

Workflow Based **IT Automation solution**



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]

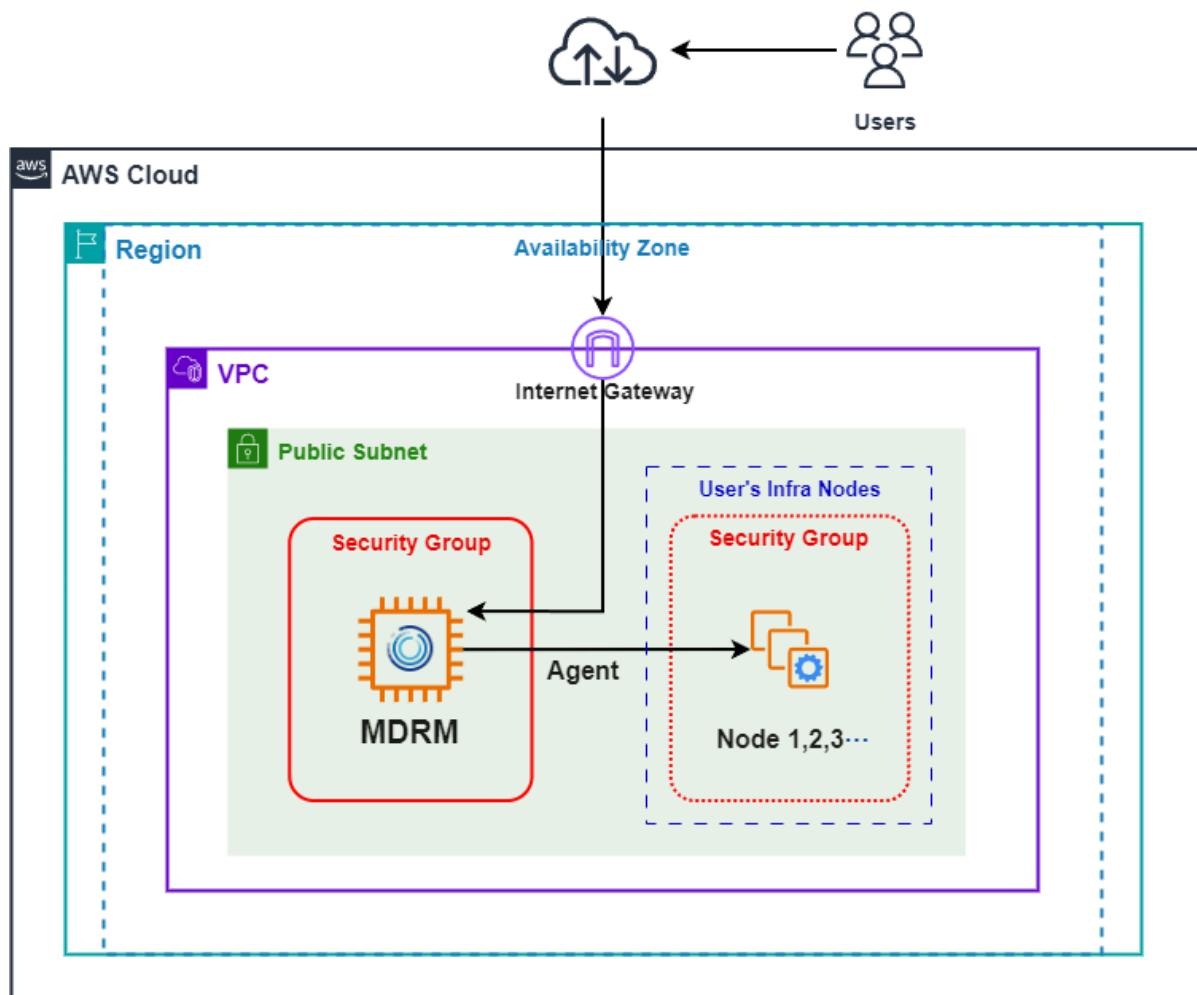
Resource	Less than 50 servers	Less than 100 servers	Less than 500 servers
vCPU	- 2.0GHz 64bit or higher - Total of at least 8 cores	- 2.0GHz 64bit or higher - Total of at least 16 cores	- 2.0GHz 64bit or higher - Total of at least 24 cores
Memory	16 GiB or more	24 GiB or more	32 GiB or more
Disk	200 GB or more	500 GB or more	800 GB or more

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_jrn3
- <https://youtu.be/wgcograNVts?si=aP4ki3aIf-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

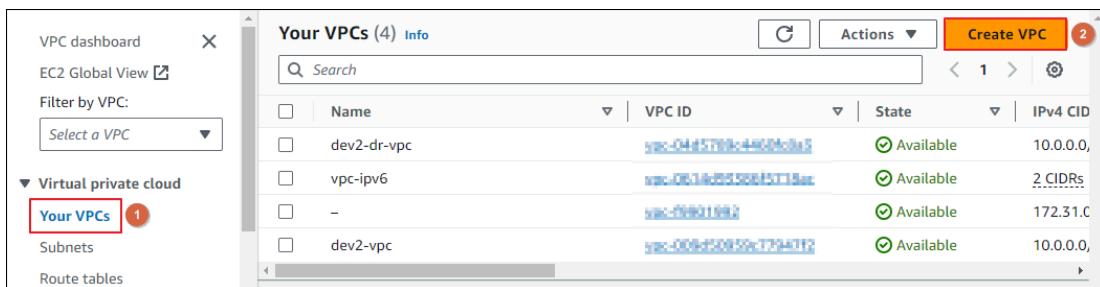
1. Prepare the network environment ("Pre-tasks" reference)
2. Create EC2 Instance with the provided AMI
3. Install MDRM (run install.sh)

3.1 Pre-tasks

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

3.1.1 Create VPCs

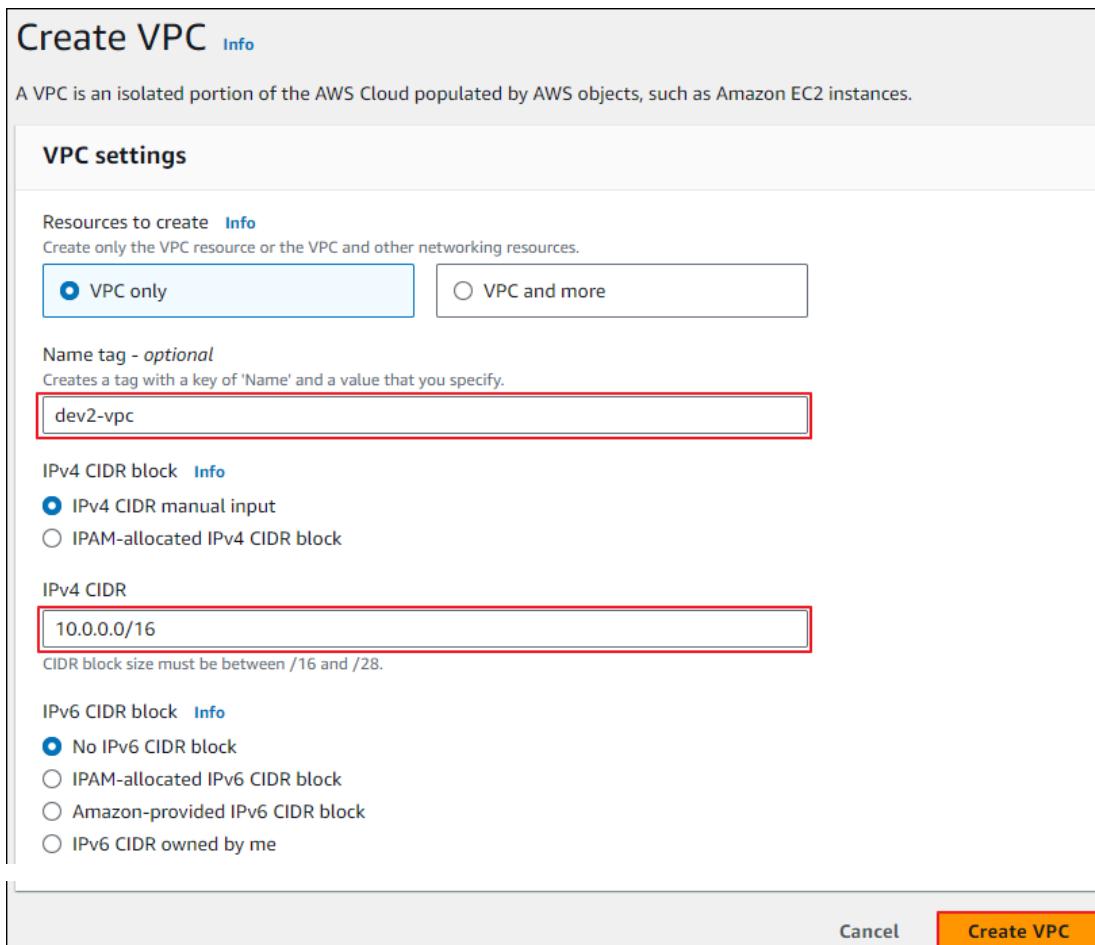
1. In the VPC dashboard, select "Your VPCs" and click [Create VPC].



The screenshot shows the AWS VPC dashboard with the 'Your VPCs' section selected. The table lists four existing VPCs: 'dev2-dr-vpc', 'vpc-ipv6', a unnamed VPC, and 'dev2-vpc'. The 'Create VPC' button is located at the top right of the table.

Name	VPC ID	State	IPv4 CIDR
dev2-dr-vpc	vpc-04d5770a446040a5	Available	10.0.0.0/16
vpc-ipv6	vpc-061a689558845318a	Available	2.0.0.0/16
-	vpc-09801982	Available	172.31.0.0/16
dev2-vpc	vpc-009ef30959c7794012	Available	10.0.0.0/16

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



The screenshot shows the 'Create VPC' wizard in the 'VPC settings' step. The 'Name tag - optional' field is set to 'dev2-vpc'. The 'IPv4 CIDR block' field is set to '10.0.0.0/16'. The 'IPv6 CIDR block' section shows 'No IPv6 CIDR block' selected. The 'Create VPC' button is located at the bottom right.

VPC settings

Resources to create [Info](#)
Create only the VPC resource or the VPC and other networking resources.

VPC only VPC and more

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

dev2-vpc

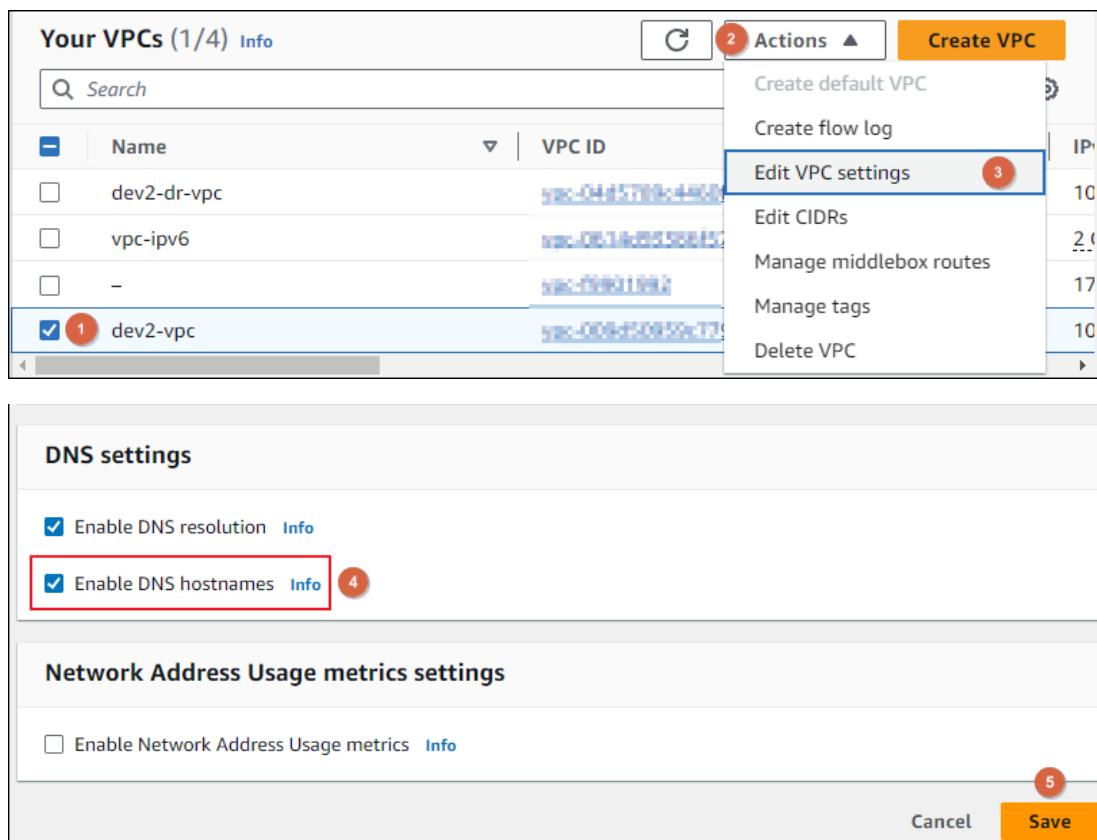
IPv4 CIDR block [Info](#)
 IPv4 CIDR manual input IPAM-allocated IPv4 CIDR block

10.0.0.0/16

IPv6 CIDR block [Info](#)
 No IPv6 CIDR block IPAM-allocated IPv6 CIDR block Amazon-provided IPv6 CIDR block IPv6 CIDR owned by me

Cancel **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.



The screenshot shows the 'Your VPCs (1/4)' list and the 'Edit VPC settings' dialog for the selected 'dev2-vpc'.

Actions menu (Step 3):

- Create default VPC
- Create flow log
- Edit VPC settings** (highlighted with a red box and step 3)
- Edit CIDRs
- Manage middlebox routes
- Manage tags
- Delete VPC

DNS settings (Step 4):

- Enable DNS resolution
- Enable DNS hostnames** (highlighted with a red box and step 4)

Network Address Usage metrics settings:

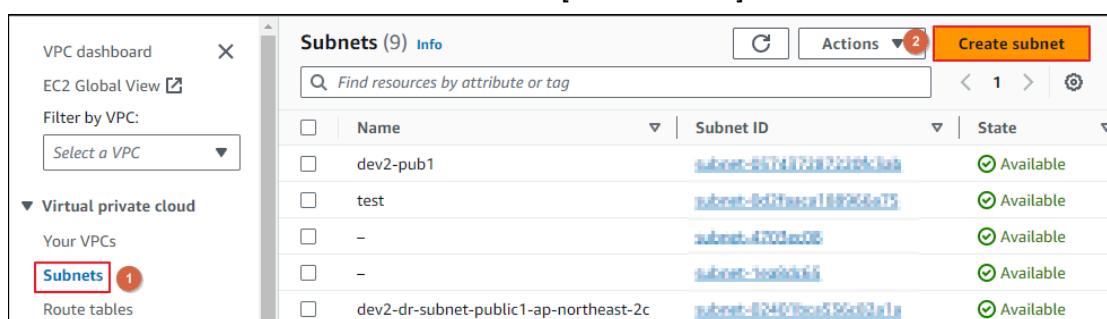
- Enable Network Address Usage metrics

Buttons:

- Cancel
- Save (highlighted with a red box and step 5)

3.1.2 Create subnets

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

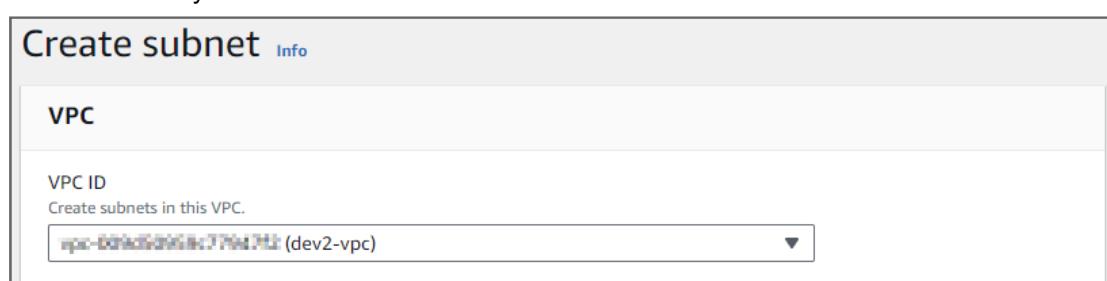


The screenshot shows the VPC dashboard with the 'Subnets' link highlighted in the left sidebar.

Subnets (9) List:

Name	Subnet ID	State
dev2-pub1	subnet-0371472172345678	Available
test	subnet-0d2f5eac11112345678	Available
-	subnet-02034ec00	Available
-	subnet-10a10a00	Available
dev2-dr-subnet-public1-ap-northeast-2c	subnet-024010a526c03a1a	Available

2. Select the VPC you created earlier.



The screenshot shows the 'Create subnet' wizard with the 'VPC' step selected.

VPC:

VPC ID: dev2-vpc

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 dev2-pub1
 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 Asia Pacific (Seoul) / ap-northeast-2c

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 10.0.0.0/16

IPv4 subnet CIDR block
 4 10.0.1.0/24 256 IPs
 < > ^ v

Tags - optional
 Key Value - optional
 Name dev2-pub1 Remove
 Add new tag
 You can add 49 more tags.
 Remove
 Add new subnet

5 Cancel **Create subnet**

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
igw-mdrm	igw-0211611112345678	Attached
dev2-dr-igw	igw-0000000000000000	Attached
-	igw-23456141	Attached

Create internet gateway 2

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.

Add new tag
You can add 50 more tags.

Cancel **Create internet gateway**

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

Name	Internet gateway ID	Actions
igw-mdrm	igw-0b2194a81a1127ec	View details
dev2-dr-igw	igw-8c1159222ee	Attach to VPC 3 Detach from VPC Manage tags Delete internet gateway
-	141	View details

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

Attach to VPC (igw-0b2194a81a1127ec) 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.

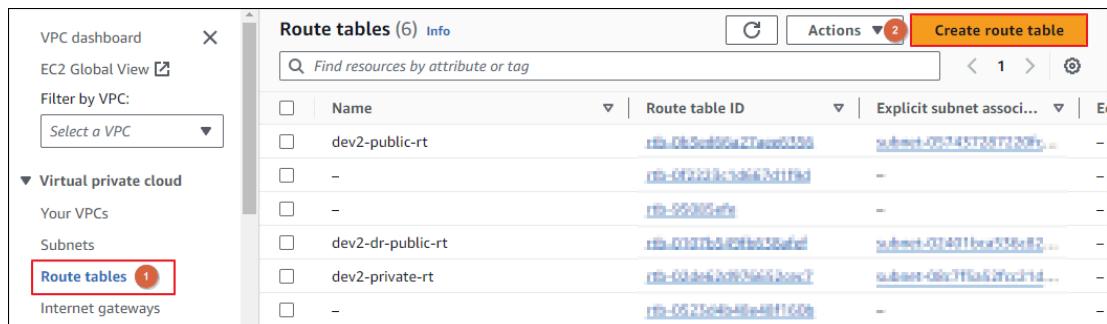
1

AWS Command Line Interface command

Cancel **Attach internet gateway**

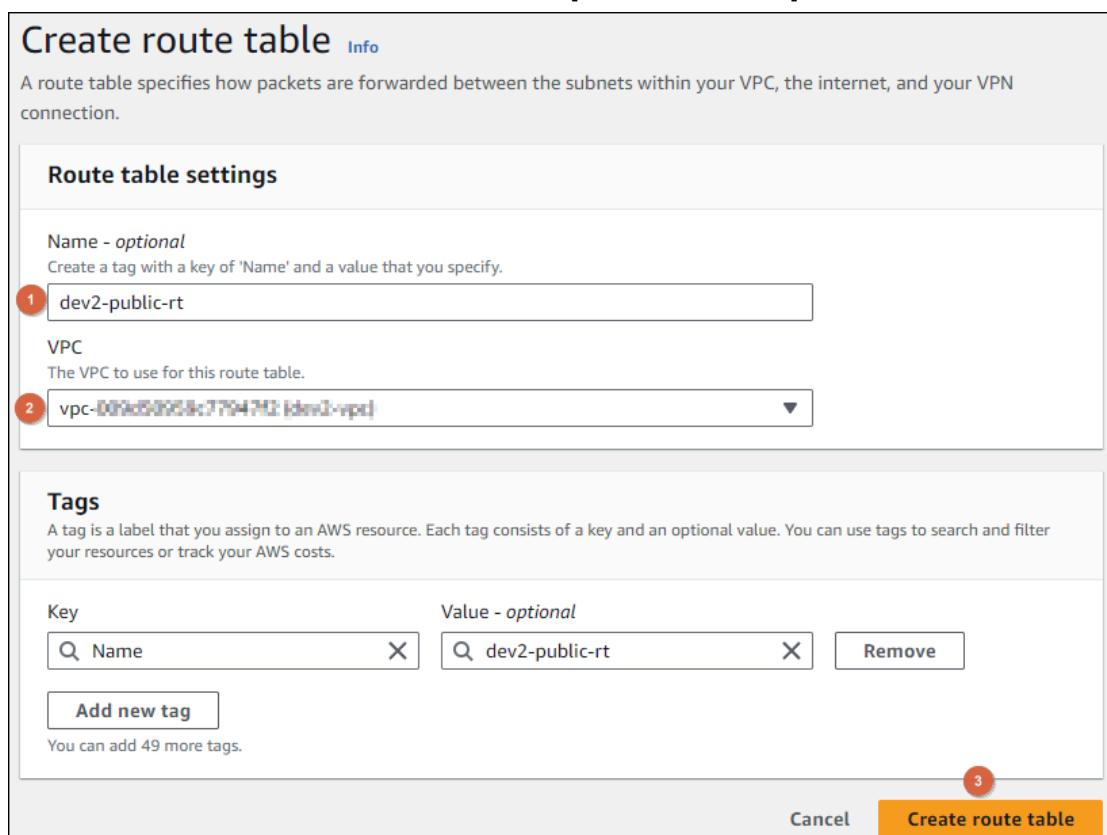
3.1.4 Routing table settings

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



Route tables (6) <small>Info</small>			
<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...
<input type="checkbox"/>	dev2-public-rt	rtb-0b5ec05a27a0e0350	subnet-031411bea538a82...
<input type="checkbox"/>	-	rtb-0f2213c3cd662d11fd	-
<input type="checkbox"/>	-	rtb-550005e7	-
<input type="checkbox"/>	dev2-dr-public-rt	rtb-0137b340fb038aef	subnet-031401bea538a82...
<input type="checkbox"/>	dev2-private-rt	rtb-034ed2d909a62a0c7	subnet-03a7f1a62f0c91d...
<input type="checkbox"/>	-	rtb-0523d45a46a48f160b	-

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



Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.

1 dev2-public-rt

VPC
The VPC to use for this route table.

2 **vpc-009d50958c77047f2 (dev2-vpc)**

Tags
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.

Key Value - optional

3 Name dev2-public-rt Remove

Add new tag

You can add 49 more tags.

Cancel Create route table

3. Click [Edit routes].

rtb-0b3ed66a27aee6356 / dev2-public-rt

Details [Info](#)

Route table ID rtb-0b3ed66a27aee6356	Main <input type="checkbox"/> No	Explicit subnet associations subnet-057437283722045ab / dev2-pub1	Edge associations -
VPC vpc-0094d10959c77347f12 dev2-vpc	Owner ID 340108000004		

Routes [Subnet associations](#) [Edge associations](#) [Route propagation](#) [Tags](#)

Routes (2)

Both < 1 > [Edit routes](#)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

4. 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 10.0.0.0/16	Target <input type="checkbox"/> local	Status Active	Propagated No
<input type="checkbox"/> 0.0.0.0/0	<input type="checkbox"/> Internet Gateway	Active	Remove

[Add route](#)

[Cancel](#) [Preview](#) [Save changes](#)

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

rtb-0b3ed66a27aee6356 / dev2-public-rt

Details [Info](#)

Route table ID rtb-0b3ed66a27aee6356	Main <input type="checkbox"/> No	Explicit subnet associations subnet-057437283722045ab / dev2-pub1	Edge associations -
VPC vpc-0094d10959c77347f12 dev2-vpc	Owner ID 340108000004		

Routes **Subnet associations** [Edge associations](#) [Route propagation](#) [Tags](#)

Explicit subnet associations (1)

[Edit subnet associations](#)

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

Available subnets (1/1)

[Filter subnet associations](#)

<input checked="" type="checkbox"/> Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/> 1 dev2-pub1	subnet-010312279e66...	10.0.1.0/24	-	Main (rtb-0b3ed66a27aee6356)

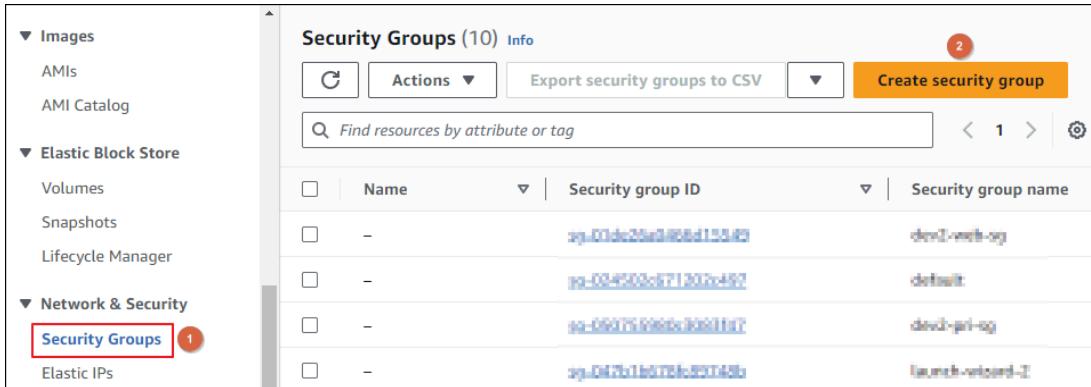
Selected subnets

[subnet-010312279e66... / dev2-pub1](#) [X](#)

[Cancel](#) [Save associations](#)

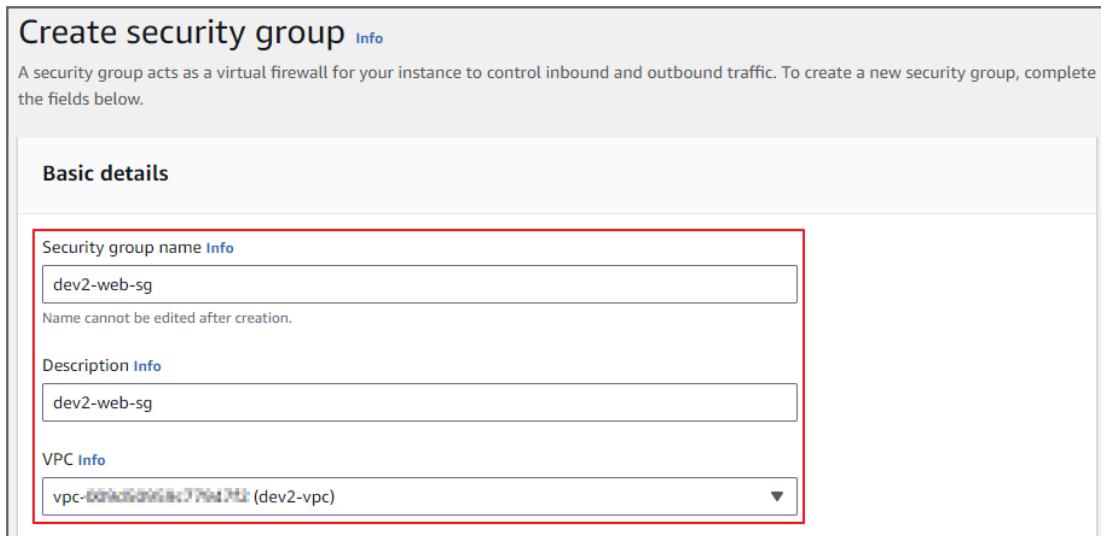
3.1.5 Create security groups

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



Security Groups (10) Info			
	Name	Security group ID	Security group name
<input type="checkbox"/>	-	sg-00dc20a3000d15540	dev2-web-sg
<input type="checkbox"/>	-	sg-004500c871302e400	default
<input type="checkbox"/>	-	sg-00075000000000000	dev2-priv-sg
<input type="checkbox"/>	-	sg-007b1b07780000000	Launch wizard-2

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



Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)
dev2-web-sg
Name cannot be edited after creation.

Description [Info](#)
dev2-web-sg

VPC [Info](#)
vpc-0000000000000000 (dev2-vpc)

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

[Inbound rules]

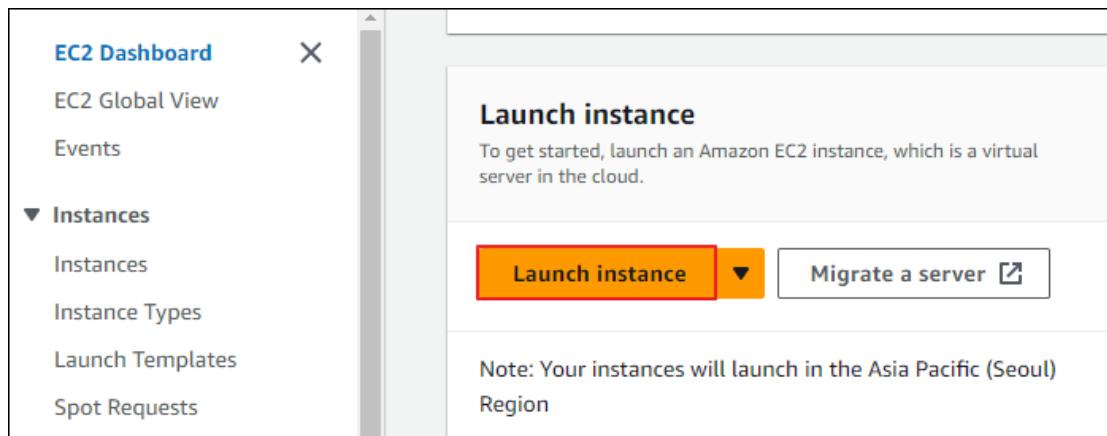
Type	Protocol	Port range	Source
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0
All ICMP - IPv4	ICMP	All	0.0.0.0/0

[Outbound rules]

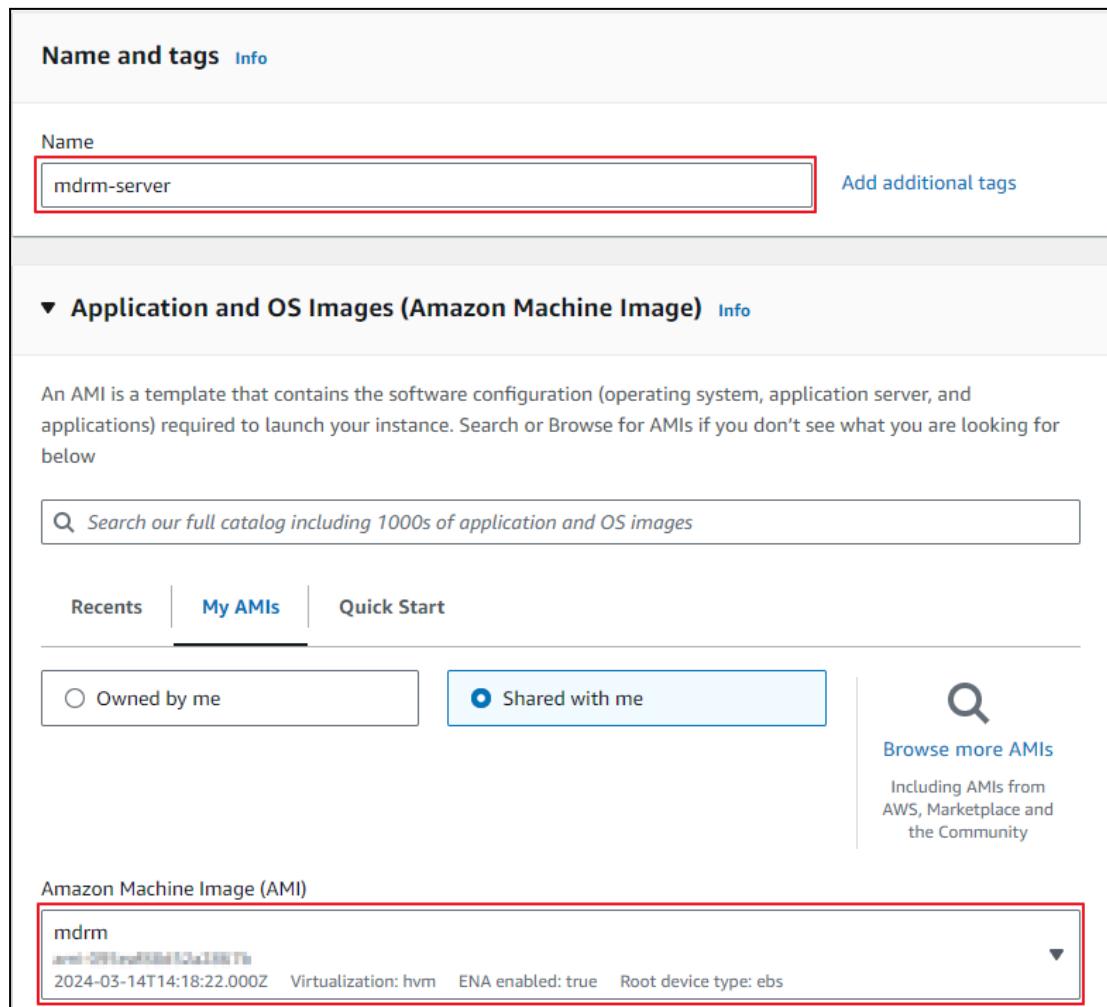
Type	Protocol	Port range	Source
All traffic	All	All	0.0.0.0/0

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.



3. Select the instance type considering the size of the system (node) to be operated.
("Requirements" reference)

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

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

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

Key pair (login)

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

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

Network settings

VPC - required

vpc-009d50959c77947f (dev2-vpc)

10.0.0.0/16

Subnet

subnet-052457287120f1ab dev2-pub1

VPC: vpc-009d50959c77947f Owner: 340103855584

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

Create new subnet

Auto-assign public IP

Enable

Firewall (security groups)

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

Select security groups

dev2-web-sg sg-0111111111111111 X

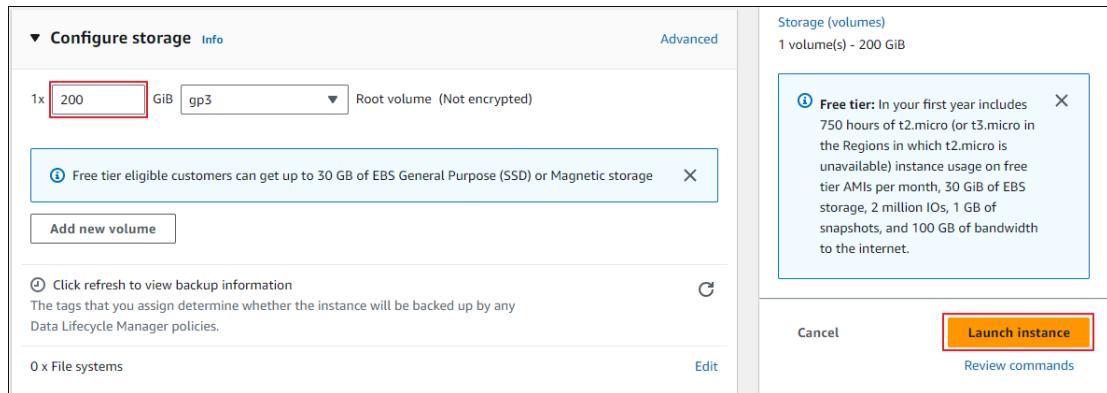
VPC: vpc-009d50959c77947f

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

6. Set up your storage, and click [Launch instance]. ("Requirements" reference)

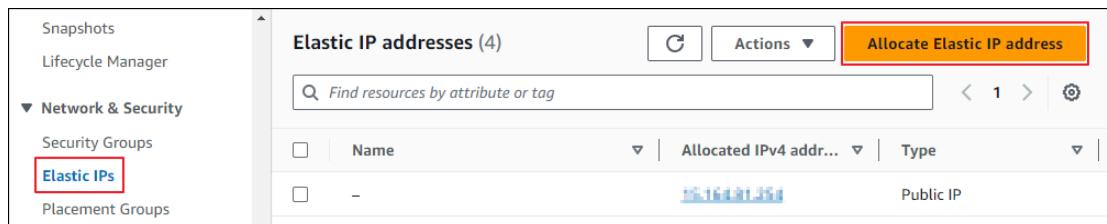


3.1.7 Elastic IP settings

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

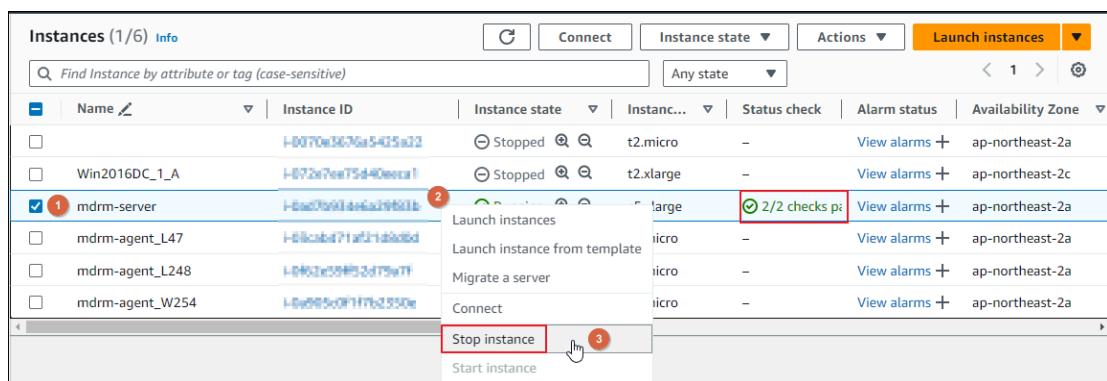
※ EIPs come standard with up to 5 per account, but you may be charged if you don't use them after they're allocated.

1. On the left menu of the EC2 screen, click "Elastic IPs" and then click [Allocate Elastic IP address].



2. Click the [Allocate] button at the bottom.
3. 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."



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

5. 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.

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 (mdrm4671.tar.gz)
```

3. Unzip the installation files (mdrm4671.tar.gz)

Unzip the installation file into the installation directory and move to the created mdrm4671 directory. Depending on your system specifications, this may take several minutes or longer.

```
# Example (when installed in /opt)
cd /opt/
sudo tar -zxfv mdrm4671.tar.gz
...
cd /opt/mdrm4671
```

4. Run `install.sh` file

Run `install.sh` with the `hostname`, `volume directory` and `port number` as input parameters. The installation will take about 10 minutes to complete.

```

# Default installation command
./install.sh <hostname> <volume_directory>

# Example 1) Default installation command
./install.sh mdrm.mantech.co.kr /opt/gam

# Example 2) To set the port number to 8443 during installation
./install.sh mdrm.mantech.co.kr /opt/gam 8443

```

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.

Argument 3) Port number(optional)

The port number is used to access the Management Server web console and to receive heartbeat data from GAM agents. Entering a port number is optional; if omitted, the default value of 443 is used.

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 podman 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

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>

The default administrator account is **mcuser**. The default password is generated as a temporary password during MDRM installation and is stored in the file **/gampkgs/bin/tmp_pw.txt** inside the GAM container. Follow the steps below to access the GAM container and check the temporary password in this file.

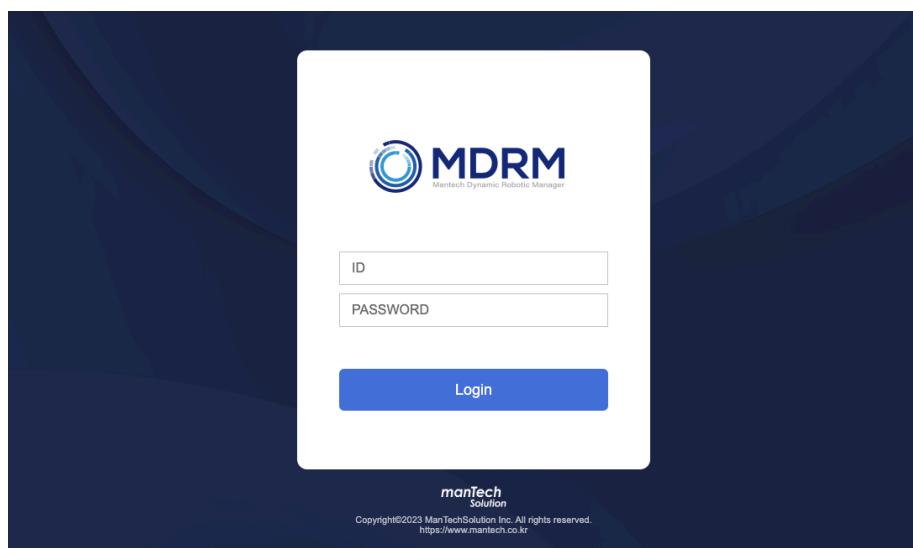
1. Access the GAM container

```
docker exec -it gam bash
```

2. Check the temporary password in the **/gampkgs/bin/tmp_pw.txt** file in the GAM container

```
# Example: 8"-@lwn7.
cat /gampkgs/bin/tmp_pw.txt
```

3. Login



- ID: mcuser

- Password: Enter temporary password

[First-Time Login]

If this is your first time logging in with the specified account, the Change Password screen will appear. Enter a password of 4 to 20 alphanumeric characters in the New Password and Confirm New Password fields, then click Submit.

[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.

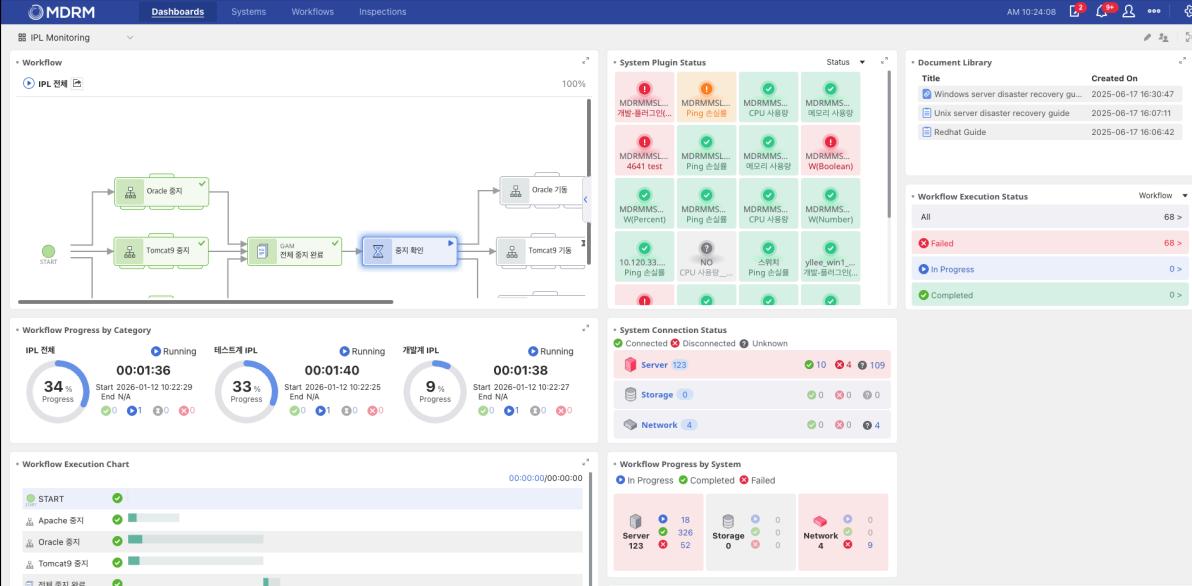
4.2.1 Menu bar



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.
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.

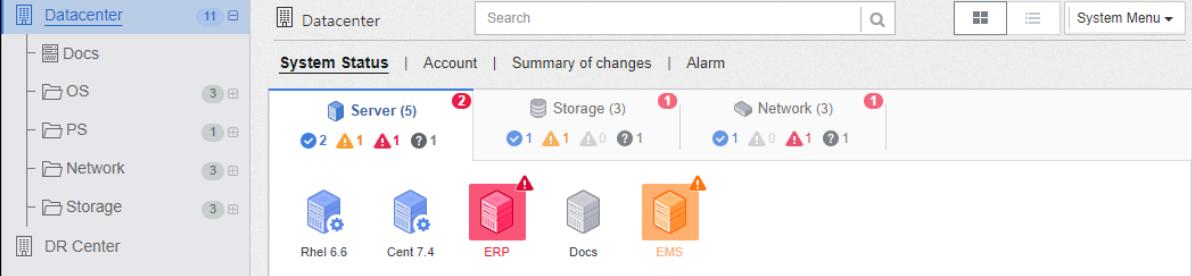


The screenshot displays a comprehensive MDRM dashboard with the following sections:

- Workflow:** Shows a workflow diagram for "IPL 전체" (IPL Full) with steps: START, Oracle 설치, Tomcat9 설치, 전체 설치 완료, 설치 확인, and Oracle 가동. Each step includes a progress bar and a status indicator.
- Workflow Progress by Category:** Three circular progress indicators for "IPL 전체" (34%), "테스트 IPL" (33%), and "개발자 IPL" (9%).
- Workflow Execution Chart:** A chart showing the execution status of tasks: START, Apache 설치, Oracle 설치, and Tomcat9 설치.
- System Plugin Status:** A grid of 16 status cards for various system metrics, with some showing red or yellow alerts.
- Document Library:** A list of documents with titles like "Windows server disaster recovery guide", "Unix server disaster recovery guide", and "Redhat Guide", along with their creation dates.
- Workflow Execution Status:** A table showing the status of workflows, with columns for "Workflow" and "Status".
- System Connection Status:** A summary of server, storage, and network connections.
- Workflow Progress by System:** A grid showing the progress of workflows across different system categories: Server, Storage, and Network.

4.2.3 System

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

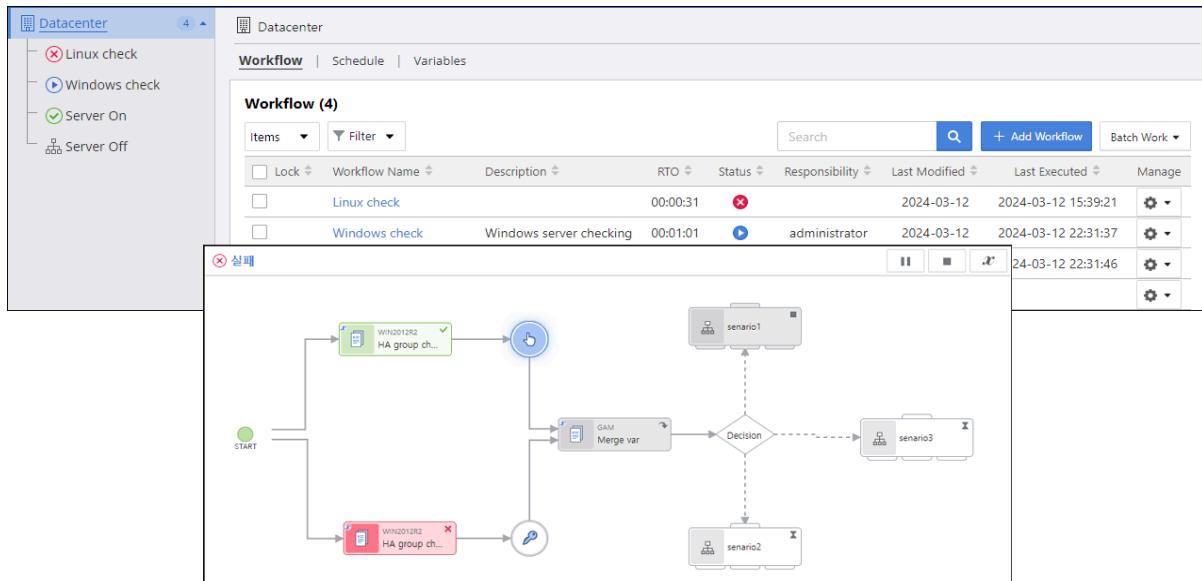


The screenshot shows the MDRM System Status page with the following interface:

- Left Sidebar:** A tree view of system categories: Datacenter, Docs, OS, PS, Network, Storage, and DR Center. Each category has a count of 11, 3, 1, 3, 3, 3, and 1 respectively.
- Header:** Includes a search bar, a system status summary (11), and a system menu.
- System Status Summary:** A grid showing the status of three main system components: Server (5), Storage (3), and Network (3). Each component has a count of 2, 1, and 1 respectively, with corresponding icons and status indicators.
- System Components:** A row of icons representing specific system components: RHEL 6.6, Cent 7.4, ERP, Docs, and EMS.

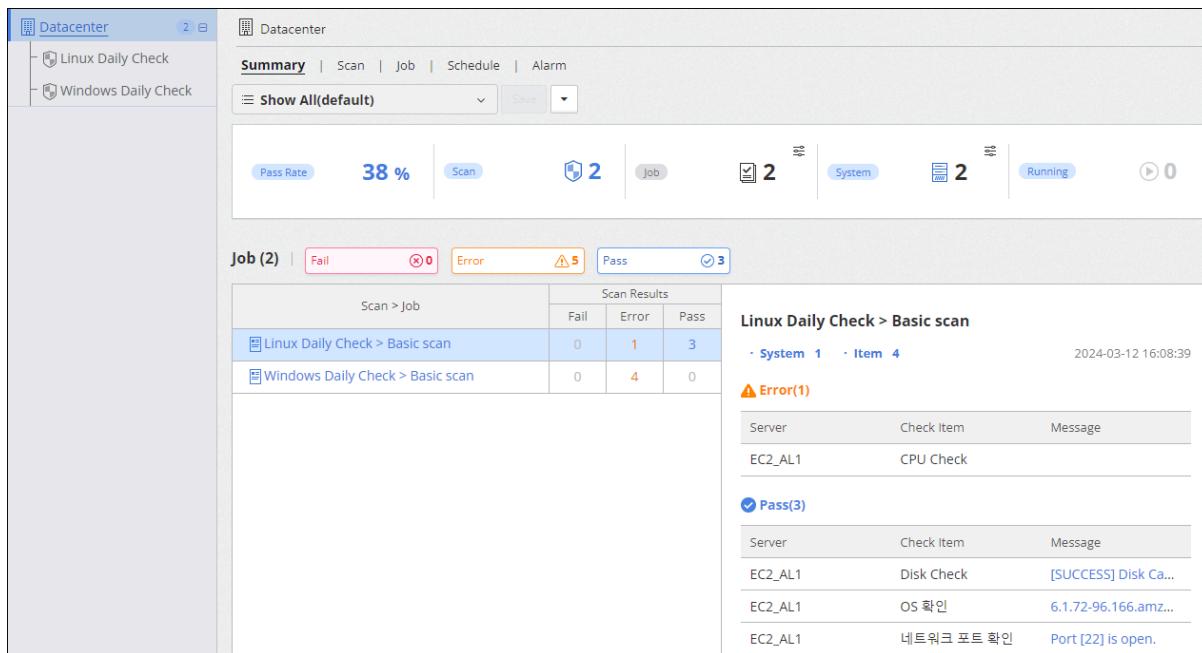
4.2.4 Workflow

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



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.



4.2.6 Settings

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

MDRM

Dashboard System Workflow Scan

PM 03:30:06

Workflow Component

Monitoring Plugins System Summary Scan

Users and User Groups Roles and Permissions Alarm Data Usage Hypervisor Schedule Board Deployment Product Logo Settings License Account Management Version

Component management | Image Management

Component Group

All (162)

Executive Command(162) | Filter ▾

Lock	Name	Description	Favorites	Type	History	Copy	Delete
<input type="checkbox"/>	Put files (GAM -> Agent)	Copies files from GAM to a remote node by using the agent.		v.1			
<input type="checkbox"/>	Pull files (Agent -> GAM)	Copies files from a remote node to GAM by using the agent.		v.1			
<input type="checkbox"/>	Run user defined script	User can write the script content and run it.		v.1			
<input type="checkbox"/>	Run user defined command	Executes user-defined script files or commands.		v.1			
<input type="checkbox"/>	Ping Check	It checks a Ping.		v.1			
<input type="checkbox"/>	Port Check	It checks a port.		v.1			
<input type="checkbox"/>	URL Check	It checks a URL.		v.1			
<input type="checkbox"/>	Service Group Online	Take the MCCS service group online.		v.1			
<input type="checkbox"/>	Service Group Offline	Take the MCCS service group offline.		v.1			
<input type="checkbox"/>	Service Group Lock	Lock the MCCS service group.		v.1			
<input type="checkbox"/>	Service Group Temp Lock	Take the MCCS service group to temporary lock.		v.1			
<input type="checkbox"/>	Service Group SwitchOver	Manually fail over the MCCS service group.		v.1			
<input type="checkbox"/>	Service Group Unlock	Unlock the MCCS service group.		v.1			
<input type="checkbox"/>	Power On VM	Powers the VM on.		v.1			
<input type="checkbox"/>	Power Off VM	Powers the VM off.		v.1			
<input type="checkbox"/>	Restart Guest OS	Restart the guest OS.		v.1			

4.3 License management

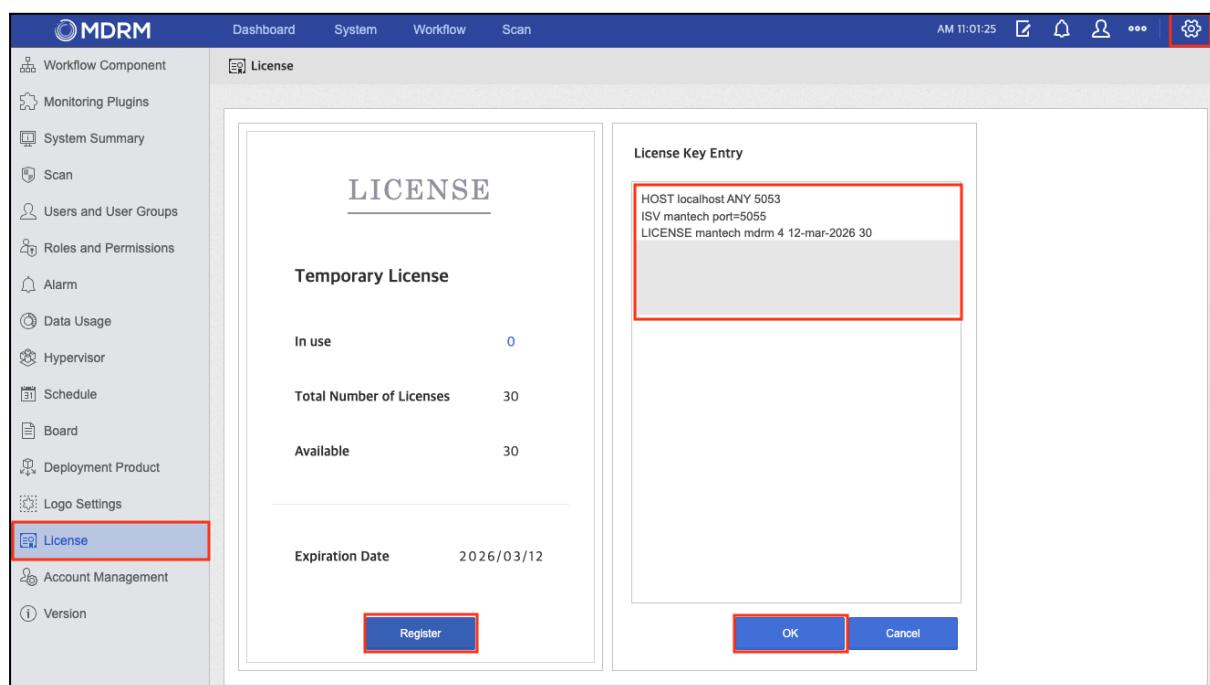
4.3.1 License type

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 registeredAvailable on all MDRM servers
Permanent license	<ul style="list-style-type: none">Available indefinitelyMDRM agents can be registered up to the number set at the time of issuanceValidity determined by the host name of the MDRM server to be used

4.3.2 How to set up a license

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



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.