-premises servers and VMs to capture system information, as well as information about the network connections between systems. For more information, see AWS Application Discovery Agent in the *Application Discovery Service User Guide*.

Group servers

To use Migration Hub Orchestrator, you must group servers as applications.

1. In AWS Migration Hub console, select **Discover**, **Servers**.
2. In the servers list, select each server that you want to group into a new or existing application.
3. To create your application, or add to an existing one, choose **Group as application**.
4. In the **Group as application** dialog box, choose **Group as a new application** or **Add to an existing application**.
5. Select **Group**.

To view and edit your applications in the AWS Migration Hub console, go to **Discover** > **Servers**.

Target environment configuration

If you want to run test scripts on migrated instances, check the box for *I want to run test scripts on the migrated instances*.

> **Note**
> We recommend having separate workflows for Linux and Windows servers if you want to run validation tests on migrated instances.

- Test script location: Specify the Amazon S3 bucket that contains your test script. For more information, see Getting started with Amazon S3.

- IAM role: Choose the IAM role you created in the section called “Prerequisites” (p. 11).
- Script run command: Enter the **run** command for your script.

Credentials to install AWS Replication Agent: Select the credentials you created in the section called “Prerequisites” (p. 11).

Rehost SQL server on Amazon EC2

With **Rehost SQL server on Amazon EC2** template, you can rehost your SQL servers on-premises to Amazon EC2 using native backup and restore. You can also migrate databases that are encrypted with transparent data encryption.

> **Note**
> This template must be used along with AWS Direct Connect. To use the template without AWS Direct Connect, send us an email at mh-orchestrator-interest@amazon.com with your AWS account number and AWS Region where you have registered the Migration Hub Orchestrator plugin.

Topics

Prerequisites

You must set up the source and target environments before creating a migration workflow.

Topics

Source environment setup

- When configuring the Migration Hub Orchestrator plugin, ensure that the username that is provided to connect to your Windows machine has the `SYSAdmin` permission on the SQL server instance.
- Ensure that PowerShell is enabled on the server that contains your SQL server instance.
- Install AWS.Tools on the server that contains your SQL server instance, with the following command.

```
Install-Module -Name AWS.Tools.Installer
```

  For more information, see What are AWS Tools for PowerShell?
- Create an IAM policy with the following permissions.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "kms:GenerateDataKey",
                "kms:CreateKey"
            ],
            "Resource": "*"
        }
    ]
}
```

- Configure a name profile for AWS Command Line Interface that uses the preceding IAM user. For more information, see Using AWS credentials.
- Install the `DBA.Tools` module on your Windows machine, with the following command.

```
Cmd: Install-Module dbatools
```

Target environment setup

- (*Optional*)If you want to use BYOL for SQL server, use AWS VM Import/Export to import your VM image.
- (*Optional*) Use AWS Launch Wizard to deploy your target SQL server.
  - Launch Wizard attaches the `AmazonEC2RoleForLaunchWizard` instance role by default when creating the target environment.
  - After creating the target environment with Launch Wizard, attach the `AWSMigrationHubOrchestratorInstanceRolePolicy` managed policy to `AmazonEC2RoleForLaunchWizard`. For more information, see AWS managed policies for Migration Hub Orchestrator.
- If you are not using Launch Wizard to create your target environment, attach the `AWSMigrationHubOrchestratorInstanceRolePolicy` managed policy to your instance role.
- Add the following permissions to your instance role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "kms:Decrypt",
                "s3:ListAllMyBuckets",
                "s3:ListBucket"
            ],
            "Resource": "*"
        }
    ]
}
```

- Create a username in your target SQL server with `SYSAdmin` permission.
- Provide credentials in AWS Secrets Manager for the username created in your target SQL server.

1. Sign in to https://console.aws.amazon.com/secretsmanager/.
2. On the AWS Secrets Manager page, select **Store a new secret**.
3. For Secret type, select **Other type of secret** and enter the following keys.
   - `username` - enter your username
   - `password` - enter your password

4. Select **Next** and enter a name for the key pair beginning with `migrationhub-orchestrator-`*`secretname123`*.

   Important
   The Secret ID must begin with the prefix `migrationhub-orchestrator-` and must only be followed by an alphanumeric value.
5. Select **Next** and then, select **Store**.

Create a migration workflow

1. Go to https://console.aws.amazon.com/migrationhub/orchestrator/, and select **Create migration workflow**.
2. On Choose a workflow template page, select **Rehost SQL server on Amazon EC2** template.
3. Configure and submit your workflow to begin migration.

Topics

Details

Enter a name for your workflow. Optionally, you can enter a description and add tags. If you intend to run multiple migrations, we recommend adding tags to enhance searchability. For more information, see Tagging AWS resources.

Application

Select the application you want to migrate. If you do not see the application in the list, you must define it in AWS Application Discovery Service.

Define applications

Define applications by adding a data source and grouping the servers as applications.

Topics

Add data source

Get metadata about the source servers and applications that you want to migrate to AWS. You can use one of the following methods to collect the data.

- **Migration Hub import** – Import information about your on-premises servers and applications into Migration Hub. For more information, see Migration Hub Import in the *Application Discovery Service User Guide*.
- **AWS Agentless Discovery Connector** – The Discovery Connector is a VMware appliance that collects information about VMware virtual machines (VMs). For more information, see AWS Agentless Discovery Connector in the *Application Discovery Service User Guide*.
- **AWS Application Discovery Agent** – The Discovery Agent is AWS software that you install on your on-premises servers and VMs to capture system information, as well as information about the network

connections between systems. For more information, see AWS Application Discovery Agent in the *Application Discovery Service User Guide*.

Group servers

To use Migration Hub Orchestrator, you must group servers as applications.

1. In AWS Migration Hub console, select **Discover**, **Servers**.
2. In the servers list, select each server that you want to group into a new or existing application.
3. To create your application, or add to an existing one, choose **Group as application**.
4. In the **Group as application** dialog box, choose **Group as a new application** or **Add to an existing application**.
5. Select **Group**.

To view and edit your applications in the AWS Migration Hub console, go to **Discover** > **Servers**.

Replatform SQL server on Amazon RDS

With **Replatform SQL server on Amazon RDS** template, you can migrate your SQL servers on-premises to Amazon RDS using native backup and restore. You can also migrate databases that are encrypted with transparent data encryption.

> **Note**
> This template must be used along with AWS Direct Connect. To use the template without AWS Direct Connect, send us an email at mh-orchestrator-interest@amazon.com with your AWS account number and AWS Region where you have registered the Migration Hub Orchestrator plugin.

Topics

Prerequisites

You must set up the source and target environments before creating a migration workflow.

Topics

Source environment setup

- When configuring the Migration Hub Orchestrator plugin, ensure that the user that is provided to connect to your Windows machine has the `SYSAdmin` permission on the SQL server instance.
- Ensure that PowerShell is enabled on the server that contains your SQL server instance.
- Install AWS.Tools on the server that contains your SQL server instance, with the following command.

```
Install-Module -Name AWS.Tools.Installer
```

For more information, see What are AWS Tools for PowerShell?

- Create an IAM policy with the following permissions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "kms:GenerateDataKey",
                "kms:CreateKey"
            ],
            "Resource": "*"
        }
    ]
}
```

- Create an IAM Role with the preceding policy attached.
- Configure a name profile for AWS Command Line Interface that uses the preceding IAM user. For more information, see Using AWS credentials.
- Install the `DBA.Tools` module on your Windows machine, with the following command.

```
Cmd: Install-Module dbatools
```

Target environment setup

- Deploy an Amazon RDS SQL server with the same version as the source SQL server.
- Configure the target Amazon RDS SQL server with the same parameter groups as the source SQL server.
- Deploy an Amazon EC2 instance and create an instance role.
  - Attach the `AWSMigrationHubOrchestratorInstanceRolePolicy` and `AmazonSSMManagedInstanceCore` managed policies to this role.
  - Add the following permissions to this role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::migrationhub-orchestrator-*",
                "arn:aws:s3:::aws-migrationhub-orchestrator-*/*"
            ]
        }
    ]
}
```

- Migration Hub Orchestrator plugin creates an Amazon S3 bucket to store on-premises backups and transparent data encryptions, if the source SQL server is using it.

  For more information, see the following.

- Importing and exporting SQL Server databases using native backup and restore
- Support for Transparent Data Encryption in SQL Server

Configure the option group for backup/restore and transparent data encryption, and attach the following policies to the created IAM role.

```
      {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "s3:ListAllMyBuckets",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "s3:ListBucket",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

```
      {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "rds.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

- Ensure that your Amazon RDS instance can be reached from the created Amazon EC2 instance.
- Provide credentials in AWS Secrets Manager for the username created in your target SQL server.

1. Sign in to https://console.aws.amazon.com/secretsmanager/.
2. On the AWS Secrets Manager page, select **Store a new secret**.
3. For Secret type, select **Other type of secret** and enter the following keys.
   - `username` - enter your username
   - `password` - enter your password
4. Select **Next** and enter a name for the key pair beginning with `migrationhub-orchestrator-`*`secretname123`*.

   Important
   The Secret ID must begin with the prefix `migrationhub-orchestrator-` and must only be followed by an alphanumeric value.
5. Select **Next** and then, select **Store**.

Create a migration workflow

1. Go to https://console.aws.amazon.com/migrationhub/orchestrator/, and select **Create migration workflow**.
2. On Choose a workflow template page, select **Rehost SQL server on Amazon EC2** template.
3. Configure and submit your workflow to begin migration.

Topics

Details

Enter a name for your workflow. Optionally, you can enter a description and add tags. If you intend to run multiple migrations, we recommend adding tags to enhance searchability. For more information, see Tagging AWS resources.

Application

Select the application you want to migrate. If you do not see the application in the list, you must define it in AWS Application Discovery Service.

Define applications

Define applications by adding a data source and grouping the servers as applications.

Topics

Add data source

Get metadata about the source servers and applications that you want to migrate to AWS. You can use one of the following methods to collect the data.

- **Migration Hub import** – Import information about your on-premises servers and applications into Migration Hub. For more information, see Migration Hub Import in the *Application Discovery Service User Guide*.
- **AWS Agentless Discovery Connector** – The Discovery Connector is a VMware appliance that collects information about VMware virtual machines (VMs). For more information, see AWS Agentless Discovery Connector in the *Application Discovery Service User Guide*.
- **AWS Application Discovery Agent** – The Discovery Agent is AWS software that you install on your on-premises servers and VMs to capture system information, as well as information about the network connections between systems. For more information, see AWS Application Discovery Agent in the *Application Discovery Service User Guide*.

Group servers

To use Migration Hub Orchestrator, you must group servers as applications.

1. In AWS Migration Hub console, select **Discover**, **Servers**.
2. In the servers list, select each server that you want to group into a new or existing application.
3. To create your application, or add to an existing one, choose **Group as application**.
4. In the **Group as application** dialog box, choose **Group as a new application** or **Add to an existing application**.
5. Select **Group**.

To view and edit your applications in the AWS Migration Hub console, go to **Discover** > **Servers**.

Import virtual machine images to AWS

You can use the *Import virtual machine images to AWS* template to convert existing images of Open Virtual Appliance (OVA) or VMware Virtual Machine Disk (VMDK) to Amazon Machine Image (AMI) for Amazon EC2.

Prerequisites

You must meet the following requirements to create a VM import workflow using this template.

- Create an IAM user and attach the required policies to use Migration Hub Orchestrator. For more information, see Create an IAM user
- Create an IAM user and a service role, and attach required policies to use VM Import/Export. For more information, see Required permissions.

  You may need to perform additional tasks to prepare your AWS environment before import. For more information, see VM Import/Export Requirements.
- **Upload images to Amazon S3**

  Create an Amazon S3 bucket, and add the OVA or VMDK files you want to import, to the bucket. The following rules and limitations apply.
  - The Amazon S3 bucket must be in the same Region as the AWS account in which you are using Migration Hub Orchestrator.
  - Create separate folders for OVA and VMDK files in your bucket.
  - The folder containing your VMDK files must be named with the prefix `migrationhub-orchestrator-vmie-`*`folder-name`* and must only contain VMDK files.
  - The folder containing your OVA file must be named with the prefix `migrationhub-orchestrator-vmie-`*`folder-name`* and must only contain an OVA file.

- The disk container path for OVA must specify the OVA file name. For more information, see the section called "Source environment configuration" (p. 22).
- Only one OVA file can be added in one import task. You can add up to five import tasks in the workflow.

For more information about creating an Amazon S3 bucket, see Creating a bucket.

Create a workflow

1. Go to https://console.aws.amazon.com/migrationhub/orchestrator/, select **Create migration workflow**.
2. On Choose a workflow template page, select **Import virtual images to AWS** template.
3. Configure and submit your workflow to begin the VM import.
   - the section called "Details" (p. 22)
   - the section called "Source environment configuration" (p. 22)
   - the section called "Target environment configuration" (p. 22)

Details

Enter a name for your workflow. Optionally, you can enter a description and add tags. If you intend to import multiple VM images, we recommend adding tags to enhance searchability. For more information, see Tagging AWS resources.

Source environment configuration

You need to specify the following parameters to configure your workflow.

- **Server IP** - This is an optional parameter where you can provide the IP address of the on-premises server that needs to be migrated. You must setup the Migration Hub Orchestrator plugin on providing the IP address. This enables Migration Hub Orchestrator to run a validation and detect any failure scenarios before import.
- **Disk container** - You must specify the path for the Amazon S3 bucket folder that you set up in the section called "Prerequisites" (p. 21). See the following examples for more details.
  - **OVA** - `s3://`*`bucket-name`*`/`**`migrationhub-orchestrator-vmie-`***`folder-name`*`/`*`file-name`*`.ova`
  - **VMDK** - `s3://`*`bucket-name`*`/`**`migrationhub-orchestrator-vmie-`***`folder-name`*

  When more than one disk container is added, Migration Hub Orchestrator runs the workflow sequentially. If the first disk container fails, you must recover the failed container or create a new workflow.
- **Add new item** - You can add up to five image tasks for the workflow.

Target environment configuration

This section of the Import virtual machine images to AWS template workflow has optional parameters for licensing. For more information, refer to the following documentation.

- Licensing options
- Boot modes

Configure the Migration Hub Orchestrator plugin

The Migration Hub Orchestrator plugin is a virtual appliance that you can install in your on-premises VMware environment.

> **Important**
> The Migration Hub Orchestrator plugin must be able to communicate with the source and target environments to orchestrate and automate migrations. The version of the plugin that is deployed in vCenter supports VMware vCenter Server 6.0, 6.5, 6.7 and 7.0.

Download

To deploy the plugin as a virtual machine (VM) in your VMware environment, download the plugin Open Virtualization Archive (OVA) file using the following steps.

1. Sign in to the https://console.aws.amazon.com/migrationhub/orchestrator/.
2. In the left navigation pane, choose **Orchestrate**.
3. On the **Migration Hub Orchestrator** page, choose **Download plugin**.
4. After the plugin is downloaded to your on-premises VMware environment, you can deploy it in vCenter. Sign in to vCenter as a VMware administrator.

   We recommend at least 8 GB of RAM and at least 4 CPUsfor the VM.
5. Deploy the OVA file that you downloaded. The OVA file includes the plugin and a CLI that can be used to access the Migration Hub Orchestrator API.
6. Sign in to the plugin using an SSH client.

   ```
   ssh ec2-user@PluginIPAddress
   ```

   When prompted for a password, enter the default password, **plugin@123**. You must change your password when you first sign in.

> **Tip**
> If you would like to use the plugin for multiple virtual machines, you can export the OVA file after you configure it, and import it to your desired source VM.

Configure

To configure the Migration Hub Orchestrator plugin using **plugin setup** commands, create a bash shell session in the plugin Docker container using the following command.

```
docker exec -it mhub-orchestrator-plugin bash
```

The **plugin setup** command runs all of the following commands in succession, but you can also run them individually:

- **plugin setup --aws-configurations**
- **plugin setup --vcenter-configurations**
- **plugin setup --remote-server-configurations**

Run the following command to set up all of the plugin configurations at the same time. Then, enter the information for AWS configurations, vCenter configurations, and remote server configurations.

```
plugin setup
```

Topics

Set up AWS configurations

Set up AWS configurations using the `plugin setup` command or the `plugin setup --aws-configurations` command.

1. Enter **Y** for yes to **Have you setup IAM permissions...**. You set up these permissions when you created an IAM user to access the plugin using the `AWSMigrationHubOrchestratorPlugin` managed policy following the steps in Setting up.
2. Enter the IAM profile that you created in the Migration Hub Orchestrator plugin using the following command.

   ```
   aws configure --profile <profile-name>
   ```
3. Enter your `access_key` and `secret_key` from the AWS account that has the IAM user that you created to access the plugin.
4. Enter a Region. For example, `us-west-2`. Choose a Region that suits your needs from the Regions that Migration Hub Orchestrator uses. For a list of these Regions, see Migration Hub Orchestrator endpoints in the *AWS General Reference*.
5. Enter **Y** for yes to **Upload plugin related metrics to Migration Hub Orchestrator?** Metrics data helps AWS to provide you with support.
6. Enter **Y** for yes to **Upload plugin related logs to Migration Hub Orchestrator?** Log data helps AWS to provide you with support.

Your configuration setup may look similar to this example.

```
plugin setup --aws-configurations
Have you setup IAM permissions in your AWS account as per the user guide? [Y/N]: Y
IAM Profile name: <profile-name>
Upload plugin related metrics to Migration Hub Orchestrator? By default plugin will upload
 metrics. [Y/N]: Y
Upload plugin related logs to Migration Hub Orchestrator? By default plugin will upload
 logs. [Y/N]: Y
Plugin configurations are saved successfully
Start registering plugin
Start registering plugin
Plugin is registered successfully.
```

Set up vCenter configurations

Set up vCenter configurations using the `plugin setup` command or the `plugin setup --vcenter-configurations` command.

1. Enter **Y** or **N** to **Would you like to authenticate using VMware vCenter credentials** based on your preference.

   > **Note**
   > Authenticating using VMware vCenter credentials requires that VMware tools are installed on the target servers.

   Enter the **Host Url**, which can be the vCenter IP address or the URL. Then, enter the **Username** and **Password** for VMware vCenter.
2. Enter **Y** for yes to **Do you have Windows machines managed by VMware vCenter** if you want to configure Windows servers. Then, enter the **Username** and **Password** for Windows.

   > **Note**
   > If your Windows Remote Server belongs to an Active Directory domain, you must enter the username as *`domain-name`\`username`* when using the CLI to provide source server configurations. For example, if the name of your domain is exampledomain and your username is Administrator, then the username you enter in the CLI is **exampledomain\Administrator**.
3. Enter **Y** for yes to **Setup for Linux using VMware vCenter** if you want to configure Linux servers. Then, enter the **Username** and **Password** for Linux.
4. Enter **Y** for yes to the **Would you like to setup credentials for servers outside vCenter using NTLM for Windows** and **SSH/Cert based for Linux** questions if you want to set up source server credentials for servers outside of vCenter.
5. For **Would you like to use the same Windows credentials used during vCenter setup**, enter **Y** for yes if the credentials for the Windows machines that are managed outside of vCenter are the same as the credentials provided when configuring credentials for vCenter Windows machines. Otherwise, enter **N** for no.

   If you answer **Y** for yes, the following questions are asked.

   a. Enter **Y** for yes to **Are you okay with the plugin accepting and locally storing server certificates on your behalf during first interaction with windows servers?**.
   b. Enter **1** for **Enter your options** if you want to configure SSH authentication.

      If you choose to use SSH authentication, you must copy the generated key credentials to your Linux servers. For more information, see [Set up key-based authentication on Linux servers (p. 27)](#).

Your configuration setup may look similar to this example.

```
Start setting up vCenter configurations for remote execution
Note: authenticating using VMware vCenter credentials requires VMware tools to be installed
 on the target servers
Would you like to authenticate using VMware vCenter credentials? [Y/N]: Y
Host Url for VMware vCenter: host-url
Username for VMware vCenter: username
Password for VMware vCenter:
Successfully stored vCenter credentials...
Setup for Windows using VMware vCenter? [Y/N]: Y
Username for Windows: username
Password for Windows:
Successfully stored vCenter windows credentials...
Setup for Linux using VMware vCenter? [Y/N]: Y
Username for Linux: username
Password for Linux:
```

```
Successfully stored vCenter linux credentials...
Would you like to setup credentials for servers outside vCenter using NTLM for windows and
 SSH/Cert based for linux? [Y/N]: Y
Would you like to use the same Windows credentials used during vCenter setup? [Y/N]: Y
Are you okay with plugin accepting and locally storing server certificates on your behalf
 during first interaction with windows servers? These certificates will be used by plugin
 for secure communication with windows servers [Y/N]:Y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/mhub-
orchestrator-plugin/remote-auth/windows/certs

Please note the IP address of the plugin and run the script specified in the user
 documentation on all the windows servers in your inventory
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert based
 for Linux? [Y/N]: Y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
Would you like to use the same Linux credentials used during vCenter setup? [Y/N]: Y
Generating SSH key on this machine...
SSH key pair path: /opt/amazon/mhub-orchestrator-plugin/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys" file
 in your remote machines.
Your Linux remote server configurations are saved successfully.
```

Set up source server configurations

Set up source server configurations using the `plugin setup` command or the `plugin setup --remote-server-configurations` command.

1. Enter **Y** for yes to **Would you like to setup credentials for servers not managed by vCenter using NLTM for Windows** if you want to configure Windows servers. Enter the **Username** and **Password** for WinRM.

   > **Note**
   > If your Windows Remote Server belongs to an Active Directory domain, you must enter the username as *`domain-name`*`\`*`username`* when using the CLI to provide source server configurations. For example, if the name of your domain is exampledomain and your username is Administrator, then the user name you enter in the CLI is **exampledomain \Administrator**.

   Enter **Y** for yes to **Are you okay with plugin accepting and locally storing server certificates on your behalf during first interaction with windows servers?**. Windows Server certificates are stored in the directory `/opt/amazon/mhub-orchestrator-plugin/remote-auth/windows/certs`. You must copy the generated server credentials to your Windows servers. For more information, see Set up the source server configuration on Windows servers (p. 28).
2. Enter **Y** for yes to **Setup for Linux using SSH or Cert** if you want to configure Linux servers.
3. Enter **1** for **Enter your options** if you want to configure for SSH key based authentication. If you choose to use SSH authentication, you must copy the generated key credentials to your Linux servers. For more information, see Set up key-based authentication on Linux servers (p. 27).
4. Enter **2** for **Enter your options** if you want to configure for certificate-based authentication. For information about setting up certificate-based authentication, see Set up certificate-based authentication on Linux servers (p. 28).

Your configuration setup may look similar to this example.

```
Setting up target server for remote execution
Would you like to setup credentials for servers not managed by vCenter using NLTM for
 Windows [Y/N]: Y
Username for WinRM: username //Enter domain-name\username, if the server is in AD domain
Password for WinRM: password
Are you okay with plugin accepting and locally storing server certificates on your behalf
 during first interaction with windows servers? These certificates will be used by plugin
 for secure communication with windows servers [Y/N]: Y
Successfully stored windows server credentials...
Please note that all windows server certificates are stored in directory /opt/amazon/mhub-
orchestrator-plugin/remote-auth/windows/certs

Please note the IP address of the plugin and run the script specified in the user
 documentation on all the windows servers in your inventory
Would you like to setup credentials for servers not managed by vCenter using SSH/Cert based
 for Linux? [Y/N]: Y
Choose one of the following options for remote authentication:
1. SSH based authentication
2. Certificate based authentication
Enter your options [1-2]: 1
User name for remote server: username
Generating SSH key on this machine...
SSH key pair path: /opt/amazon/mhub-orchestrator-plugin/remote-auth/linux/keys/
id_rsa_assessment
Please add the public key "id_rsa_assessment.pub" to the "$HOME/.ssh/authorized_keys" file
 in your remote machines.
Your Linux remote server configurations are saved successfully.
```

Enable the Migration Hub Orchestrator plugin to communicate with source servers

> **Note**
> This step isn't necessary if you set up the Migration Hub Orchestrator plugin using vCenter credentials.

After you set up your remote server configurations, if you are using the `plugin setup` or `plugin setup --remote-server-configurations` command, you must prepare your remote servers so that the Migration Hub Orchestrator plugin can collect data from them.

> **Note**
> You must make sure that the servers are reachable using their private IP address. For further instructions on how to set up the environment through a virtual private cloud (VPC) on AWS for remote running, see the Amazon Virtual Private Cloud User Guide.

Prepare source Linux servers

Set up key-based authentication on Linux servers

If you choose to set up SSH key-based authentication for Linux when configuring source server configurations, you must perform the following steps to set up key-based authentication on your servers so that the Migration Hub Orchestrator plugin can communicate with source server.

To set up key-based authentication on your Linux servers

1. Copy the public key that was generated with the name **id_rsa_assessment.pub** from the following folder in the container:

/opt/amazon/mhub-orchestrator-plugin/remote-auth/linux/keys.

2. Append the copied public key in the `$HOME/.ssh/authorized_keys` file for all of the remote machines. If there is no file available, create it using the `touch` or `vim` command.
3. Ensure that the home folder on the source server has a permission level of `755` or less. You can use the `chmod` command to restrict permissions.

Set up certificate-based authentication on Linux servers

If you choose to set up certificate-based authentication for Linux when configuring source server configurations, you must perform the following steps so that the Migration Hub Orchestrator plugin can communicate with the source server.

We recommend this option if you already have Certificate Authority (CA) set up for your application servers.

To set up certificate-based authentication on your Linux servers

1. Copy the username that works with all of your remote servers.
2. Copy the public key of the plugin to the CA.

   The public key for the plugin can be found in the following location:

   /opt/amazon/mhub-orchestrator-plugin/remote-auth/linux/keys/id_rsa_assessment.pub

   This public key must be added to your CA for generating the certificate.
3. Copy the certificate that was generated in the previous step to the following location in the plugin:

   /opt/amazon/mhub-orchestrator-plugin/remote-auth/linux/keys

   The name of the certificate must be **id_rsa_assessment-cert.pub**.
4. Provide the certificate file name during setup.

Set up the source server configuration on Windows servers

If you choose to set up Windows when you set up the source server in the **plugin setup**, you must perform the following steps so that the Migration Hub Orchestrator plugin can communicate with the source server.

> **To understand more about the PowerShell script that's executed on the source server, read this note.**
> The script enables PowerShell remote and disables all authentication methods other than negotiate. This is used for Windows NT LAN Manager (NTLM) and sets the "AllowUnencrypted" WSMan protocol to false to ensure that the newly created listener accepts only encrypted traffic.
> Using the Microsoft provided script, `New-SelfSignedCertificateEx.ps1`, it creates a self-signed certificate.
> Any WSMan Instance that has an HTTP listener is removed, along with existing HTTPS listeners. Then, it creates a new HTTPS listener. It also creates an inbound firewall rule for TCP port 5986. In the final step, the WinRM service is restarted.

To set up a remote connection on Windows 2008 servers

1. Use the following command to check the version of PowerShell installed on your server.

```
$PSVersionTable
```

2. If the PowerShell version is not 5.1, then download and install WMF 5.1 by following the instructions at Install and Configure WMF 5.1 in the Microsoft documentation.
3. Use the following command in a new PowerShell window to ensure that PowerShell 5.1 is installed.

```
$PSVersionTable
```

To set up a remote connection on Windows 2012 and newer servers

1. Download the setup script from the following URL:

   Setup script
2. Download the `New-SelfSignedCertificateEx.ps1` from the following URL and paste the script into the same folder in which you downloaded `WinRMSetup.ps1`:

   https://github.com/Azure/azure-libraries-for-net/blob/master/Samples/Asset/New-SelfSignedCertificateEx.ps1
3. To complete the setup, run the downloaded PowerShell script on all application servers.

```
.\WinRMSetup.ps1
```

Note

If Windows Remote Management (WinRM) is not set up properly on the Windows Remote Server, an attempt to communicate will fail. If this happens, you must delete the certificate that corresponds to that server from the following location on the container: **/opt/amazon/mhub-orchestrator-plugin/remote-auth/windows/certs/*`ads-server-id`*.cer**
After you delete the certificate, wait for the ongoing process to be retried.

Migration workflows

Migration Hub Orchestrator provides predefined templates that offer automation capabilities and facilitate the migration of your on-premises servers and applications to AWS. A template consists of one or more step groups that contain steps. A step can be automated or manual.

You can create a workflow with one of the following templates.

- Migrate SAP NetWeaver applications to AWS

  A template to migrate SAP NetWeaver-based applications (S/4HANA, BW4HANA, and ECC on HANA) running on SAP HANA database to AWS.
- Rehost applications on Amazon EC2

  A template to rehost applications on Amazon EC2 using AWS Application Migration Service (AWS MGN).

Add a step

You can add, reorder, and delete step groups and steps *after* you create the workflow.

1. Sign in to the https://console.aws.amazon.com/migrationhub/orchestrator/.
2. In the left navigation pane, choose **Orchestrate** > **Workflows**.
3. On the **Workflows** page, select the workflow that you want to customize and choose **View details**.
4. Under **Steps**, select **Add**.
5. To create a manual step, enter a **Name** for your step and choose **Add**.

   > **Note**
   > Manual steps require user intervention. After completing the step, you must update the status to enable the migration workflow to continue.
6. To create an automated step:

   - Enter a **Name** for your step.
   - Specify a **Script location**. You can upload a custom script to an Amazon S3 bucket or upload a file from your local machine. For more information, see Getting started with Amazon S3.
   - Enter the **Script run command** that Migration Hub Orchestrator can use to run your script.
   - In **Script run environment**, select **On premises** to run the script in the source environment, or select **AWS** to run the script in the target environment.
   - Based on your selection for the **Script run environment**, the list under **Server** displays the applications that you configured in the Application Discovery Service. For more information, see Define applications.

Rules and limitations

There are some rules and limitations when customizing migration workflows:

- You can make modifications to a migration workflow after it's created.
- A step must be placed within a step group. You can choose to add a step to an existing step group or create a new step group.

- A step group must have at least one step.
- A step can't be added to a step group with a status of **Completed**.
- To delete an ongoing migration workflow, you must pause it first.

Security in Migration Hub Orchestrator

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to Migration Hub Orchestrator, see AWS services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations

This documentation helps you understand how to apply the shared responsibility model when using Migration Hub Orchestrator. It shows you how to configure Migration Hub Orchestrator to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Migration Hub Orchestrator resources.

Contents

Data protection in Migration Hub Orchestrator

The AWS shared responsibility model applies to data protection in Migration Hub Orchestrator. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual users with AWS IAM Identity Center (successor to AWS Single Sign-On) or AWS Identity and

Access Management (IAM). That way, each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We require TLS 1.2 and recommend TLS 1.3.
- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing sensitive data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form text fields such as a **Name** field. This includes when you work with Migration Hub Orchestrator or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form text fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Encryption at rest

Migration Hub Orchestrator encrypts all data at rest.

Encryption in transit

Migration Hub Orchestrator inter-network communications support TLS 1.2 encryption between all components and clients.

AWS managed policies for Migration Hub Orchestrator

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ReadOnlyAccess** AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the *IAM User Guide*.

AWS managed policy: AWSMigrationHubOrchestratorConsoleFullAccess

Attach the `AWSMigrationHubOrchestratorConsoleFullAccess` policy to your IAM identities.

The `AWSMigrationHubOrchestratorConsoleFullAccess` policy grants an AWS account full access to the Migration Hub Orchestrator service through the AWS Management Console.

Permissions details

This policy includes the following permissions.

- `migrationhub-orchestrator` – Allows AWS account full access to Migration Hub Orchestrator.
- `s3` – Allows AWS account to create and read from the S3 buckets used by Migration Hub Orchestrator.
- `secretsmanager` – Allows AWS account to access to AWS Secrets Manager.
- `discovery` – Allows AWS account access to Application Discovery Service.
- `iam` – Allows a service-linked role to be created for the AWS account, which is a requirement for using Migration Hub Orchestrator.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "migrationhub-orchestrator:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:CreateBucket",
                "s3:PutEncryptionConfiguration",
                "s3:PutBucketPublicAccessBlock",
                "s3:PutBucketPolicy",
                "s3:PutBucketVersioning",
                "s3:PutLifecycleConfiguration"
            ],
            "Resource": "arn:aws:s3:::migrationhub-orchestrator-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:ListSecrets"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "discovery:GetDiscoverySummary"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "migrationhub-orchestrator.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetRole"
            ],
            "Resource": "arn:aws:iam::*:role/aws-service-role/migrationhub-
orchestrator.amazonaws.com/AWSMigrationHubOrchestratorServiceRolePolicy*"
        }
    ]
}
```

AWS managed policy: AWSMigrationHubOrchestratorPlugin

Attach the `AWSMigrationHubOrchestratorPlugin` policy to your IAM identities.

The `AWSMigrationHubOrchestratorPlugin` policy grants an AWS account access to the Migration Hub Orchestrator service, read/write access to the S3 buckets that are related to the service, Amazon API Gateway access to upload logs and metrics to AWS, and AWS Secrets Manager access to fetch credentials.

Permissions details

This policy includes the following permissions.

- `migrationhub-orchestrator` – Allows the AWS account access to the Orchestrator plugin.
- `s3` – Allows the AWS account write access to the S3 buckets used by Migration Hub Orchestrator.
- `secretsmanager` – Allows AWS account access to AWS Secrets Manager.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketAcl"
            ],
            "Resource": "arn:aws:s3:::migrationhub-orchestrator-*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:ListAllMyBuckets"
            ],
            "Resource": "arn:aws:s3:::*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "execute-api:Invoke",
                "execute-api:ManageConnections"
            ],
            "Resource": [
                "arn:aws:execute-api:*:*:*/prod/*/put-log-data",
                "arn:aws:execute-api:*:*:*/prod/*/put-metric-data"
            ]
        },
            {
                "Effect": "Allow",
                "Action": [
                    "migrationhub-orchestrator:RegisterPlugin",
                    "migrationhub-orchestrator:GetMessage",
                    "migrationhub-orchestrator:SendMessage"
                ],
                "Resource": "arn:aws:migrationhub-orchestrator:*:*:*"
            },
        {
            "Effect": "Allow",
            "Action": [
                "secretsmanager:GetSecretValue"
            ],
            "Resource": "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
        }
    ]
}
```

AWS managed policy: AWSMigrationHubOrchestratorInstanceRolePolicy

Attach the `AWSMigrationHubOrchestratorInstanceRolePolicy` policy to your IAM identities.

This policy grants an AWS account read/write access to Amazon S3 buckets that are related to the service and to AWS Secrets Manager to fetch credentials.

Permissions details

This policy includes the following permissions.

- `migrationhub-orchestrator` – Allows AWS account access to Migration Hub Orchestrator.
- `s3` – Allows AWS account read/write access to Amazon S3 buckets used by Migration Hub Orchestrator.
- `secretsmanager` – Allows AWS account access to AWS Secrets Manager.

```
{
    "Effect": "Allow",
    "Action": [
        "secretsmanager:GetSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:migrationhub-orchestrator-*"
}, {
        "Effect": "Allow",
        "Action": [
            "s3:GetObject"
        ],
        "Resource": [
            "arn:aws:s3:::migrationhub-orchestrator-*",
            "arn:aws:s3:::aws-migrationhub-orchestrator-*/*"
        ]
    }
```

Migration Hub Orchestrator updates to AWS managed policies

View details about updates to AWS managed policies for Migration Hub Orchestrator since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Migration Hub Orchestrator Document history page.

Change	Description	Date
AWSMigrationHubOrchestratorServiceRolePolicy - Updated policy	ec2:DescribeLaunchTemplates action added to the policy.	February 24, 2023
AWSMigrationHubOrchestratorServiceRolePolicy - Updated policy	ec2:DescribeImportImageTasks, s3:ListBucket, and events:RemoveTargets actions added to the policy.	December 21, 2022
AWSMigrationHubOrchestratorConsoleFullAccess (p. 34) – New policy made available at launch	AWSMigrationHubOrchestratorConsoleFullAccess grants an AWS account full access to the Migration Hub Orchestrator service through the AWS Management Console.	April 20, 2022
AWSMigrationHubOrchestratorPlugin (p. 35) – New policy made available at launch	AWSMigrationHubOrchestratorPlugin grants an AWS account access to the Migration Hub Orchestrator service and read/write access to Amazon S3 buckets that are related to the service. It also grants Amazon API Gateway access to upload logs and metrics to AWS, and AWS Secrets Manager access to fetch credentials.	April 20, 2022
AWSMigrationHubOrchestratorServiceRolePolicy (p. 38) – New policy made available at launch	The AWSMigrationHubOrchestratorServiceRolePolicy service-linked role policy provides access to AWS Migration Hub and AWS Application Discovery Service. This policy also grants permissions for storing reports in Amazon Simple Storage Service (Amazon S3).	April 20, 2022

Change	Description	Date
`AWSMigrationHubOrchestratorInstanceRolePolicy` – New policy	`AWSMigrationHubOrchestratorInstanceRolePolicy` grants an AWS account read/write access to Amazon S3 buckets that are related to the service and to AWS Secrets Manager to fetch credentials.	April 20, 2022
Migration Hub Orchestrator started tracking changes	Migration Hub Orchestrator started tracking changes for its AWS managed policies.	April 20, 2022

Using service-linked roles for Migration Hub Orchestrator

Migration Hub Orchestrator uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to Migration Hub Orchestrator. Service-linked roles are predefined by Migration Hub Orchestrator and include all of the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up Migration Hub Orchestrator easier because you don’t have to manually add the necessary permissions. Migration Hub Orchestrator defines the permissions of its service-linked roles, and unless you make changes to the configuration, only Migration Hub Orchestrator can assume its roles. Configurable permissions include the trust policy and the permissions policy. You can't attach the permissions policy to any other IAM entity.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have **Yes** in the **Service-Linked Role** column. Follow the **Yes** link to view the service-linked role documentation for that service, if applicable.

Service-linked role permissions for Migration Hub Orchestrator

Migration Hub Orchestrator uses the service-linked role named **AWSServiceRoleForMigrationHubOrchestrator** and associates it with the **AWSMigrationHubOrchestratorServiceRolePolicy** IAM policy – Provides access to AWS Migration Hub and AWS Application Discovery Service. This policy also grants permissions for storing reports in Amazon Simple Storage Service (Amazon S3).

The **AWSServiceRoleForMigrationHubOrchestrator** service-linked role trusts the following services to assume the role:

- `migrationhub-orchestrator.amazonaws.com`

The role permissions policy allows Migration Hub Orchestrator to complete the following actions.

AWS Application Discovery Service actions

```
discovery:ListConfigurations
```

```
discovery:DescribeConfigurations
```

AWS Launch Wizard actions

`launchwizard:ListProvisionedApps`

`launchwizard:DescribeProvisionedApp`

Amazon Elastic Compute Cloud actions

`ec2:DescribeInstances`

`ec2:CreateLaunchTemplateVersion`

`ec2:ModifyLaunchTemplate`

`ec2:DescribeImportImageTasks`

`ec2:DescribeLaunchTemplates`

AWS Migration Hub actions

`mgh:GetHomeRegion`

Amazon EC2 Systems Manager actions

`ssm:SendCommand`

`ssm:GetCommandInvocation`

`ssm:CancelCommand`

`ssm:DescribeInstanceInformation`

`ssm:GetCommandInvocatio`

Amazon S3 actions

`s3:GetObject`

`s3:ListBucket`

Amazon EventBridge actions

`events:PutTargets`

`events:DescribeRule`

`events:DeleteRule`

`events:PutRule`

`events:RemoveTargets`

AWS Application Migration Service actions

`mgn:GetReplicationConfiguration`

`mgn:GetLaunchConfiguration`

`mgn:StartCutover`

`mgn:FinalizeCutover`

`mgn:StartTest`

`mgn:UpdateReplicationConfiguration`

`mgn:DescribeSourceServers`

`mgn:MarkAsArchived`

`mgn:ChangeServerLifeCycleState`

`mgn:StartReplication`

The following is the full policy showing which resources the above actions apply to:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "discovery:DescribeConfigurations",
                "discovery:ListConfigurations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "launchwizard:ListProvisionedApps",
                "launchwizard:DescribeProvisionedApp"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateLaunchTemplateVersion",
                "ec2:ModifyLaunchTemplate"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AWSApplicationMigrationServiceManaged":
 "mgn.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeLaunchTemplates"
            ],
            "Resource": "*"
         },
         {
            "Action": [
            "Action": [
                "mgh:GetHomeRegion"
            ],
            "Effect": "Allow",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:SendCommand",
                "ssm:GetCommandInvocation",
                "ssm:CancelCommand"
            ],
            "Resource": [
                "arn:aws:ssm:*::document/AWS-RunRemoteScript",
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:s3:::aws-migrationhub-orchestrator-*",
                "arn:aws:s3:::migrationhub-orchestrator-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:DescribeInstanceInformation",
                "ssm:GetCommandInvocation"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::migrationhub-orchestrator-*",
                "arn:aws:s3:::migrationhub-orchestrator-*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:PutTargets",
                "events:DescribeRule",
                "events:DeleteRule",
                "events:PutRule",
                "events:RemoveTargets"
            ],
            "Resource": "arn:aws:events:*:*:rule/MigrationHubOrchestratorManagedRule*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "mgn:GetReplicationConfiguration",
                "mgn:GetLaunchConfiguration",
                "mgn:StartCutover",
                "mgn:FinalizeCutover",
                "mgn:StartTest",
                "mgn:UpdateReplicationConfiguration",
                "mgn:DescribeSourceServers",
                "mgn:MarkAsArchived",
                "mgn:ChangeServerLifeCycleState",
                "mgn:StartReplication"
            ],
            "Resource": "*"
            },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeImportImageTasks"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "s3:ListBucket",
            "Resource": "arn:aws:s3:::*",
            "Condition": {
                "StringLike": {
                    "s3:prefix": "migrationhub-orchestrator-vmie-*"
        }
            }
        }
    ]
}
```

To view the update history of this policy, see [Migration Hub Orchestrator updates to AWS managed policies (p. 37)](#).

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see [Service-Linked Role Permissions](#) in the *IAM User Guide*.

Creating a service-linked role for Migration Hub Orchestrator

You don't need to manually create a service-linked role. When you agree to allow Migration Hub to create a service-linked role (SLR) in your account in the AWS Management Console, Migration Hub Orchestrator creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you agree to allow Migration Hub to create a service-linked role (SLR) in your account, Migration Hub Orchestrator creates the service-linked role for you again.

Editing a service-linked role for Migration Hub Orchestrator

Migration Hub Orchestrator does not allow you to edit the **AWSServiceRoleForMigrationHubOrchestrator** service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using the Migration Hub Orchestrator console, CLI, or API.

Deleting a service-linked role for Migration Hub Orchestrator

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the **AWSServiceRoleForMigrationHubOrchestrator** service-linked role. For more information, see [Deleting a Service-Linked Role](#) in the *IAM User Guide*.

When deleting Migration Hub Orchestrator resources used by the **AWSServiceRoleForMigrationHubOrchestrator** SLR, you cannot have any running assessments (tasks for generating recommendations). No background assessments can be running, either. If assessments are running, the SLR deletion fails in the IAM console. If the SLR deletion fails, you can retry the deletion after all background tasks have completed. You don’t need to clean up any created resources before you delete the SLR.

Supported Regions for Migration Hub Orchestrator service-linked roles

Migration Hub Orchestrator supports using service-linked roles in all of the regions where the service is available. For more information, see AWS Regions and Endpoints.

Migration Hub Orchestrator and interface VPC endpoints (AWS PrivateLink)

You can establish a private connection between your VPC and Migration Hub Orchestrator by creating an *interface VPC endpoint*. Interface endpoints are powered by AWS PrivateLink. With AWS PrivateLink, you can privately access Migration Hub Orchestrator API operations without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to communicate with Migration Hub Orchestrator API operations. Traffic between your VPC and Migration Hub Orchestrator stays within the Amazon network.

Each interface endpoint is represented by one or more Elastic Network Interfaces in your subnets.

For more information, see Interface VPC endpoints (AWS PrivateLink) in the *Amazon VPC User Guide*.

Considerations for Migration Hub Orchestrator VPC endpoints

Before you set up an interface VPC endpoint for Migration Hub Orchestrator, ensure that you review Interface endpoint properties and limitations and AWS PrivateLink quotas in the *Amazon VPC User Guide*.

Migration Hub Orchestrator supports making calls to all of its API actions from your VPC. To use all of Migration Hub Orchestrator, you must create a VPC endpoint.

Creating an interface VPC endpoint for Migration Hub Orchestrator

You can create a VPC endpoint for Migration Hub Orchestrator using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see Creating an interface endpoint in the *Amazon VPC User Guide*.

Create a VPC endpoint for Migration Hub Orchestrator using the following service name:

- `com.amazonaws.region.migrationhub-orchestrator`

If you use private DNS for the endpoint, you can make API requests to Migration Hub Orchestrator using its default DNS name for the Region. For example, you can use the name `migrationhub-orchestrator.us-east-1.amazonaws.com`.

For more information, see Accessing a service through an interface endpoint in the *Amazon VPC User Guide*.

Creating a VPC endpoint policy for Migration Hub Orchestrator

You can attach an endpoint policy to your VPC endpoint. The VPC endpoint policy controls access to Migration Hub Orchestrator. The policy specifies the following information:

- The principal that can perform actions
- The actions that can be performed
- The resources on which these actions can be performed

For more information, see Controlling access to services with VPC endpoints in the *Amazon VPC User Guide*.

Example: VPC endpoint policy for Migration Hub Orchestrator actions

The following is an example of an endpoint policy for Migration Hub Orchestrator. When attached to an endpoint, this policy grants access to the listed Migration Hub Orchestrator actions for all principals on all resources.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "migrationhub-orchestrator:ListMigrationWorkflowTemplates",
         ],
         "Resource":"*"
      }
   ]
}
```

Compliance validation for Migration Hub Orchestrator

Third-party auditors assess the security and compliance of Migration Hub Orchestrator as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see AWS services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using Migration Hub Orchestrator is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.

- Evaluating Resources with Rules in the *AWS Config Developer Guide* – AWS Config; assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in Migration Hub Orchestrator

The AWS global infrastructure is built around AWS Regions and Availability Zones. Regions provide multiple physically separated and isolated Availability Zones, which are connected through low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Infrastructure security in Migration Hub Orchestrator

As a managed service, Migration Hub Orchestrator is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access Migration Hub Orchestrator through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

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

Logging Migration Hub Orchestrator API calls using AWS CloudTrail

Migration Hub Orchestrator integrates with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in Migration Hub Orchestrator. CloudTrail captures all API calls for Migration Hub Orchestrator as events. The calls that are captured include calls from the Migration Hub Orchestrator console and code calls to Migration Hub Orchestrator API operations. If you create a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for Migration Hub Orchestrator. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to Migration Hub Orchestrator, the IP address from which the request was made, who made the request, when it was made, and other details.

To learn more about CloudTrail, see the AWS CloudTrail User Guide.

Migration Hub Orchestrator information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When there is activity in Migration Hub Orchestrator, it's recorded in a CloudTrail event along with other AWS service events in the **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for Migration Hub Orchestrator, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Overview for creating a trail
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple Regions
- Receiving CloudTrail log files from multiple accounts

Migration Hub Orchestrator supports logging the following actions as events in CloudTrail log files:

- CreateMigrationWorkflow
- UpdateMigrationWorkflow
- DeleteMigrationWorkflow
- StartMigrationWorkflow
- StopMigrationWorkflow

- TagResource
- UntagResource
- CreateWorkflowStep
- UpdateWorkflowStep
- DeleteWorkflowStep
- RetryWorkflowStep
- CreateWorkflowStepGroup
- UpdateWorkflowStepGroup
- DeleteWorkflowStepGroup
- GetMigrationWorkflow
- ListMigrationWorkflows
- GetMigrationWorkflowTemplate
- ListMigrationWorkflowTemplates
- ListTemplateStepGroups
- GetTemplateStepGroup
- ListTemplateSteps
- GetTemplateStep
- ListTagsForResource
- GetWorkflowStep
- ListWorkflowSteps
- GetWorkflowStepGroup
- ListWorkflowStepGroups

- ListPlugins

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity element.

Understanding Migration Hub Orchestrator log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `GetWorkflowStep` action.

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        type": "AssumedRole",
        "principalId": "777777777777",
        "arn": "arn:aws:sts::111122223333:assumed-role/myUserName/...",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "777777777777",
                "arn": "arn:aws:iam::111122223333:role/myUserName",
                "accountId": "111122223333",
                "userName": "myUserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2022-03-22T23:29:22Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2022-03-23T03:16:55Z",
    "eventSource": "migrationhub-orchestrator.amazonaws.com",
    "eventName": "GetWorkflowStep",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "99.99.999.999",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:91.0) Gecko/20100101
 Firefox/91.0",
    "requestParameters": {
        "stepGroupId": "act-1",
        "id": "step-11111",
        "workflowId": "mw-1111111"
    },
    "responseElements": null,
    "requestID": "068e87d1",
    "eventID": "e699238c",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Quotas for Migration Hub Orchestrator

Your AWS account has default quotas, formerly referred to as limits, for each AWS service. Unless otherwise noted, each quota is Region-specific. You can request increases for some quotas, and other quotas cannot be increased.

To view a list of the quotas for Migration Hub Orchestrator, see Orchestrator service quotas.

To view the quotas for Migration Hub Orchestrator, open the Service Quotas console. In the navigation pane, choose **AWS services** and select **Migration Hub Orchestrator**.

To request a quota increase, see Requesting a Quota Increase in the *Service Quotas User Guide*. If the quota is not yet available in Service Quotas, use the limit increase form.

Version history of AWS Migration Hub Orchestrator plugin

The following table provides a version history of the AWS Migration Hub Orchestrator plugin.

Version	Details	Release date
1.0.3	Bug fix: reduced redundant file creation	April 18, 2023
1.0.1	Bug fix: improved mechanisms for plugin tasks	March 03, 2023
1.0	Initial release	April 20, 2022

Document history

Change	Description	Date
New section	Added How it works section.	May 22, 2023
Updated section	Updated Configure plugin section.	May 22, 2023
Updated feature	Updates to the Migrate SAP template.	April 04, 2023
Updated policy	Updates to the `AWSMigrationHubOrchestratorServiceRolePolicy`.	February 24, 2023
New feature	Added Import virtual machine images to AWS template.	December 21, 2022
Updated policy	Updates to the `AWSMigrationHubOrchestratorServiceRolePolicy`.	December 21, 2022
New feature	Added Replatform SQL server on Amazon RDS template.	November 01, 2022
New feature	Added Rehost SQL server on Amazon EC2 template.	November 01, 2022
Initial release	Initial release of the Migration Hub Orchestrator User Guide.	April 20, 2022