

Workflow Based **IT Automation solution**



MDRM

Mantech Dynamic Robotic Manager

Installing MDRM on AWS



IPL



Monitoring



Simulation
Training



Daily Routine
Checks



Disaster
Recovery

manTech
Solution

Table of Contents

1. Product Overview	3
1.1 Introduction.....	3
1.1.1 Requirements.....	3
1.1.2 Supported regions.....	4
1.1.3 Architecture.....	4
1.1.4 Use cases.....	4
2. Planning Guidelines	5
2.1 Security.....	5
2.1.1 IAM policy settings.....	5
2.2 Costs and licenses.....	7
2.3 Instance type.....	7
3. Deployment Procedure	8
3.1 Pre-tasks.....	8
3.1.1 Create VPCs.....	8
3.1.2 Create subnets.....	9
3.1.3 Internet gateway settings.....	10
3.1.4 Routing table settings.....	12
3.1.5 Create security groups.....	14
3.1.6 Create an instance.....	15
3.1.7 Elastic IP settings.....	17
3.2 Install MDRM.....	19
4. System Administration	21
4.1 Login.....	21
4.2 Main menu.....	22
4.2.1 Menu bar.....	22
4.2.2 Dashboard.....	23
4.2.3 System.....	23
4.2.4 Workflow.....	23
4.2.5 Scan.....	24
4.2.6 Settings.....	24
4.3 License management.....	25
4.3.1 License type.....	25
4.3.2 How to set up a license.....	25
4.4 Version upgrade.....	26
5. Support	26
5.1 Technical support.....	26
5.2 Support costs.....	26
5.3 SLA.....	26

1. Product Overview

This guide assumes that you have experience with AWS and are familiar with AWS services. In particular, basic knowledge of VPC and EC2 services is required. If you're new to AWS, see [“Getting Started with AWS Documentation”](#).

- **Amazon VPC**
Amazon Virtual Cloud (Amazon VPC) service allows you to provision a dedicated, isolated section of the AWS Cloud where you can launch AWS services and other resources in a virtual network that you define. You have complete control over your virtual networking environment, including choosing your own IP address ranges, creating subnets, and configuring routing tables and network gateways.
- **Amazon EC2**
The Amazon Elastic Compute Cloud (Amazon EC2) service allows you to launch virtual machine instances on a variety of operating systems. You can select an existing Amazon Machine Image (AMI) or import your own virtual machine image.

1.1 Introduction

Mantech Dynamic Robotic Manager (MDRM) is an IT automation solution for efficient operation management and rapid restart of systems in various customer environments.

Workflow-based business process management, operational procedure validation and monitoring capabilities, and visualization of the system recovery process enable efficient operational management of your data center.

Systematic system management through MDRM eliminates the inconvenience of managing diverse, complex tasks, and saves time and resources by streamlining repetitive tasks.

1.1.1 Requirements

The hardware specifications required for the MDRM installation server depend on the number of managed servers (MDRM agent installation servers). Please refer to the table below when choosing an instance type.

[System requirements]

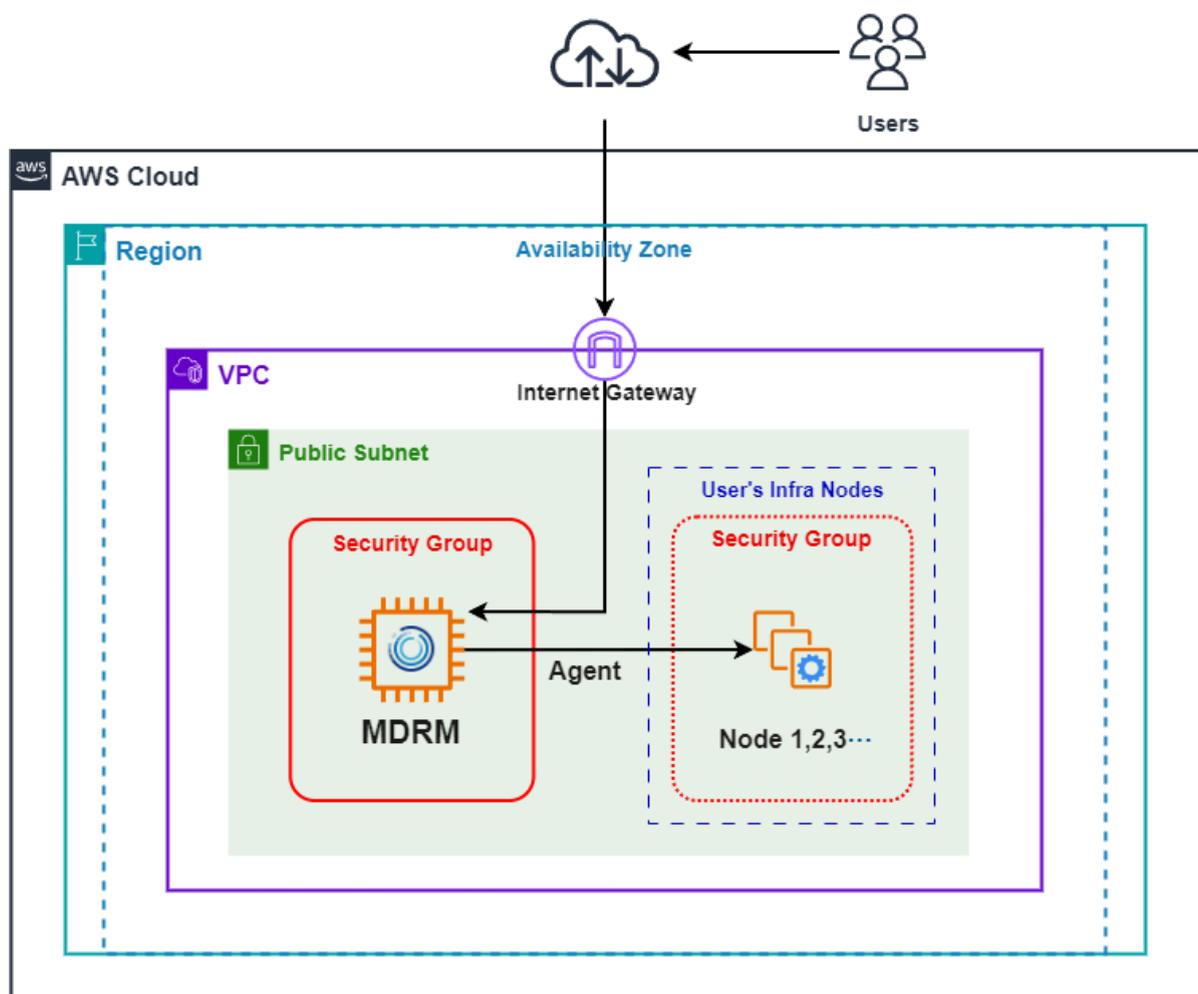
Resource	Less than 50 servers	Less than 100 servers	Less than 500 servers
vCPU	- 2.0GHz 64bit - 6 cores	- 2.0GHz 64bit - 8 cores	- 2.0GHz 64bit - 16 Core - Recommended: 24 Core
Memory	12 GiB	24 GiB	- 32 GiB - Recommended: 48 GiB
Disk	200 GB	500 GB	800 GB

1.1.2 Supported regions

Name	Code
Asia Pacific (Seoul)	ap-northeast-2

1.1.3 Architecture

MDRM EC2 instances are deployed in a VPC environment where users can communicate with the managed systems (nodes) they operate. And set up an Internet gateway to allow users to access the MDRM console from outside the VPC environment.



1.1.4 Use cases

Please see the following videos for use cases of MDRM.

- https://youtu.be/TNmlowp0L8M?si=RbGV3R8uzGX_jm3
- <https://youtu.be/wgcograNVts?si=aP4ki3alf-22tRpP>

2. Planning Guidelines

2.1 Security

To install and control MDRM, AWS root credential is not used but SSH access is required.

2.1.1 IAM policy settings

To deploy and service MDRM, you need permission to create and view VPCs, EC2s, Subnets, and SGs. To gain permission, set up the IAM policy by referring to the following procedure and JSON contents.

- 1) In the AWS Management Console, open the "[IAM dashboard](#)".
- 2) On the left menu, click "Access Management > Policy" and then click [Create Policy].
- 3) Select the JSON tab and create a policy by referring to the contents below.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CopyImage",
        "ec2:CreateImage",
        "ec2:CreateKeyPair",
        "ec2:CreateSecurityGroup",
        "ec2:CreateSnapshot",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2>DeleteKeyPair",
        "ec2>DeleteSecurityGroup",
        "ec2>DeleteSnapshot",
        "ec2>DeleteVolume",
        "ec2:DeregisterImage",
        "ec2:DescribeImageAttribute",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeRegions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",
        "ec2:DescribeSubnets",
        "ec2:DescribeTags",
        "ec2:DescribeVolumes",
```

"ec2:DetachVolume",
"ec2:GetPasswordData",
"ec2:ModifyImageAttribute",
"ec2:ModifyInstanceAttribute",
"ec2:ModifySnapshotAttribute",
"ec2:RegisterImage",
"ec2:RunInstances",
"ec2:StopInstances",
"ec2:TerminateInstances",
"ec2:AcceptVpcPeeringConnection",
"ec2:AcceptVpcEndpointConnections",
"ec2:AllocateAddress",
"ec2:AssignIpv6Addresses",
"ec2:AssignPrivateIpAddresses",
"ec2:AssociateAddress",
"ec2:AssociateDhcpOptions",
"ec2:AssociateRouteTable",
"ec2:AssociateSubnetCidrBlock",
"ec2:AssociateVpcCidrBlock",
"ec2:AttachClassicLinkVpc",
"ec2:AttachInternetGateway",
"ec2:AttachNetworkInterface",
"ec2:AttachVpnGateway",
"ec2:AuthorizeSecurityGroupEgress",
"ec2:AuthorizeSecurityGroupIngress",
"ec2:CreateCarrierGateway",
"ec2:CreateCustomerGateway",
"ec2:CreateDefaultSubnet",
"ec2:CreateDefaultVpc",
"ec2:CreateDhcpOptions",
"ec2:CreateEgressOnlyInternetGateway",
"ec2:CreateFlowLogs",
"ec2:CreateInternetGateway",
"ec2:CreateLocalGatewayRouteTableVpcAssociation",
"ec2:CreateNatGateway",
"ec2:CreateNetworkAcl",
"ec2:CreateNetworkAclEntry",
"ec2:CreateNetworkInterface",
"ec2:CreateNetworkInterfacePermission",
"ec2:CreateRoute",
"ec2:CreateRouteTable",
"ec2:CreateSecurityGroup",
"ec2:CreateSubnet",

```

    "ec2:CreateTags",
    "ec2:CreateVpc",
    "ec2:CreateVpcEndpoint",
    "ec2:CreateVpcEndpointConnectionNotification",
    "ec2:CreateVpcEndpointServiceConfiguration",
    "ec2:CreateVpcPeeringConnection",
    "ec2:CreateVpnConnection",
    "ec2:CreateVpnConnectionRoute",
    "ec2:CreateVpnGateway"
  ],
  "Resource": "*"
}
]
}

```

2.2 Costs and licenses

MDRM supports BYOL license. Bring Your Own License(BYOL) is available from your partner or distributor and provides the same ordering method across all private and public clouds, regardless of platform. To use the features of MDRM you must apply your license key in the management console. How to apply the license: ["How to set up a license"](#).

License	Price(per 1ea)	Scope of technical support
MDRM ASP	¥60,000	"Technical support" reference

AWS services that may be charged

AWS service costs are your responsibility including EC2 instances. Resource costs vary depending on instance type and usage.

For more information, see "AWS official website(<https://aws.amazon.com/pricing>)".

- EC2 instance (required)
- EBS (required)

2.3 Instance type

The instance type is recommended to be "C5.2xlarge" specification or higher, but it will depend on the size of the system you operate. Please refer to the ["Requirements"](#) to choose the appropriate instance type.

For more information about instance types, see <https://aws.amazon.com/ko/ec2/instance-types/>.

3. Deployment Procedure

Summary

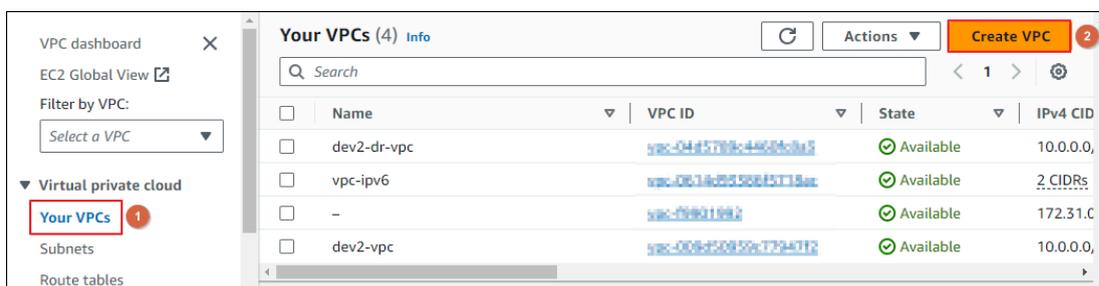
1. Prepare the network environment (“[Pre-tasks](#)” reference)
2. Create EC2 Instance with the provided AMI
3. Install MDRM (run install.sh)

3.1 Pre-tasks

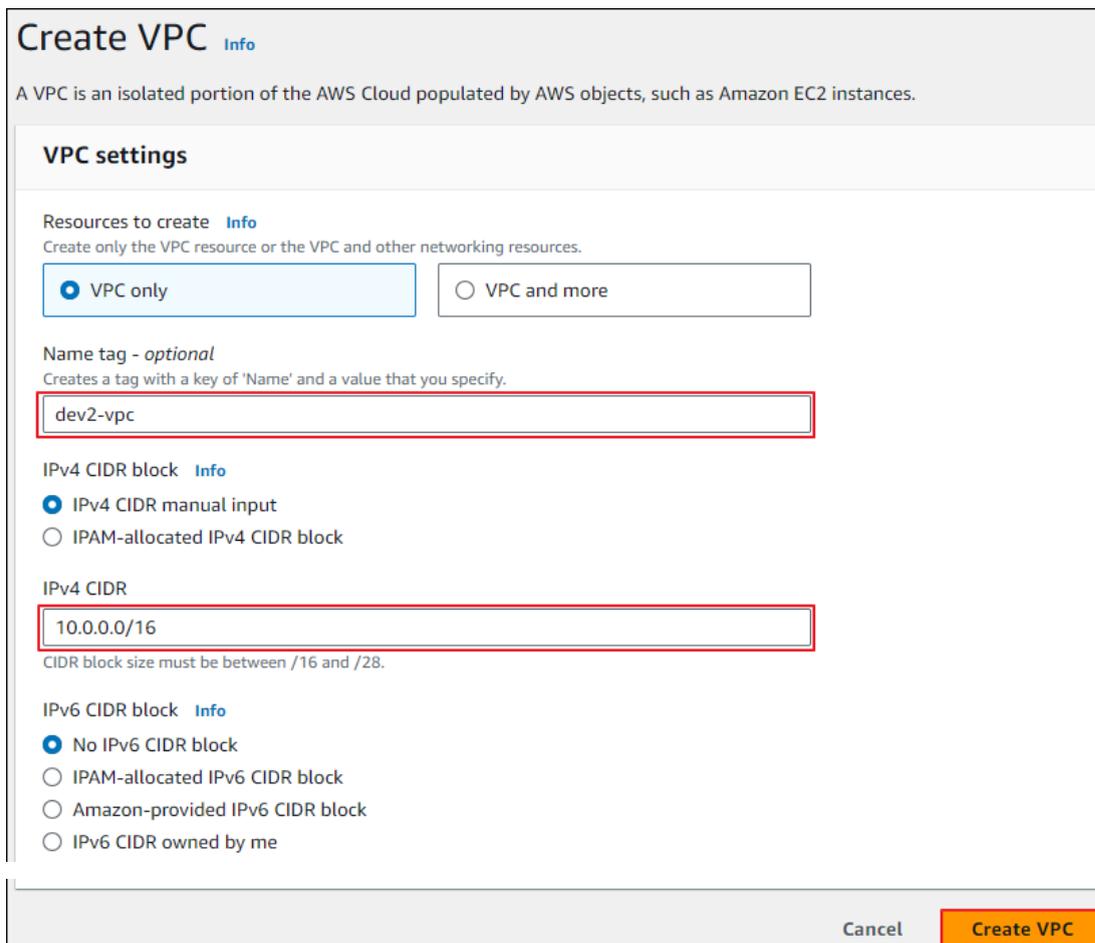
Before installing MDRM, set up your network environment and create an instance with ‘MDRM’ AMI.

3.1.1 Create VPCs

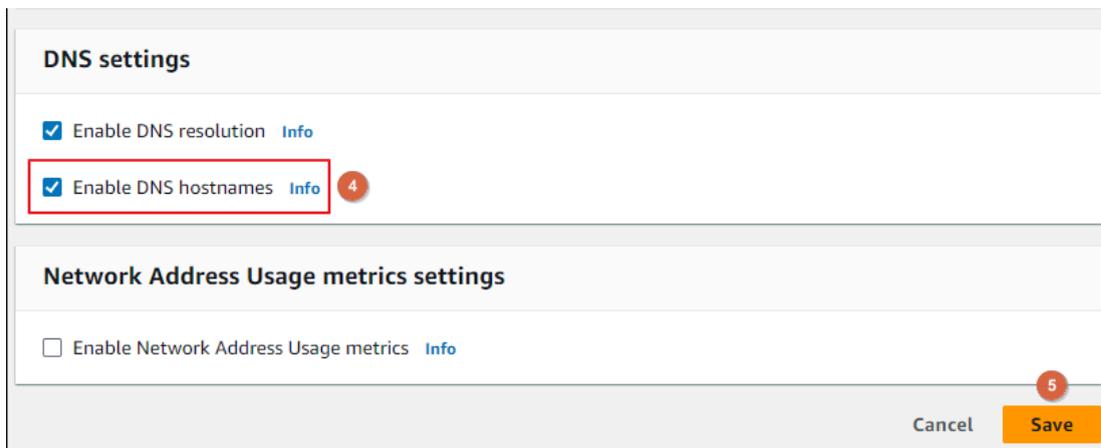
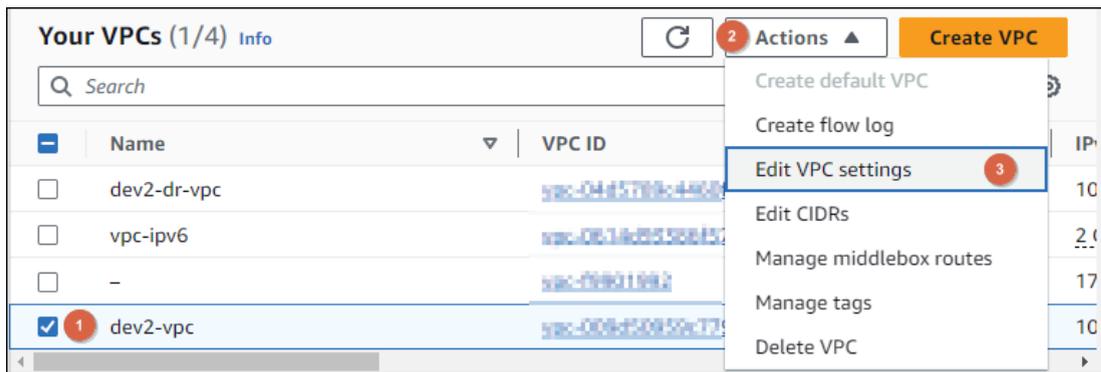
1. In the VPC dashboard, select "Your VPCs" and click [Create VPC].



2. After setting the name (tag) and CIDR block, click [Create VPC].

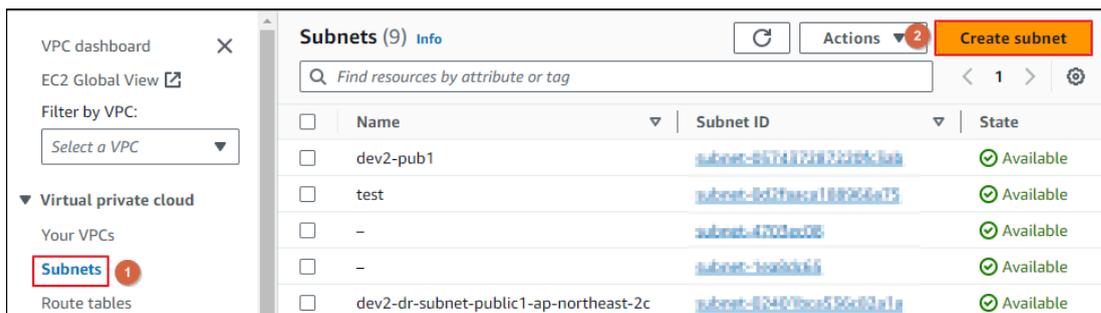


3. Select the VPC you created > Edit VPC settings > Check “Enable DNS hostnames” and save. If you enable “Enable DNS hostnames”, the DNS hostnames are automatically created for all EC2 instances within your VPC.



3.1.2 Create subnets

1. Click “Subnets” on the left menu and then click [Create subnet].



2. Select the VPC you created earlier.



3. Create a subnet by specifying the subnet name, availability zone, and CIDR block.
 - ✂ If you use multiple subnets on one instance, set the Availability Zones to be the same.

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

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

1

The name can be up to 256 characters long.

Availability Zone [Info](#)
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

2

IPv4 VPC CIDR block [Info](#)
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

3

IPv4 subnet CIDR block

4 256 IPs

< > ^ v

▼ Tags - optional

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="dev2-pub1"/>	<input type="button" value="Remove"/>

You can add 49 more tags.

5

3.1.3 Internet gateway settings

1. On the left menu, click "Internet gateways" and then click [Create internet gateway].

- ▼ Virtual private cloud
- Your VPCs
- Subnets
- Route tables
- Internet gateways 1
- Egress-only internet gateways

Internet gateways (3) [Info](#)

<input type="checkbox"/>	Name	Internet gateway ID	State
<input type="checkbox"/>	igw-mdrm	igw-80c118ad1a11c122e0e	✔ Attached
<input type="checkbox"/>	dev2-dr-igw	igw-08c1a76c11593220ac	✔ Attached
<input type="checkbox"/>	-	igw-25ad1141	✔ Attached

manTech
Solution

9

2. After writing the name (tag), click [Create internet gateway].

Create internet gateway [Info](#)

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

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

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add 50 more tags.

3. Select the created internet gateway and click [Actions] > [Attach to VPC].
Or, right-click on the internet gateway name and click [Attach to VPC].

Internet gateways (1/3) [Info](#)

<input type="checkbox"/>	Name	Internet gateway ID	VPC ID
<input type="checkbox"/>	igw-mdrm	igw-Ob2194a81a1127ec	vpc-009
<input checked="" type="checkbox"/>	dev2-dr-igw	igw-Ob42b8c1159222ee	vpc-009
<input type="checkbox"/>	-	igw-141	vpc-f99

Context menu for 'dev2-dr-igw':

- Create internet gateway
- View details
- Attach to VPC**
- Detach from VPC
- Manage tags
- Delete internet gateway

4. Select the VPC to connect to and click [Attach internet gateway].

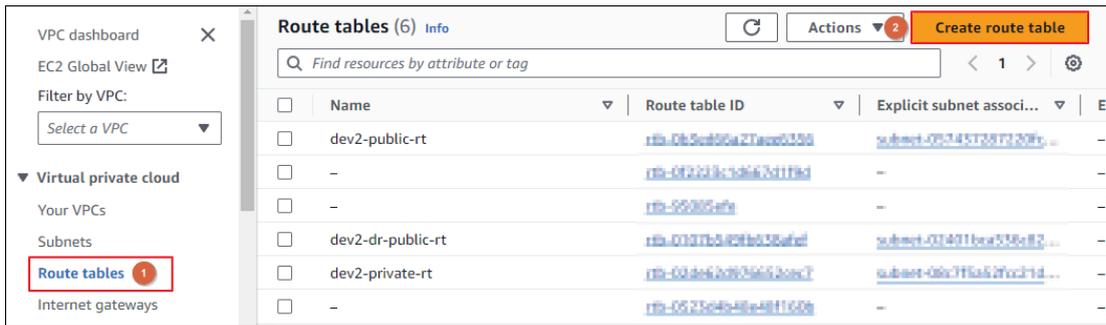
Attach to VPC (igw-0a1091d19a6506679) [Info](#)

VPC
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

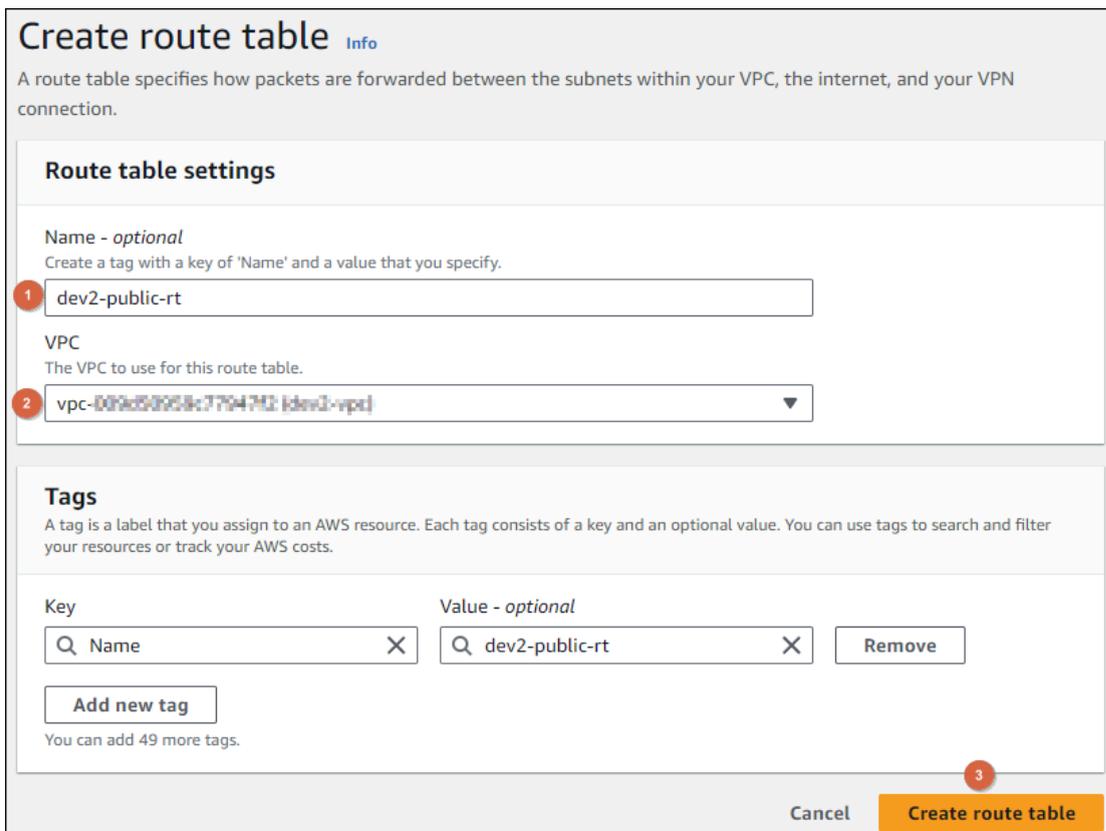
Available VPCs
Attach the internet gateway to this VPC.

3.1.4 Routing table settings

1. Click “Route tables” on the left menu and then click [Create route table].



2. Enter a route table name, select VPC, and click [Create route table].



- Click [Edit routes].

rtb-0b3ed86a27ace6356 / dev2-public-rt

Details Info

Route table ID rtb-0b3ed86a27ace6356	Main No	Explicit subnet associations subnet-0574572872204c3ab / dev2-pub1	Edge associations -
VPC vpc-009d50859c77947f2 dev2-vpc	Owner ID 340108855584		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (2) Both Edit routes

Filter routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

- After clicking [Add route], specify the destination (0.0.0.0/0) and select the Internet gateway you created. After checking the contents, click [Save changes].

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	Internet Gateway	Active	No

Add route

Cancel Preview Save changes

- To connect subnets, click the “Subnet associations” tab and then click [Edit subnet associations].

rtb-0b3ed86a27ace6356 / dev2-public-rt

Details Info

Route table ID rtb-0b3ed86a27ace6356	Main No	Explicit subnet associations subnet-0574572872204c3ab / dev2-pub1	Edge associations -
VPC vpc-009d50859c77947f2 dev2-vpc	Owner ID 340108855584		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Explicit subnet associations (1) Edit subnet associations

Find subnet association

- Select the subnets you want to connect to and click [Save associations].

Available subnets (1/1)

Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
dev2-pub1	subnet-010312279e66...	10.0.1.0/24	-	Main (rtb-0b3ed86a27ace6356)

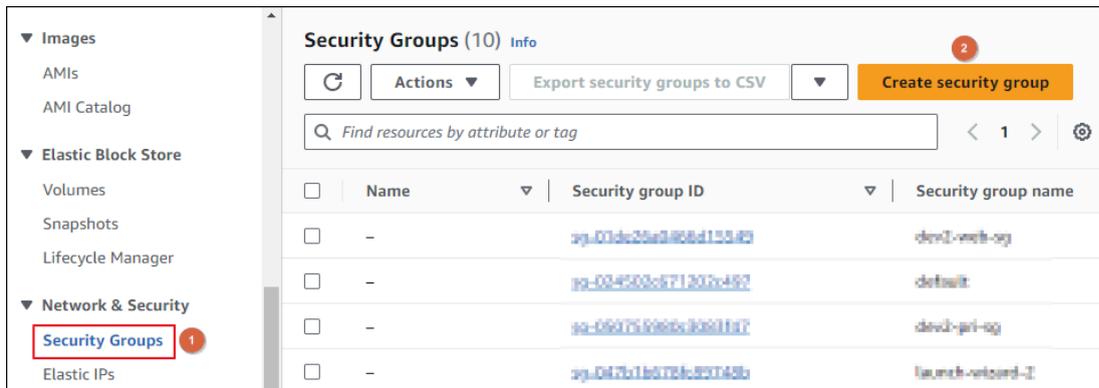
Selected subnets

subnet-010312279e66... / dev2-pub1

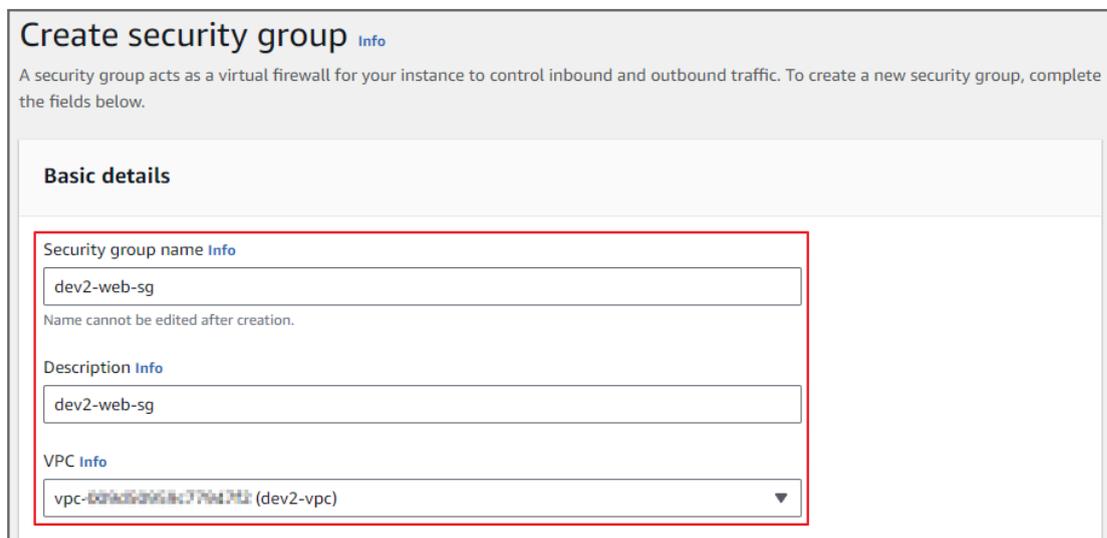
Cancel Save associations

3.1.5 Create security groups

1. Access the AWS EC2 Management Console.
2. On the left menu, click “Security Groups” and then click [Create security group].



3. Enter a security group name, description, and select a VPC.



4. Add inbound rules and outbound rules by referring to the table below.

[Inbound rules]

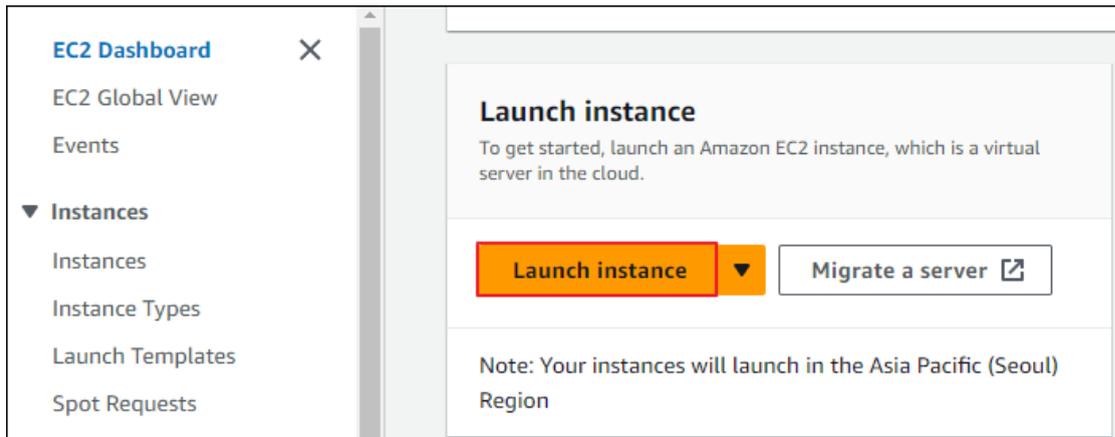
Type	Protocol	Port range	Source
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0
All ICMP - IPv4	ICMP	All	0.0.0.0/0

[Outbound rules]

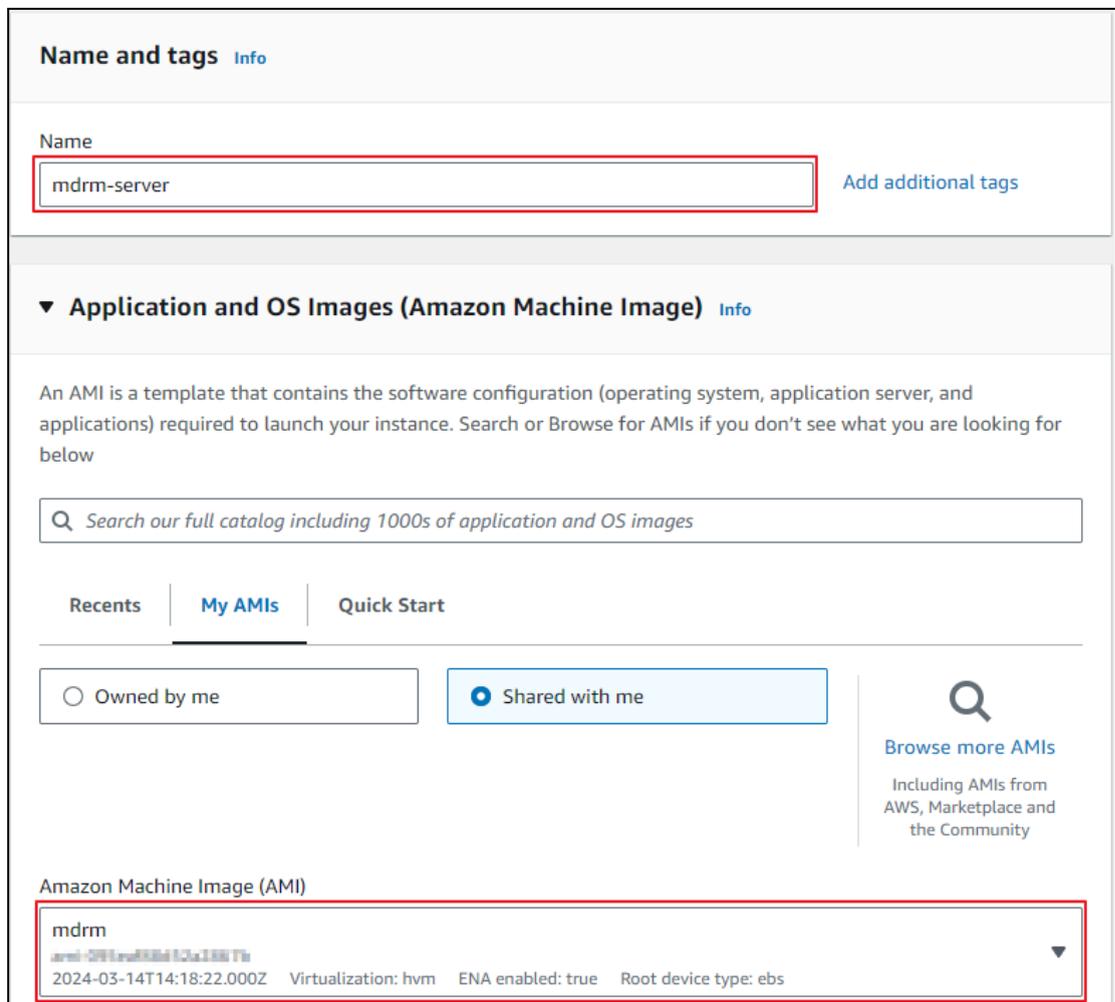
Type	Protocol	Port range	Source
All traffic	All	All	0.0.0.0/0

3.1.6 Create an instance

1. On the EC2 dashboard, click [Launch instance].



2. Enter an instance name and select the 'MDRM' AMI shared through AWS Marketplace.



- Select the instance type considering the size of the system (node) to be operated. (“Requirements” reference)

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

Instance type

c5.2xlarge

Family: c5 8 vCPU 16 GiB Memory Current generation: true

On-Demand Linux base pricing: 0.384 USD per Hour

On-Demand RHEL base pricing: 0.514 USD per Hour

On-Demand Windows base pricing: 0.752 USD per Hour

On-Demand SUSE base pricing: 0.484 USD per Hour

Additional costs apply for AMIs with pre-installed software

All generations

[Compare instance types](#)

- Create or select the key pair for administrator to use.

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

AWS_MDRM_jhyoo

[Create new key pair](#)

- Click [Edit] in the network settings and select the VPC, Subnet, and Security group created earlier.

▼ Network settings [Info](#)

VPC - *required* | [Info](#)

vpc-009d50959c77947f2 (dev2-vpc)

10.0.0.0/16

[Refresh](#)

Subnet | [Info](#)

subnet-057457287f320fcdab dev2-pub1

VPC: vpc-009d50959c77947f2 Owner: 340103855584

Availability Zone: ap-northeast-2a IP addresses available: 247 CIDR: 10.0.1.0/24

[Refresh](#) [Create new subnet](#)

Auto-assign public IP | [Info](#)

Enable

Firewall (security groups) | [Info](#)

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

Create security group

Select existing security group

Common security groups [Info](#)

Select security groups

dev2-web-sg sg-012e28e0a86c7106d8 X

VPC: vpc-009d50959c77947f2

[Refresh](#) [Compare security group rules](#)

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

[▶ Advanced network configuration](#)

- Set up your storage, and click [Launch instance]. (“[Requirements](#)” reference)

The screenshot shows the 'Configure storage' section of the AWS console. The 'Root volume' is configured as 1x 200 GiB gp3 (Not encrypted). A notification states: 'Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage'. On the right, a 'Storage (volumes)' summary shows '1 volume(s) - 200 GiB'. A 'Free tier' notification is also present. At the bottom right, the 'Launch instance' button is highlighted in orange, with a 'Review commands' link below it.

3.1.7 Elastic IP settings

Set up Elastic IP (EIP) to set a static IP for the instance (MDRM server) created earlier.

※ EIPs come standard with up to 5 per account, but you may be charged if you don't use them after they're allocated.

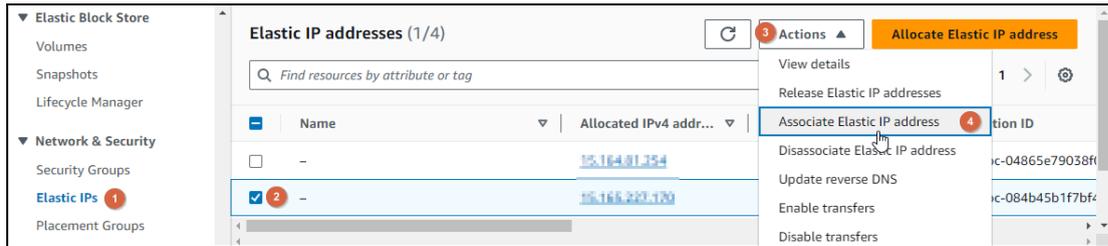
- On the left menu of the EC2 screen, click “Elastic IPs” and then click [Allocate Elastic IP address].

The screenshot shows the 'Elastic IP addresses' page in the AWS console. The left-hand navigation menu has 'Elastic IPs' highlighted in a red box. The main content area shows a table with one entry: a Public IP. An 'Allocate Elastic IP address' button is highlighted in orange at the top right.

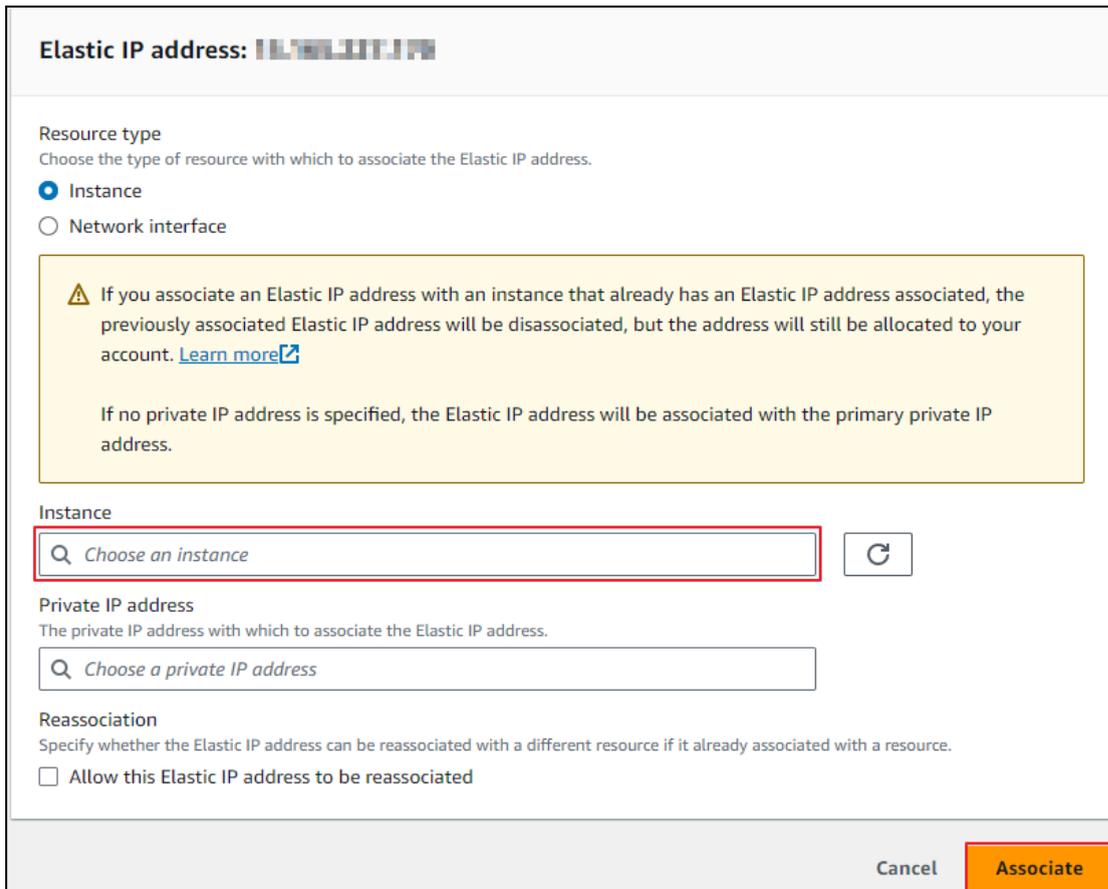
- Click the [Allocate] button at the bottom.
- Click “Instances” in the left menu and stop the MDRM EC2 instance. At this time, confirm that the “Status check” of the instance is “2/2 checks passed”, right-click on the instance, and click “Stop instance.”

The screenshot shows the 'Instances' page in the AWS console. The instance 'mdrm-server' is selected and highlighted in blue. A context menu is open over it, with 'Stop instance' highlighted in a red box. The 'Status check' column for this instance shows '2/2 checks passed'. Other instances listed include 'Win2016DC_1_A', 'mdrm-agent_L47', 'mdrm-agent_L248', and 'mdrm-agent_W254'.

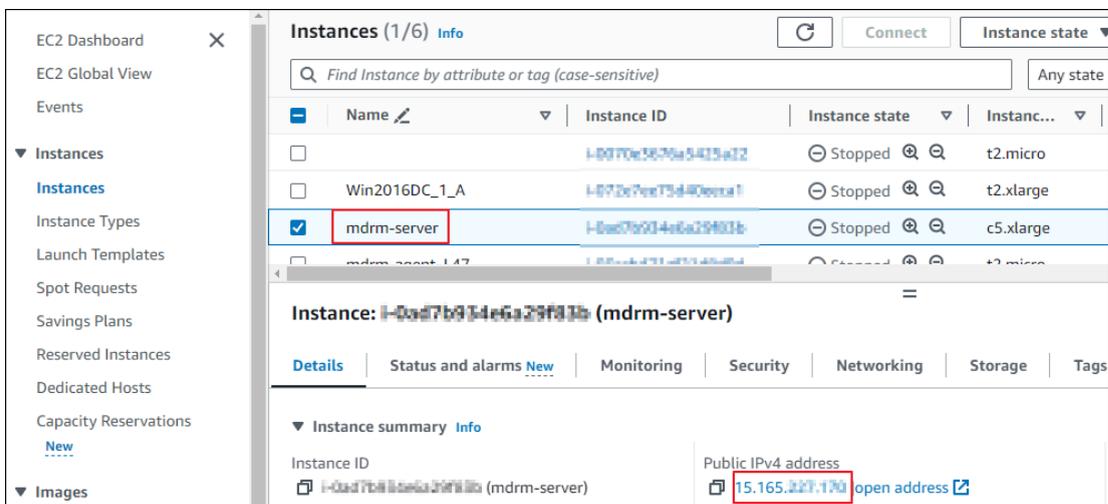
- On the "Elastic IPs" screen, select the IP you want to associate with and click [Actions] > [Associate Elastic IP address].



- Select the instance to connect to and click [Associate].



Verify that the instance's Public IPv4 address is set to EIP.



3.2 Install MDRM

To install MDRM, you need the container management tools Docker and Docker Compose (or Podman and Podman Compose). The MDRM EC2 instance has Docker and docker-compose installed and includes the MDRM installation package.

Below are the steps to install MDRM.

1. Connect to MDRM EC2 instance

Connect to the MDRM EC2 instance using the ssh command as follows.

On your first connection, enter "yes" to the "Are you sure you want to continue connecting (yes/no/[fingerprint])?" question.

```
# ssh -i "YourKey.pem" ec2-user@your-instance-ip/dns
ex)
ssh -i "AWS_MDRM_jhyoo.pem"
ec2-user@ec2-15-123-222-111.ap-northeast-2.compute.amazonaws.com

root@main:/home/aws# ll
total 12
drwxr-xr-x 2 root root 4096 Mar 11 08:35 ./
drwxr-xr-x 4 root root 4096 Jan 26 07:34 ../
-rw-r--r-- 1 root root 1678 Jan 23 08:39 AWS_MDRM_jhyoo.pem
root@main:/home/aws# ssh -i "AWS_MDRM_jhyoo.pem" ec2-user@ec2-15-165-186-77.ap-northeast-2.compute.amazonaws.com
The authenticity of host 'ec2-15-165-186-77.ap-northeast-2.compute.amazonaws.com (15.165.186.77)' can't be established.
ED25519 key fingerprint is SHA256:ogfk2hCmn2xyS6Gkgf2HRDsytdnJlC281/yCPrW3218.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-15-165-186-77.ap-northeast-2.compute.amazonaws.com' (ED25519) to the list of known hosts.

#####
          Amazon Linux 2023
#####
          https://aws.amazon.com/linux/amazon-linux-2023
#####
V..!
#####

[ec2-user@ip-10-0-1-56 ~]$
```

2. Check whether Docker & Docker-compose is installed and the MDRM installation file

Check the docker and docker-compose versions, and check the MDRM installation file.

```
# Check docker version
docker version

# Check docker-compose version
docker-compose version

# Check MDRM installation package file (mdrm4624.tar.gz)
ll /opt

[ec2-user@ip-10-0-1-16 opt]$ ll /opt
total 4204420
-rwxr-xr-x. 1 ec2-user ec2-user 4305323091 Jan 29 03:43 mdrm4624.tar.gz
```

3. Unzip the installation files (mdrm4624.tar.gz)

Unzip the installation file into the installation directory and move to the created mdrm4624 directory. Depending on your system specifications, this may take several minutes or longer.

```
# Example (when installed in /opt)
cd /opt/
sudo tar -zxvf mdrm4624.tar.gz
...
cd /opt/mdrm4624
```

4. Run install.sh file

Run install.sh with **hostname** and **volume directory** as arguments.

The installation will take about 10 minutes to complete.

```
# example (hostname: mdrm.mantech.co.kr, volume directory absolute path: /opt/gam)
sudo ./install.sh mdrm.mantech.co.kr /opt/gam
```

Argument 1) hostname: Enter the hostname of the MDRM server ('gam' container).

The entered hostname is automatically entered as the hostname value of the gam service in the docker-compose.yml file. This is the same as the -h option value of the docker run command.

Argument 2) volume directory: The mount target directory, enter an absolute path.

The paths you enter are automatically populated into the "volumes:" of the gam, mdrm-postgres, and alert-controller services in the docker-compose.yml file and mapped to the config and DB file paths.

5. Check if installed

Access the MDRM web console and check whether it has been installed properly.

```
https://<MDRM server IP address>
Example) https://10.20.30.40
```

[Reference command]

The following are frequently used commands when managing containers.

Run the docker-compose command from where the docker-compose.yml file is located.

```
# Check progress log in real time (e.g. gam container)
docker logs -f gam

# GAM container connection
docker exec -it gam bash

# Create and run the entire container (similar to docker run)
docker-compose up -d

# Stop and remove the entire container
docker-compose down

# Stop and run the entire container
docker-compose stop
docker-compose start

# Restart entire container
docker-compose restart

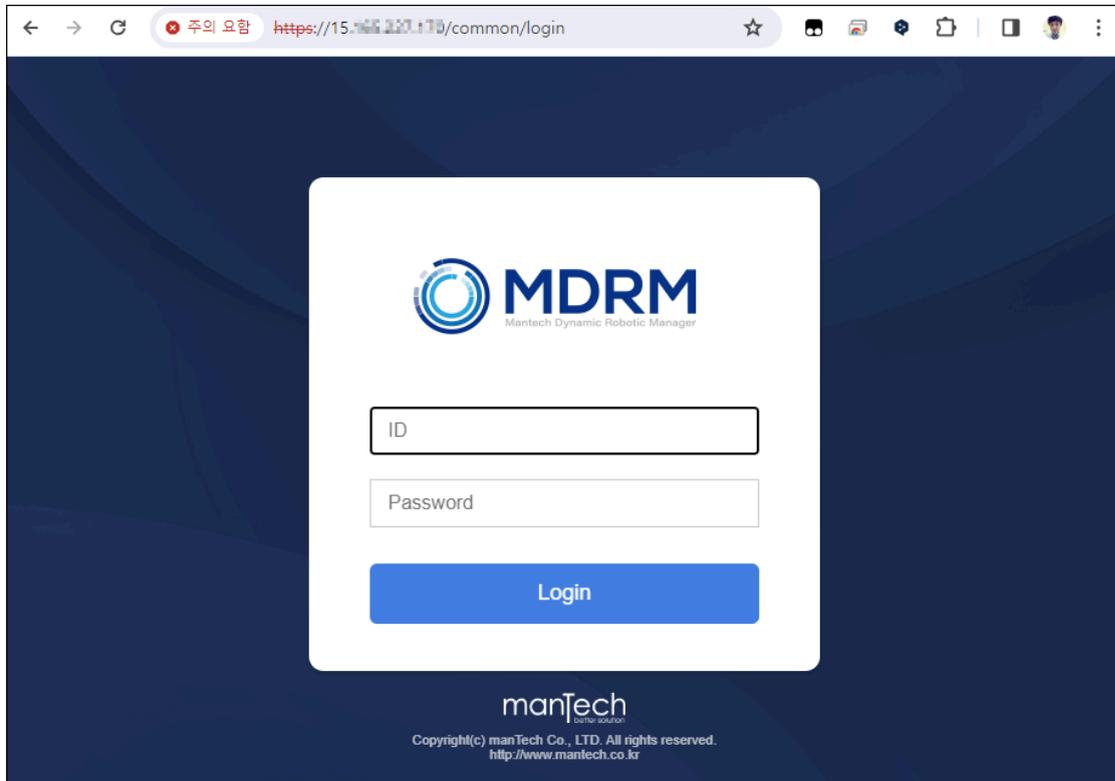
# Delete unused images
docker image prune -a
```

4. System Administration

4.1 Login

1. To access the console, enter the IP address or domain address of the server where MDRM is installed in the address field of your web browser. Use the domain address after registering it on the DNS server.

Example) <https://10.20.30.40> or <https://mdrm.mantech.co.kr>



2. Enter the basic administrator account information below and click the [Login] button.
 - ID: mcuser
 - Password: mdrm

[For first login]

If this is your first time logging in using the account you entered, the 'Change Password' screen will appear.

Enter the 'Current Password', enter 4 to 20 English letters or numbers in the 'New Password' and 'Confirm New Password' fields, and then click the [Change] button.

[Change password every 90 days]

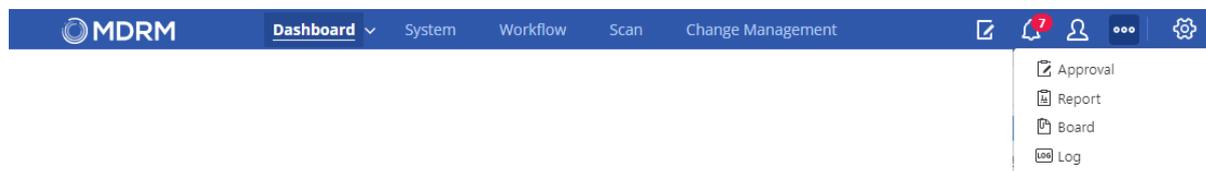
You must change your password periodically, every 90 days. If you do not change your password for 90 days, the password change screen will appear when you log in.

If you want to keep your existing password, click "Change later" under the [Change] button.

4.2 Main menu

This briefly introduces the main menu and main functions of the management console.

4.2.1 Menu bar



Menu	Explanation
Dashboard	Monitor management resources by configuring a dashboard with the widgets of your choice.
System	Monitor and manage IT resources such as servers, storage, and networks.
Workflow	Automate various work processes by defining various scripts required for IT operations in the form of a workflow.
Scan	Automate repetitive inspection tasks by defining daily inspection targets and inspection items.
Change Management	If you operate two MDRM servers (main center + DR center), you can manage changes in system components between both centers.
Approval	Provides an approval process for locked workflows or inspection tasks.
Report	Issue reports on changes to system configuration information and the execution results of inspection tasks.
Board	Like a bulletin board, create and share posts including text or files.
Log	Check logs generated by MDRM on the console screen.
Alarm	Check various notification information that occurs during MDRM operation.
My Page	Manage the profiles and notification settings of connected users.
Settings	Perform various settings required to operate the MDRM server, from dashboard settings to version checking.

4.2.2 Dashboard

You can configure desired widgets for each user to create various dashboards and monitor management resources. Dashboards can be created in the “Settings > Dashboard Settings” screen.

The screenshot shows the MDRM Dashboard with a navigation menu at the top. A dropdown menu is open under 'Dashboard', listing options: dashboard (default), Drill, Scan, Linux, Windows, and IPL. The main dashboard area contains several widgets:

- Time Recorder:** Shows 'Drill' with a start time of 11:55 on 2024/03/12 and an elapsed time of 10 minutes.
- System Connection Status:** Shows a table with columns for System, Access, and a status indicator (Failed).
- Scan Results:** Shows a table with columns for Server, IP Address, Fail, Error, and Pass. One server, EC2_AL1, is listed with 0 fails, 1 error, and 3 passes.
- Workflow Progress Multiple Chart:** Displays two progress charts: '(2/3) Linux check' at 100% and '(1/5) Windows check' at 59%.
- Running Workflows List:** A table showing workflow counts and status.

Category	Count	Ready	Running	Completed	Failed
Linux	1	0	0	0	1
Windows	1	0	1	0	0
Total	2	0	1	0	1

Category	Workflow	Start Time	Elapsed Time	Responsibility
Linux	Linux check	15:39:21	00:00:37	-
Windows	Windows check	15:39:16	06:24:35	-

4.2.3 System

You can register with MDRM for integrated management of various IT resources such as servers, storage, and networks.

The screenshot shows the MDRM System interface. The 'System Status' section displays a summary of resources:

- Server (5):** 2 OK, 1 Warning, 1 Error, 1 Unknown.
- Storage (3):** 1 OK, 1 Warning, 1 Error, 0 Unknown.
- Network (3):** 1 OK, 1 Warning, 1 Error, 0 Unknown.

Below the summary, specific resources are listed: RHEL 6.6, Cent 7.4, ERP, Docs, and EMS.

4.2.4 Workflow

You can standardize and automate various work processes by defining the scripts required for IT operations in the form of a workflow.

The screenshot shows the MDRM Workflow interface. The 'Workflow (4)' section lists the following workflows:

Workflow Name	Description	RTO	Status	Responsibility	Last Modified	Last Executed
Linux check		00:00:31	Failed		2024-03-12	2024-03-12 15:39:21
Windows check	Windows server checking	00:01:01	Running	administrator	2024-03-12	2024-03-12 22:31:37

A detailed view of a workflow diagram is shown below, illustrating a process flow starting from 'START', passing through 'WIN2012R2 HA group ch...', 'GAM Merge var', and a 'Decision' point, leading to 'senario1', 'senario2', and 'senario3'.

4.2.5 Scan

You can automate repetitive tasks such as daily inspections by defining tasks to perform inspection items on the system being inspected and executing the inspections periodically.

The screenshot displays the 'Datacenter' dashboard for a scan. The top section shows a summary with a pass rate of 38%, 2 scans, 2 jobs, 2 systems, and 0 running tasks. Below this, a table shows scan results for two jobs: 'Linux Daily Check > Basic scan' (0 Fail, 1 Error, 3 Pass) and 'Windows Daily Check > Basic scan' (0 Fail, 4 Error, 0 Pass). To the right, a detailed view for the 'Linux Daily Check > Basic scan' shows 1 error and 3 passes for server EC2_AL1, including items like CPU Check, Disk Check, OS 확인, and 네트워크 포트 확인.

Scan > Job	Scan Results		
	Fail	Error	Pass
Linux Daily Check > Basic scan	0	1	3
Windows Daily Check > Basic scan	0	4	0

4.2.6 Settings

You can perform various settings required to operate the MDRM server, from dashboard settings to version checking.

The screenshot shows the 'Dashboard Settings' page. It includes a sidebar with navigation options like Monitoring Plugins, System Summary, Workflow Component, Scan, Users and User Groups, Roles and Permissions, Alarm, Data Usage, Hypervisor, Schedule, Board, Deployment Product, Logo Settings, License, and Version. The main content area is titled 'Dashboard Settings' and features a 'dashboard (default)' dropdown, 'Share Dashboard' button, and options to 'Adjust Widget Height', 'Import Widget', and 'Add Widget'. The 'Top Field' is currently empty. Below, there are several widget configuration sections: 'Time Recorder' with a table of Name, Running Type, and Delete; 'System Connection Status' with a table of System, Count, Success, and Failed; 'Scan Results' with a table of System, Count, Success, and Failed; 'Workflow Progress Multiple Chart' with a table of Workflow Name and Delete; and 'Running Workflows List' with a table of Category, Count, and Delete.

4.3 License management

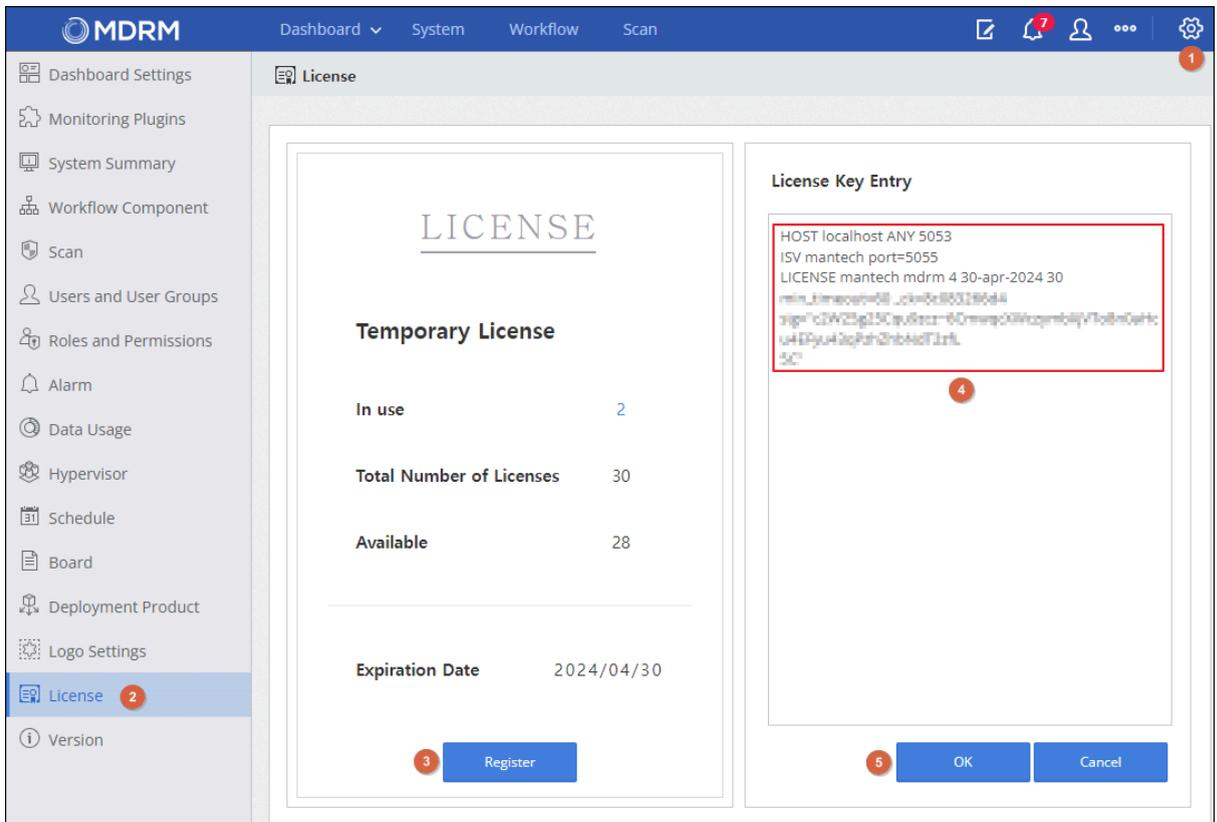
4.3.1 License type

MDRM licenses come in two types and generally have the following characteristics:

Category	Characteristic
Temporary license	<ul style="list-style-type: none">• Can be used until expiration date (approximately 3 months after issuance)• Up to 30 MDRM agents can be registered• Available on all MDRM servers
Permanent license	<ul style="list-style-type: none">• Available indefinitely• MDRM agents can be registered up to the number set at the time of issuance• Validity determined by the host name of the MDRM server to be used

4.3.2 How to set up a license

1. After accessing the MDRM management console, click the Settings button ().
2. Click “License” in the left menu.
3. Click the [Register] button, enter your license key, and click the [OK] button.



The screenshot shows the MDRM management console interface. The top navigation bar includes 'Dashboard', 'System', 'Workflow', and 'Scan'. The left sidebar lists various settings and monitoring options, with 'License' highlighted. The main content area is titled 'License' and features a 'Temporary License' section with the following data:

Category	Value
In use	2
Total Number of Licenses	30
Available	28
Expiration Date	2024/04/30

Below the statistics is a 'Register' button. To the right is the 'License Key Entry' section, which contains a text area with the following license key:

```
HOST localhost ANY 5053
ISV mantech port=5055
LICENSE mantech mdrm 4 30-apr-2024 30
min_timecat=08 ...
sig=c2W23g15CpU8tcc=60mmp0XWozym0jV70b0D0h0
u44Fyu40qPah2hb0dF1zrl
5C
```

Below the text area are 'OK' and 'Cancel' buttons.

4.4 Version upgrade

Version upgrades work as follows:

1. Backup files to be preserved (data areas, custom monitoring plugins, etc.)
2. Stop and remove existing docker containers
3. Stop and remove existing docker image
4. Remove or move existing files excluding data area
5. Deploy a new version of a container (same as a new install)

5. Support

5.1 Technical support

The scope of technical support includes:

- Product installation support (installation and usage manual provided)
- Automation and management target server agent installation
- Task analysis, script verification and creation
- Establishment of inspection work/automation workflow/distribution work
- Creating an integrated management dashboard (apply multiple dashboards for each user)
- RTO definition and result report for each task stage
- Support for work changes and modifications
- Support for mock training twice a year

Technical inquiry

- E-mail: cs@mantech.co.kr
- Web page: <https://www.mantech.co.kr/inquiry>

5.2 Support costs

Technical support is provided pursuant to the license agreement.

5.3 SLA

SLAs are provided pursuant to a license agreement.