Workflow Based **IT Automation solution**

MDRM

Mantech Dynamic Robotic Manager

Installing MDRM on AWS

manTech Solution

Table of Contents

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]

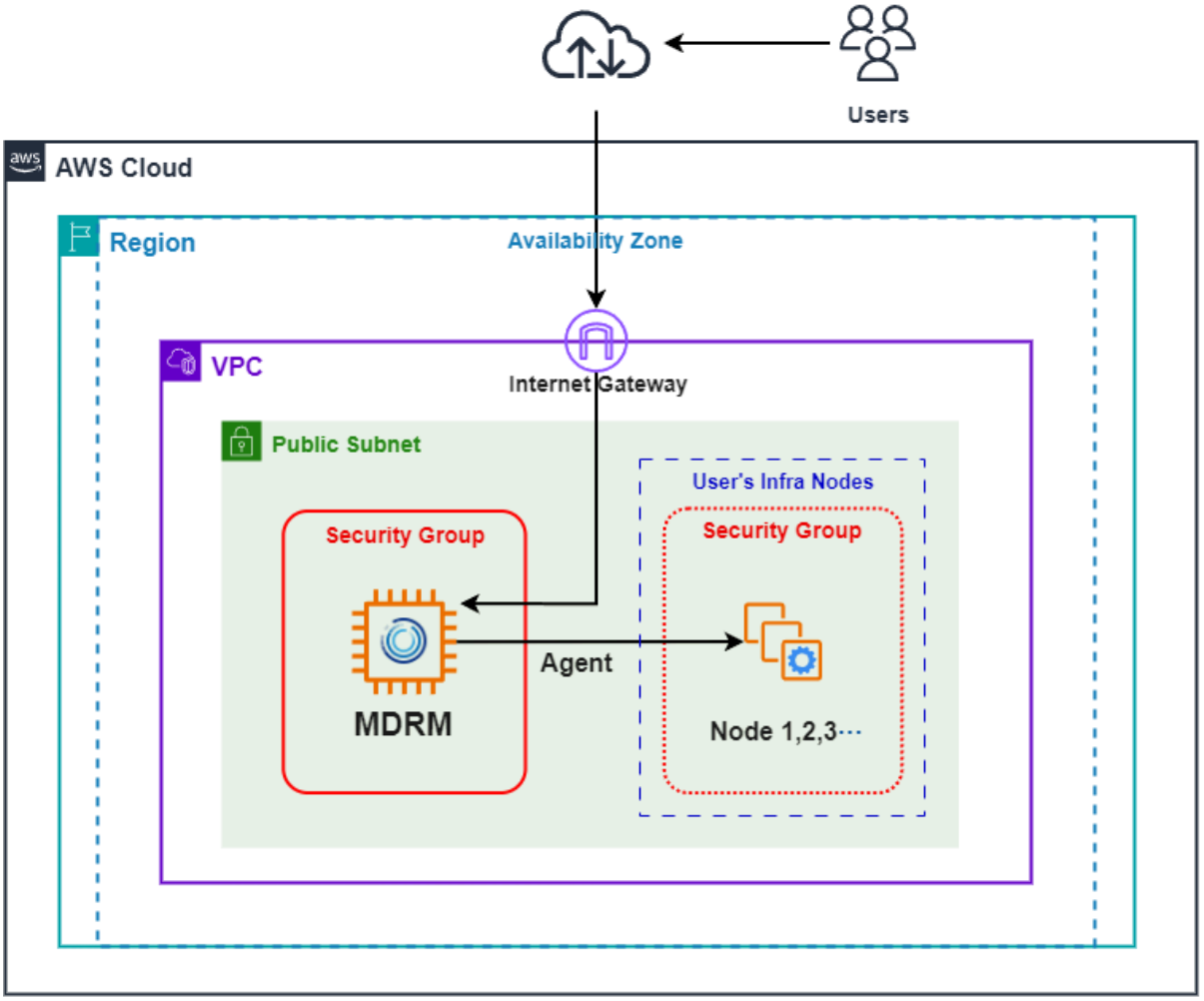
Resource	Less than 50 servers	Less than 100 servers	Less than 500 servers
vCPU	- 2.0GHz 64bit - 6 cores	- 2.0GHz 64bit - 8 cores	- 2.0GHz 64bit - 16 Core - Recommended: 24 Core
Memory	12 GiB	24 GiB	- 32 GiB - Recommended: 48 GiB
Disk	200 GB	500 GB	800 GB

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/TNmIowp0L8M?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

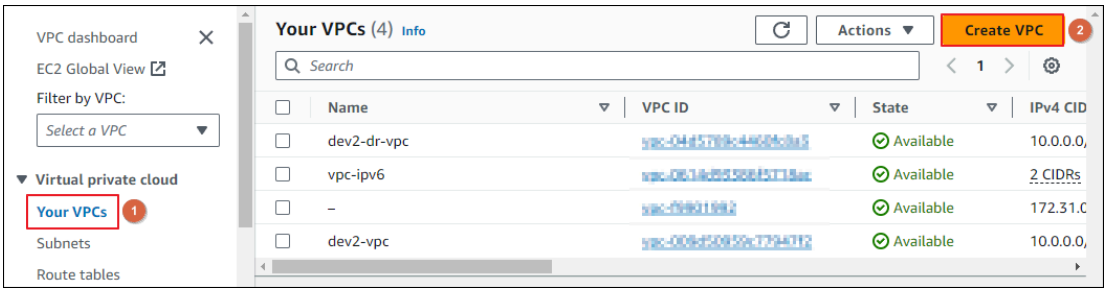
1. Prepare the network environment (“Pre-tasks” reference)
2. Create EC2 Instance with the provided AMI
3. Install MDRM (run install.sh)

3.1 Pre-tasks

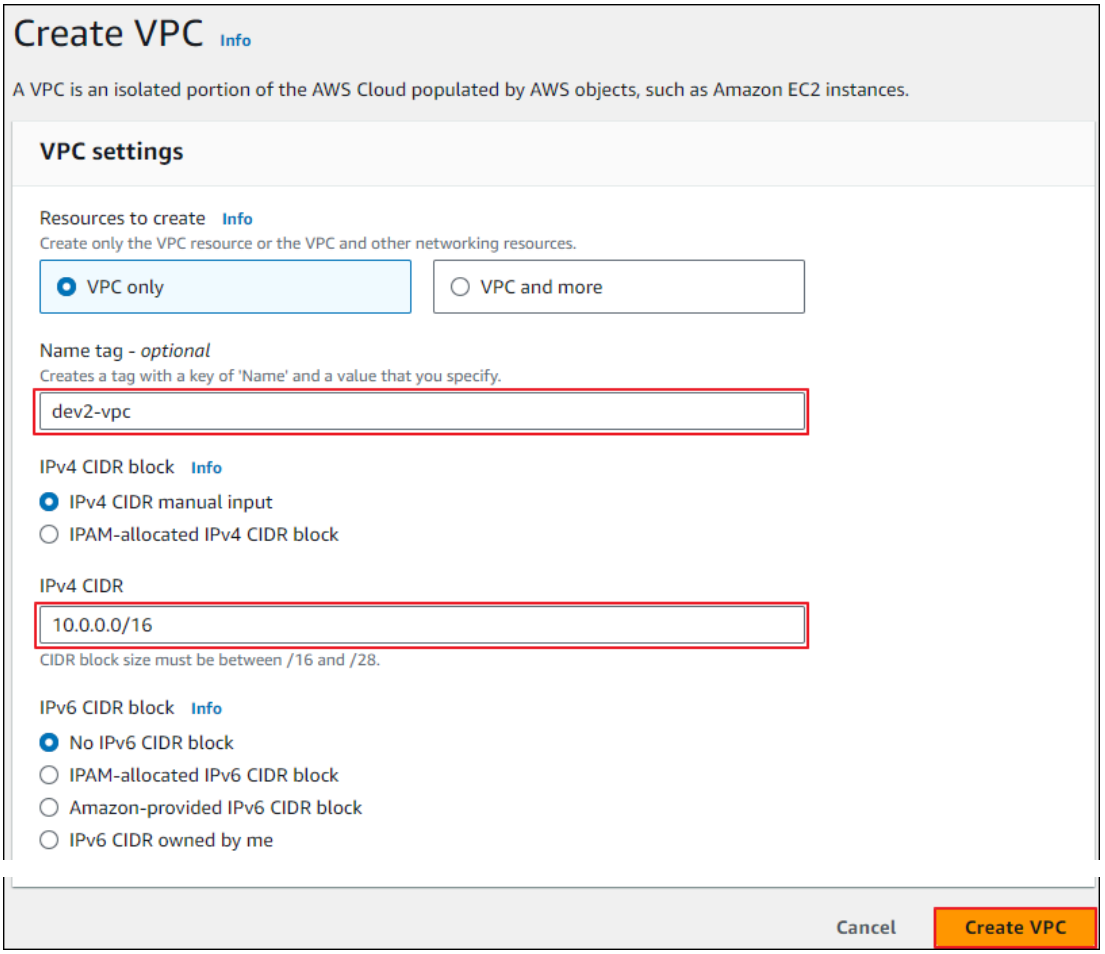
Before installing MDRM, set up your network environment and create an instance with ‘MDRM’ AMI.

3.1.1 Create VPCs

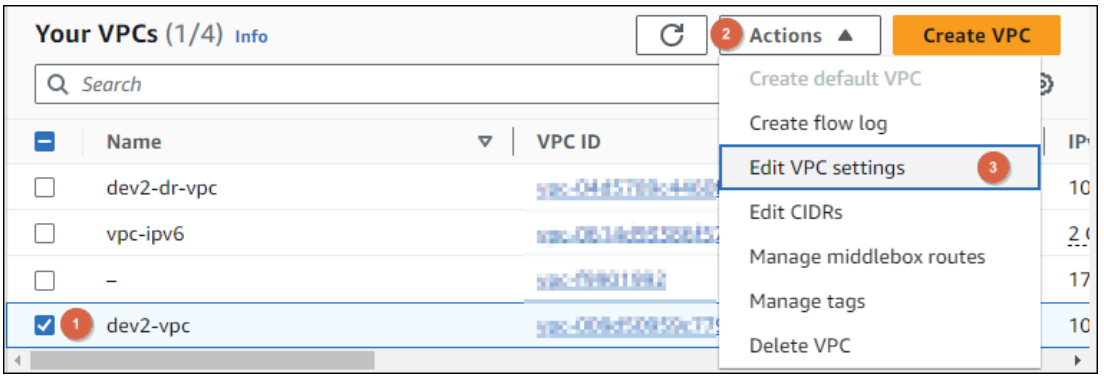
1. In the VPC dashboard, select "Your VPCs" and click [Create VPC].

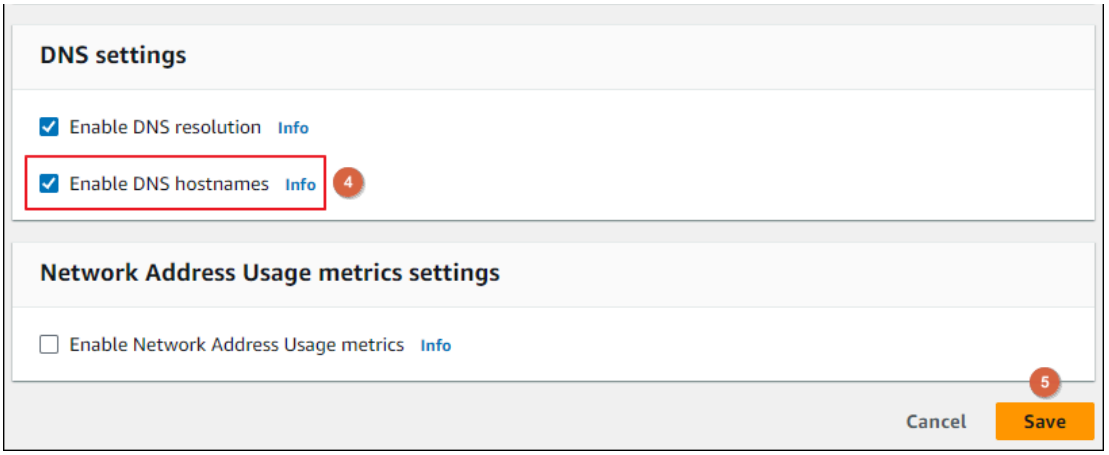


2. After setting the name (tag) and CIDR block, click [Create VPC].



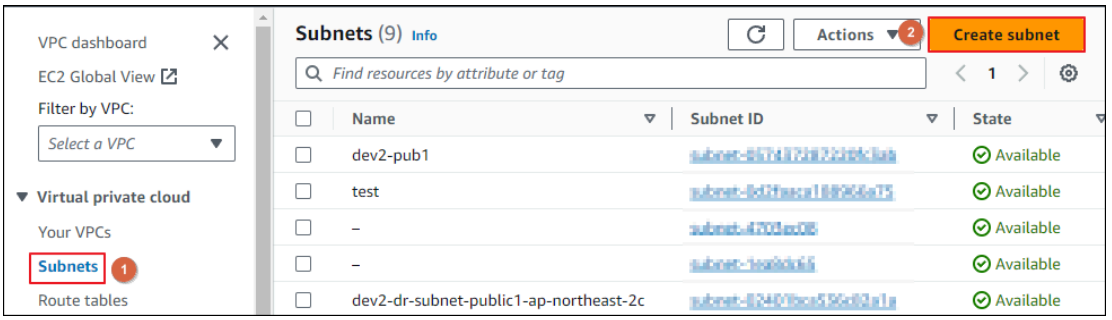
3. Select the VPC you created > Edit VPC settings > Check “Enable DNS hostnames” and save. If you enable “Enable DNS hostnames”, the DNS hostnames are automatically created for all EC2 instances within your VPC.



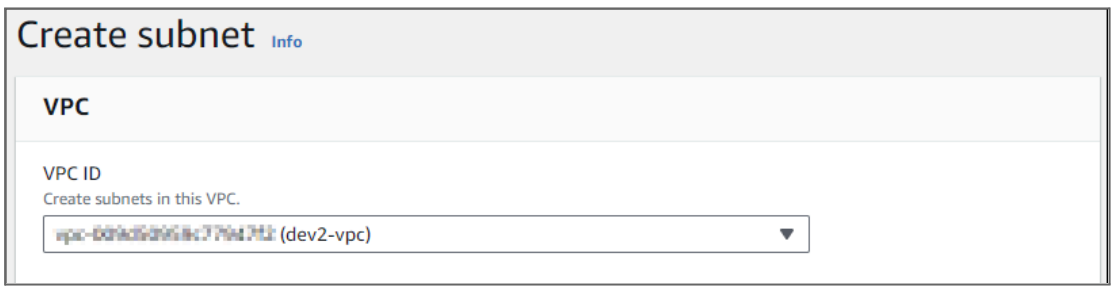


3.1.2 Create subnets

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

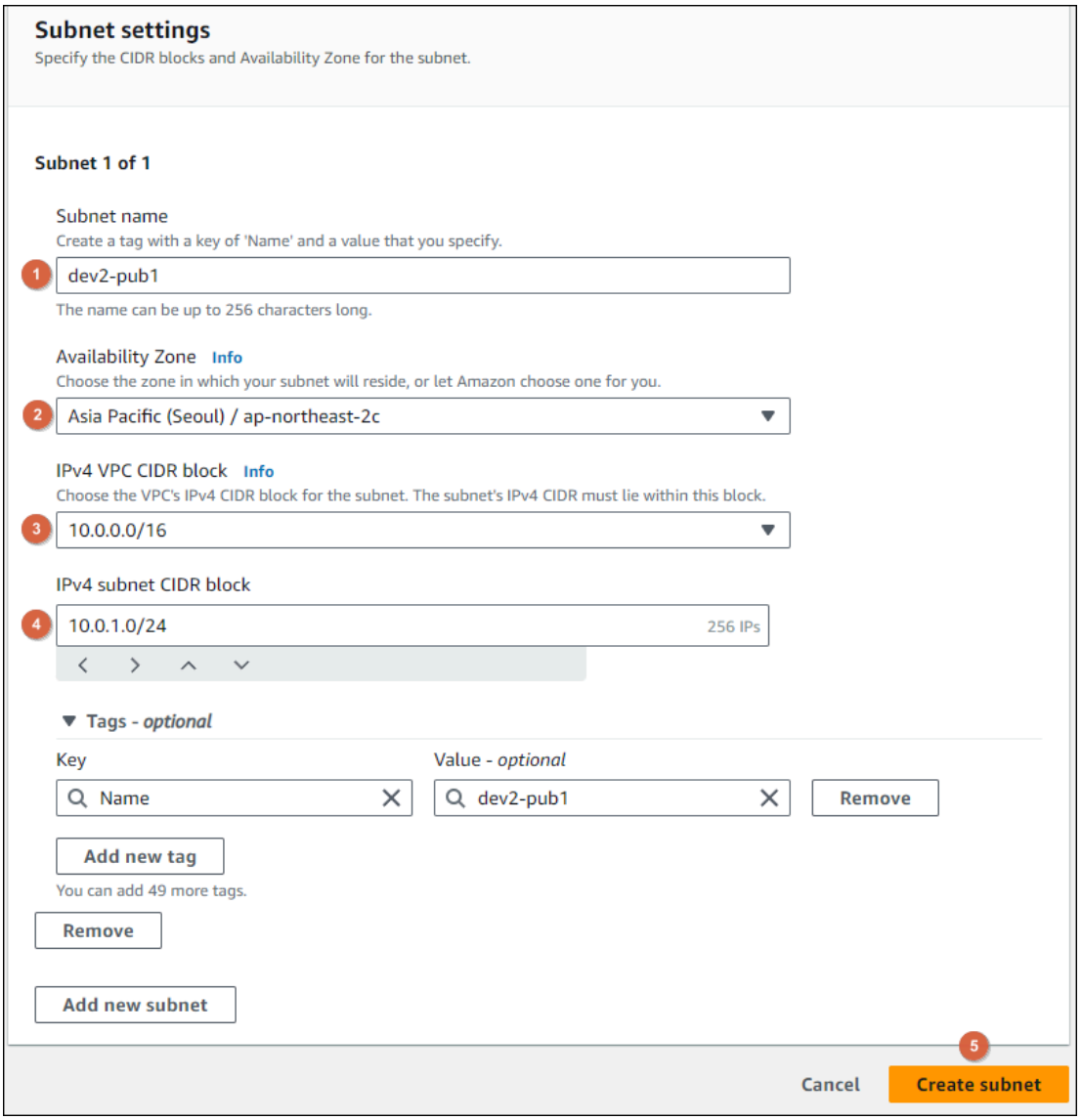


2. Select the VPC you created earlier.



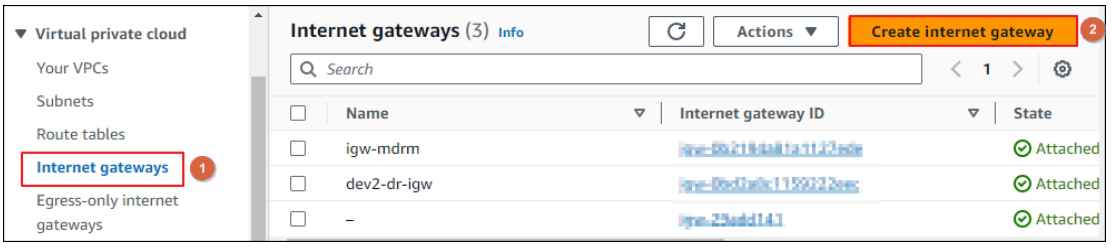
3. Create a subnet by specifying the subnet name, availability zone, and CIDR block.

※ If you use multiple subnets on one instance, set the Availability Zones to be the same.

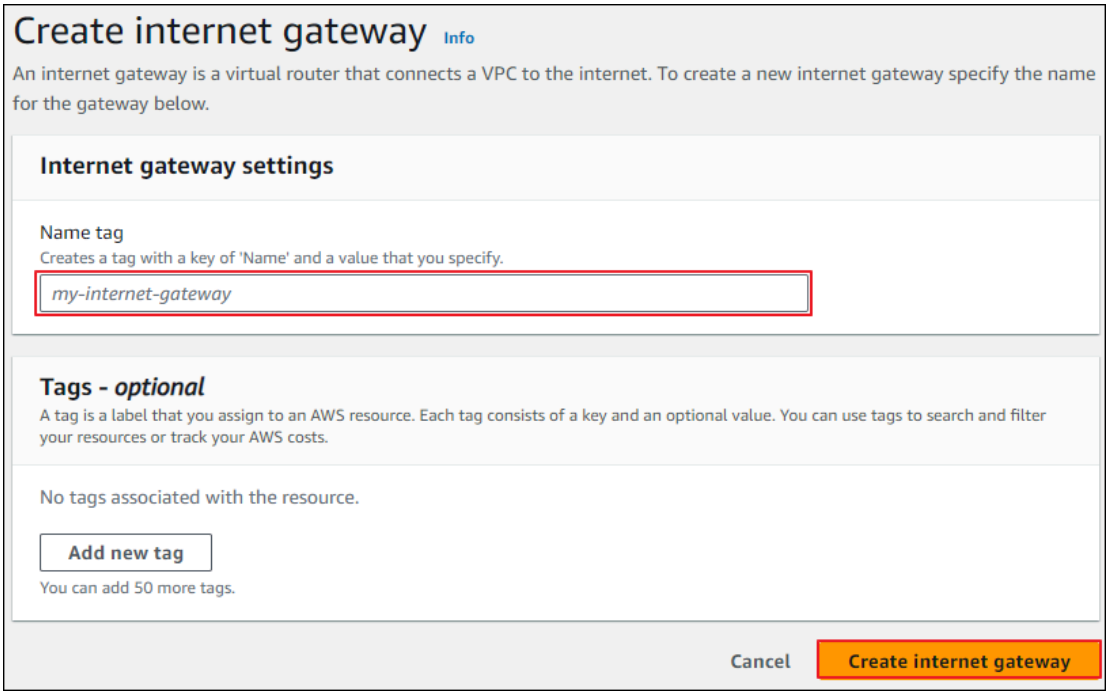


3.1.3 Internet gateway settings

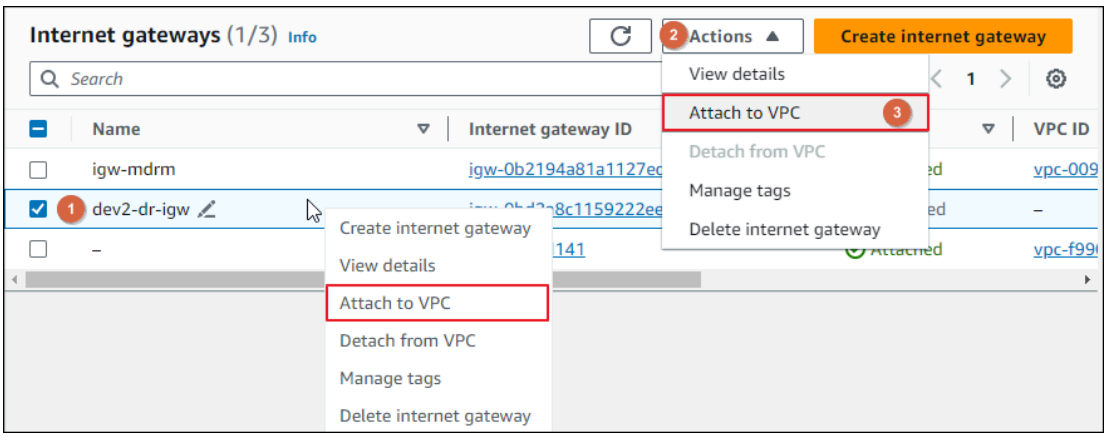
1. On the left menu, click “Internet gateways” and then click [Create internet gateway].



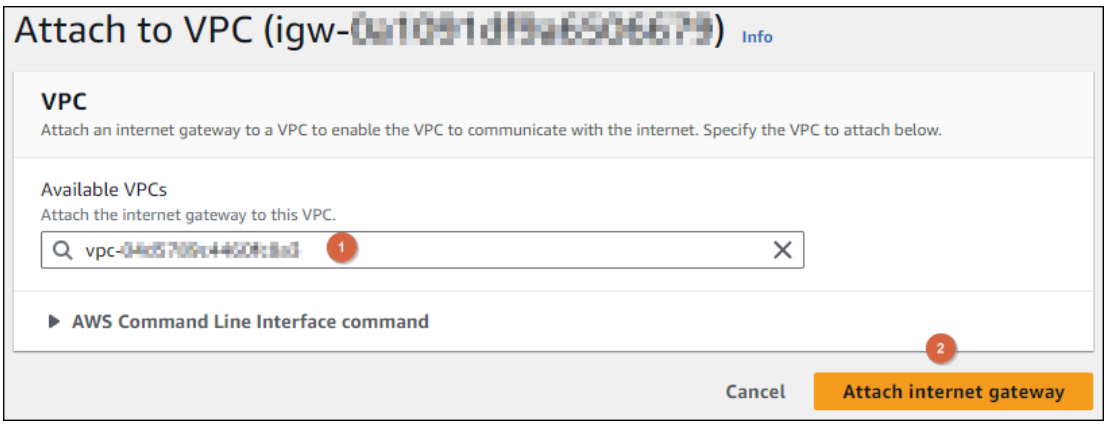
2. After writing the name (tag), click [Create internet gateway].



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].

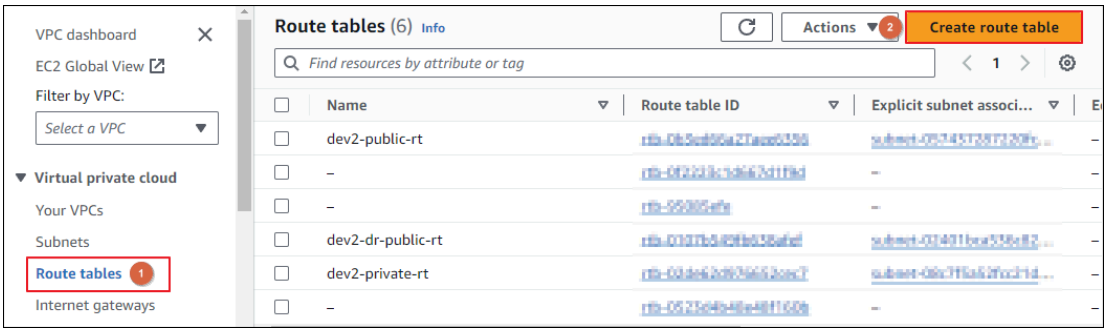


4. Select the VPC to connect to and click [Attach internet gateway].

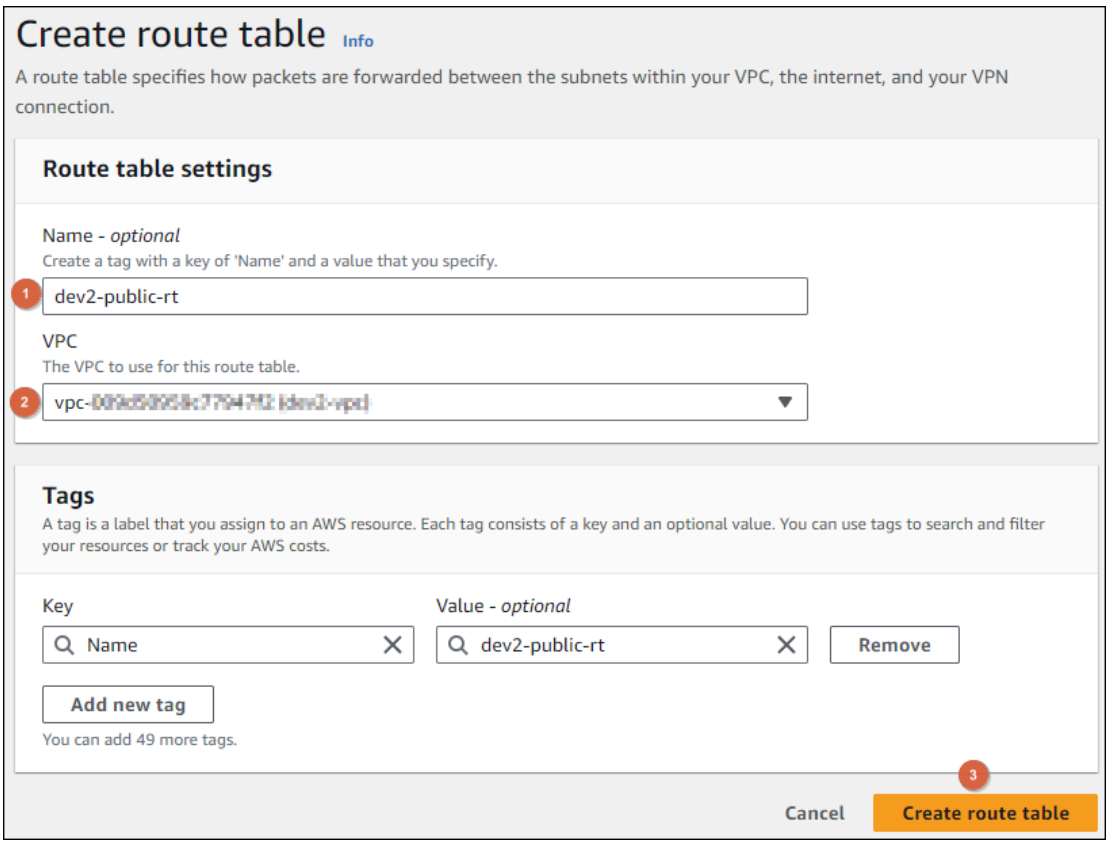


3.1.4 Routing table settings

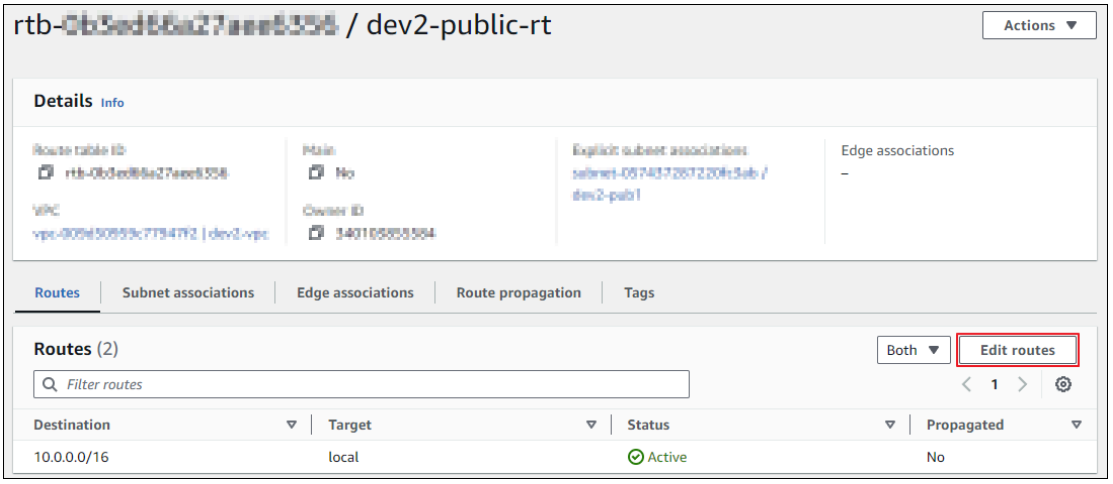
1. Click “Route tables” on the left menu and then click [Create route table].



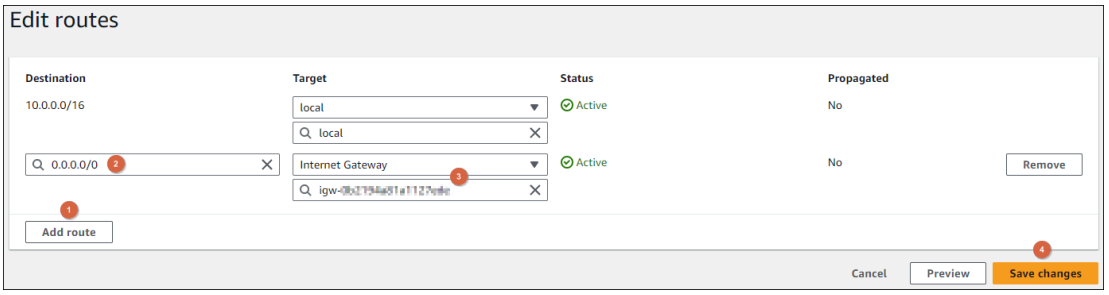
2. Enter a route table name, select VPC, and click [Create route table].



3. Click [Edit routes].

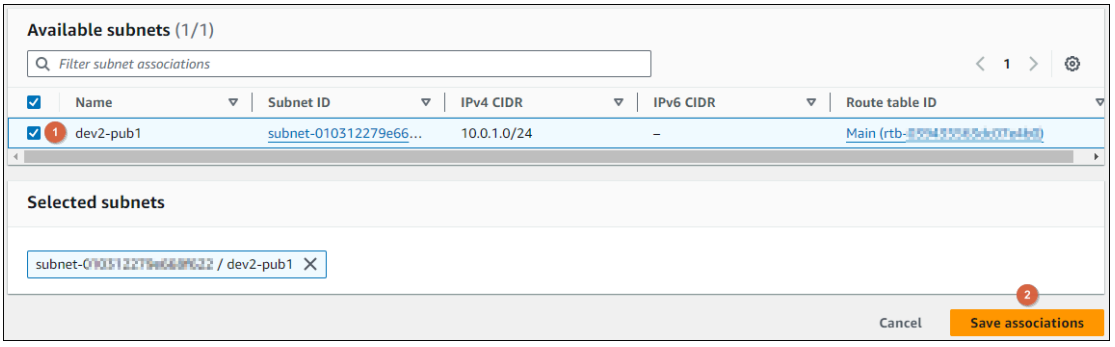


4. After clicking [Add route], specify the destination (0.0.0.0/0) and select the Internet gateway you created. After checking the contents, click [Save changes].



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

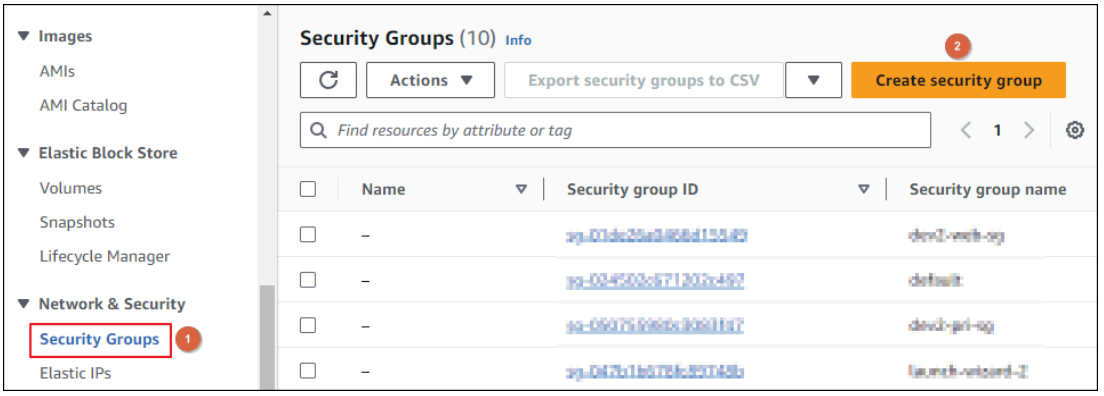
6. Select the subnets you want to connect to and click [Save associations].



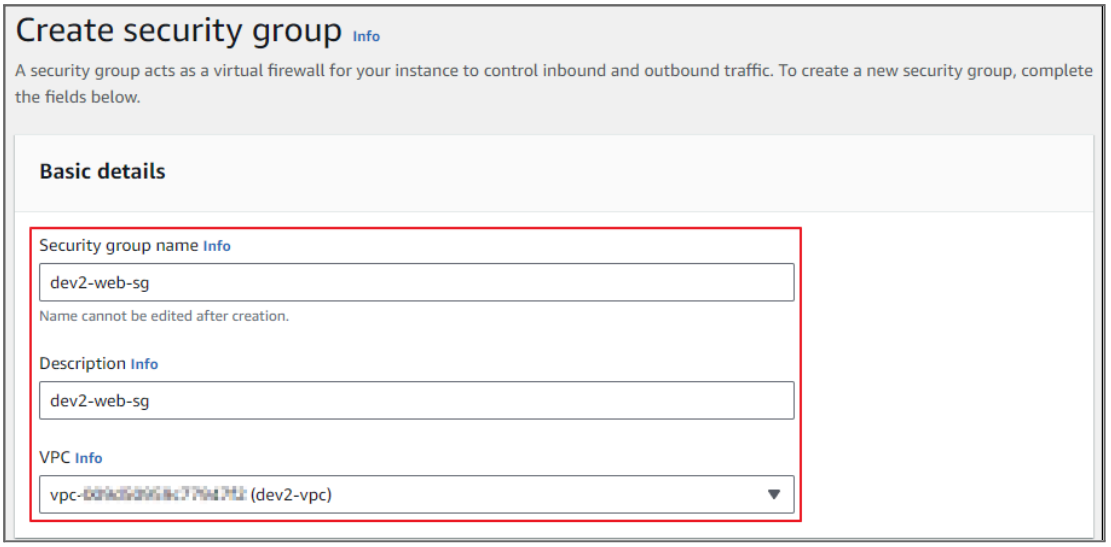
3.1.5 Create security groups

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]

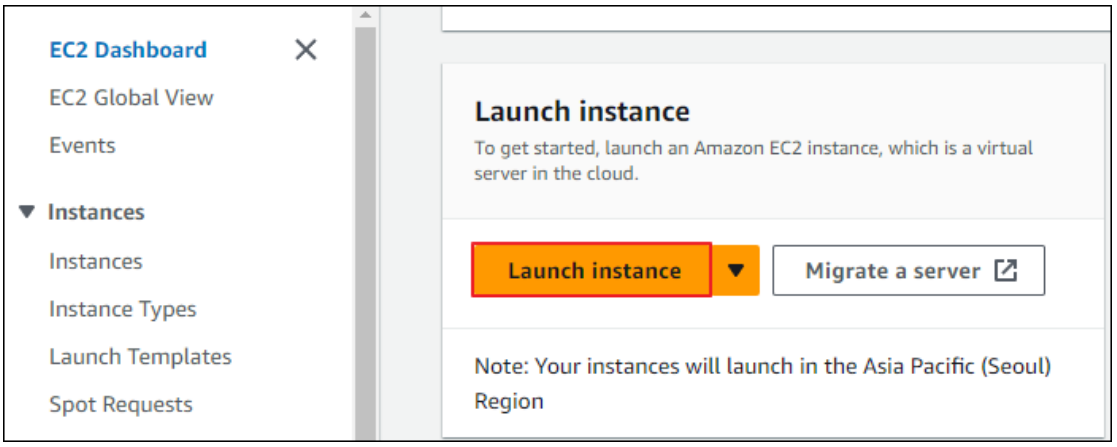
Type	Protocol	Port range	Source
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0
All ICMP - IPv4	ICMP	All	0.0.0.0/0

[Outbound rules]

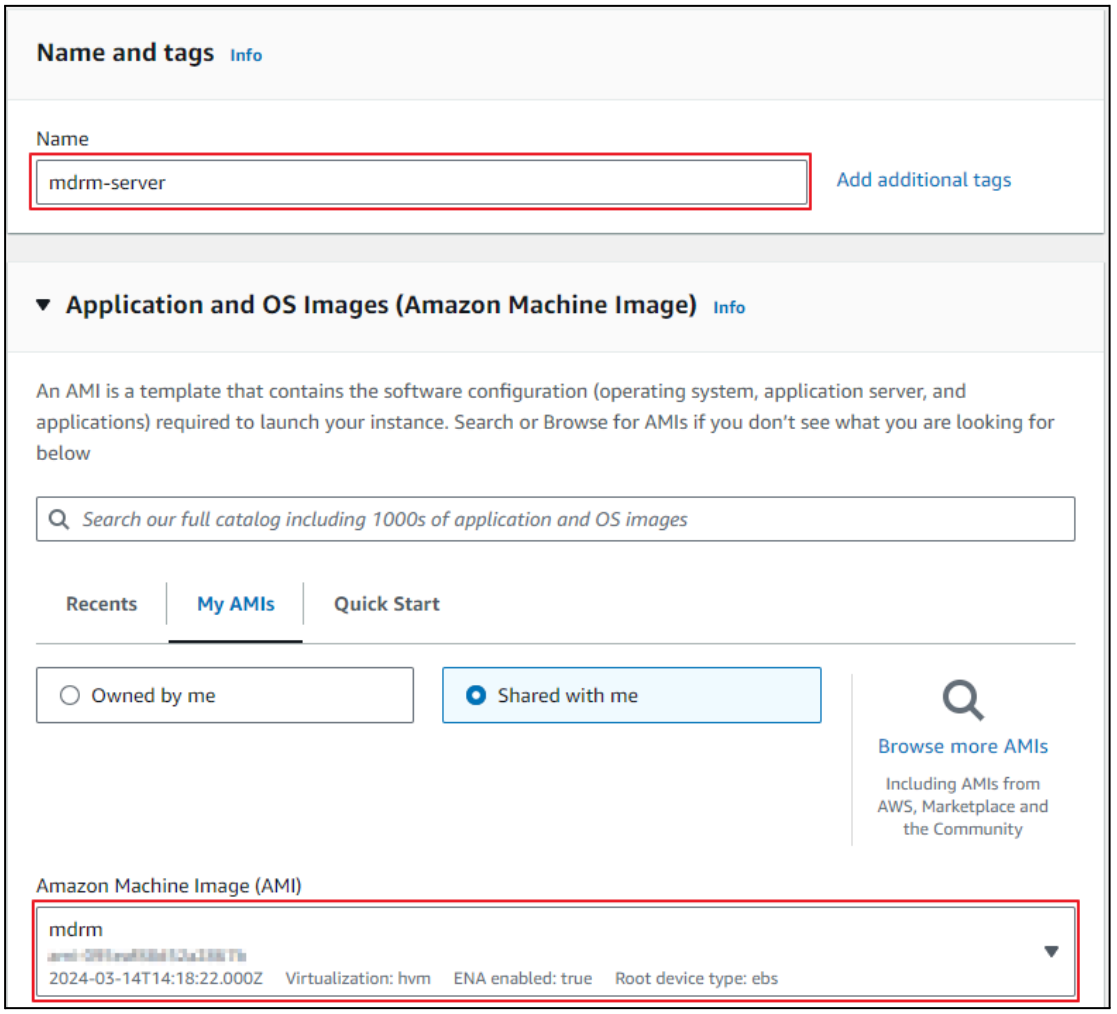
Type	Protocol	Port range	Source
All traffic	All	All	0.0.0.0/0

3.1.6 Create an instance

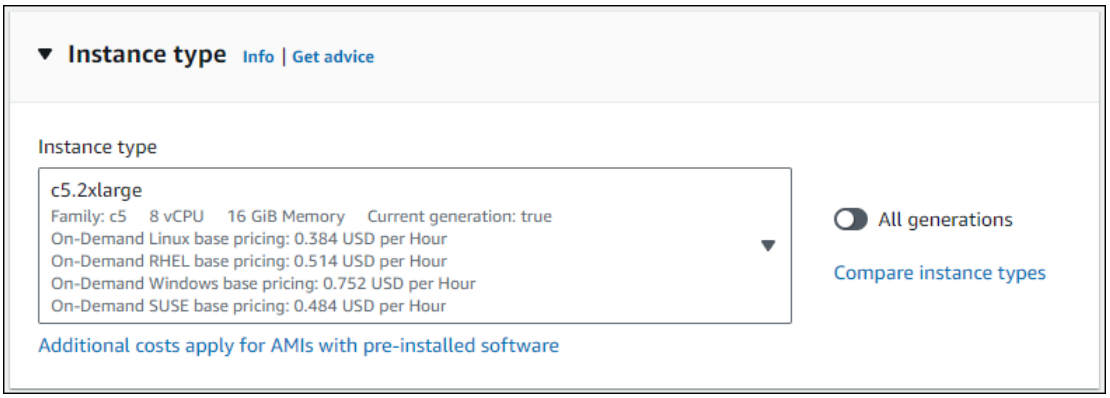
1. On the EC2 dashboard, click [Launch instance].



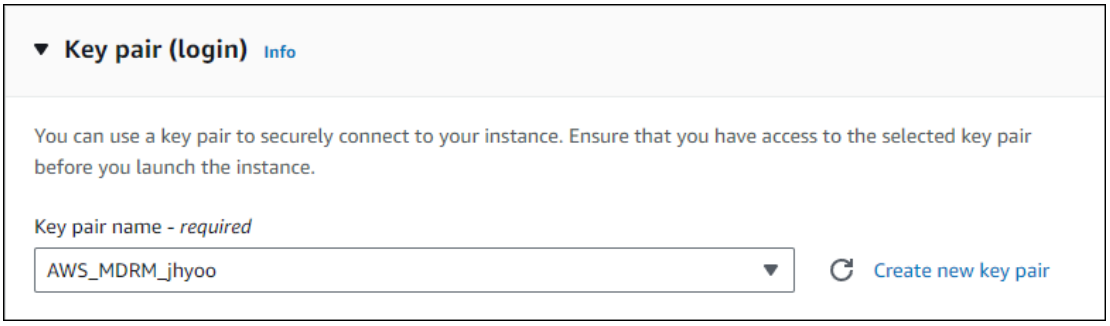
2. Enter an instance name and select the 'MDRM' AMI shared through AWS Marketplace.



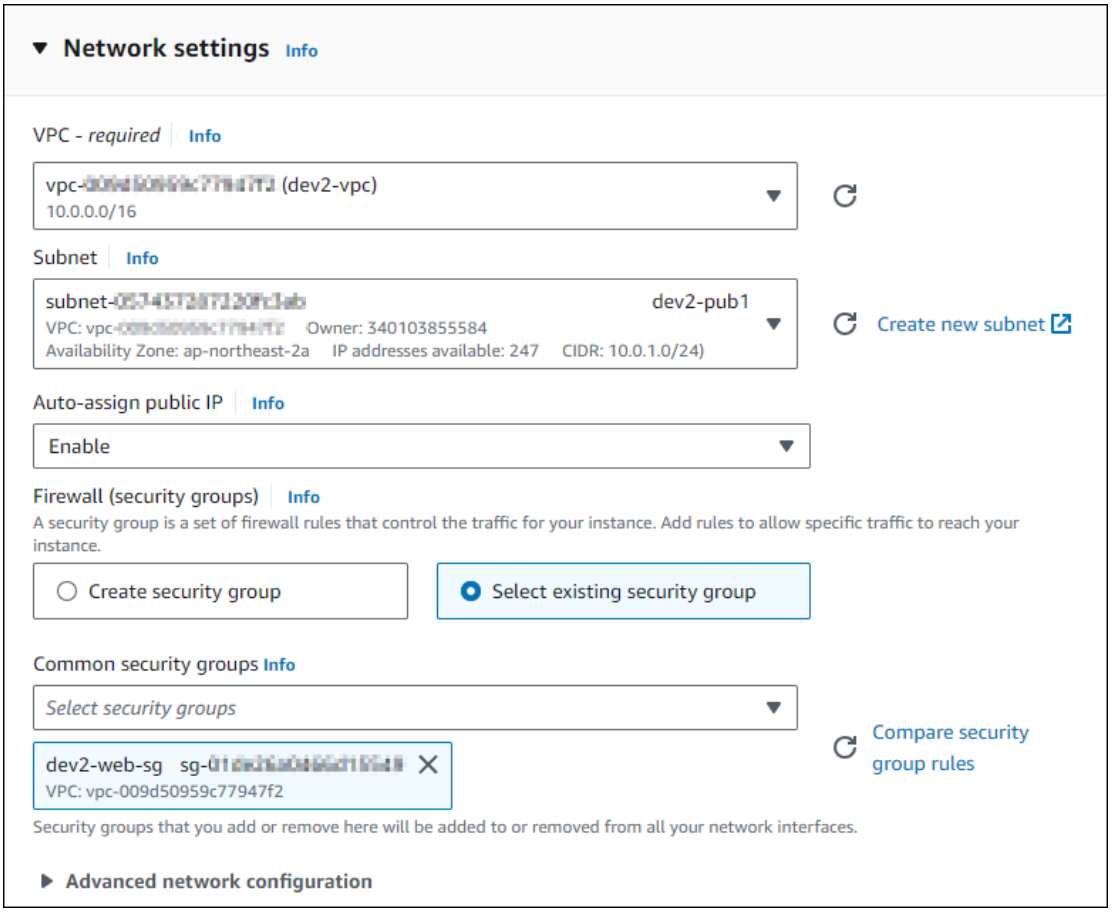
3. Select the instance type considering the size of the system (node) to be operated. (“Requirements” reference)



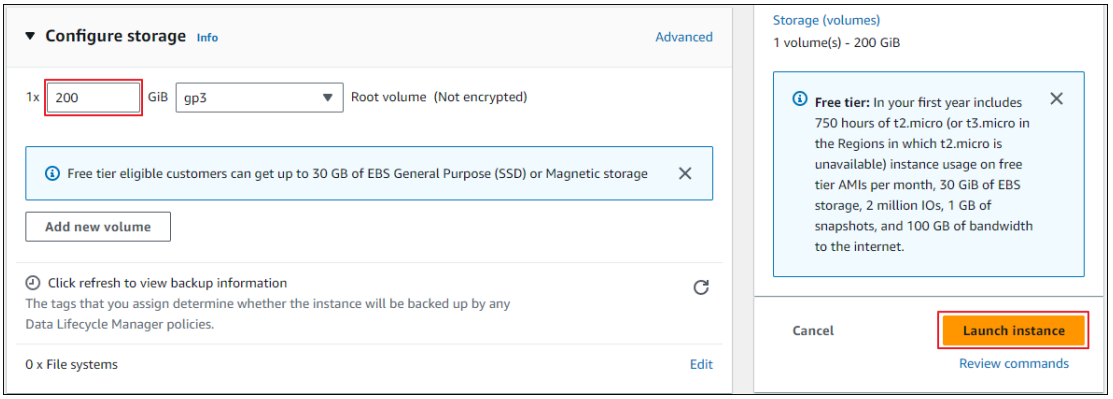
4. Create or select the key pair for administrator to use.



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



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

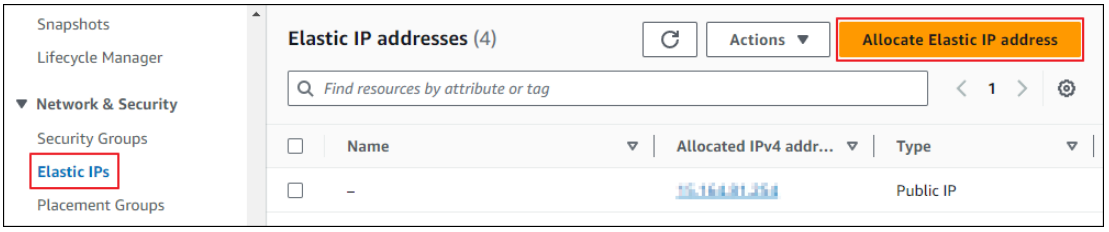


3.1.7 Elastic IP settings

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

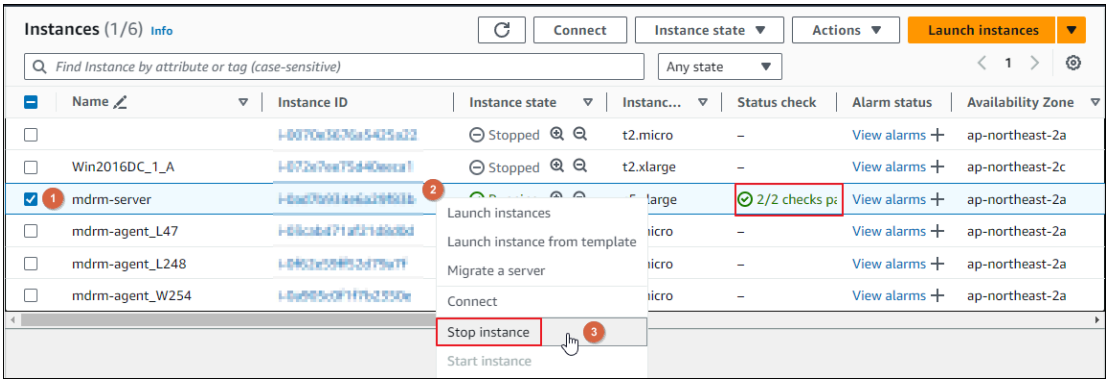
※ EIPs come standard with up to 5 per account, but you may be charged if you don't use them after they're allocated.

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

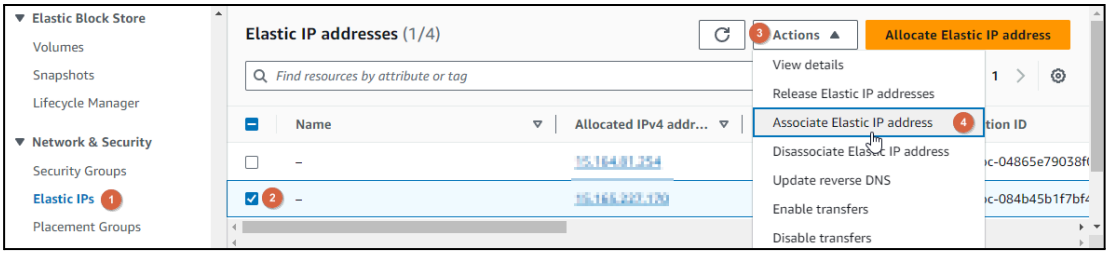


2. Click the [Allocate] button at the bottom.

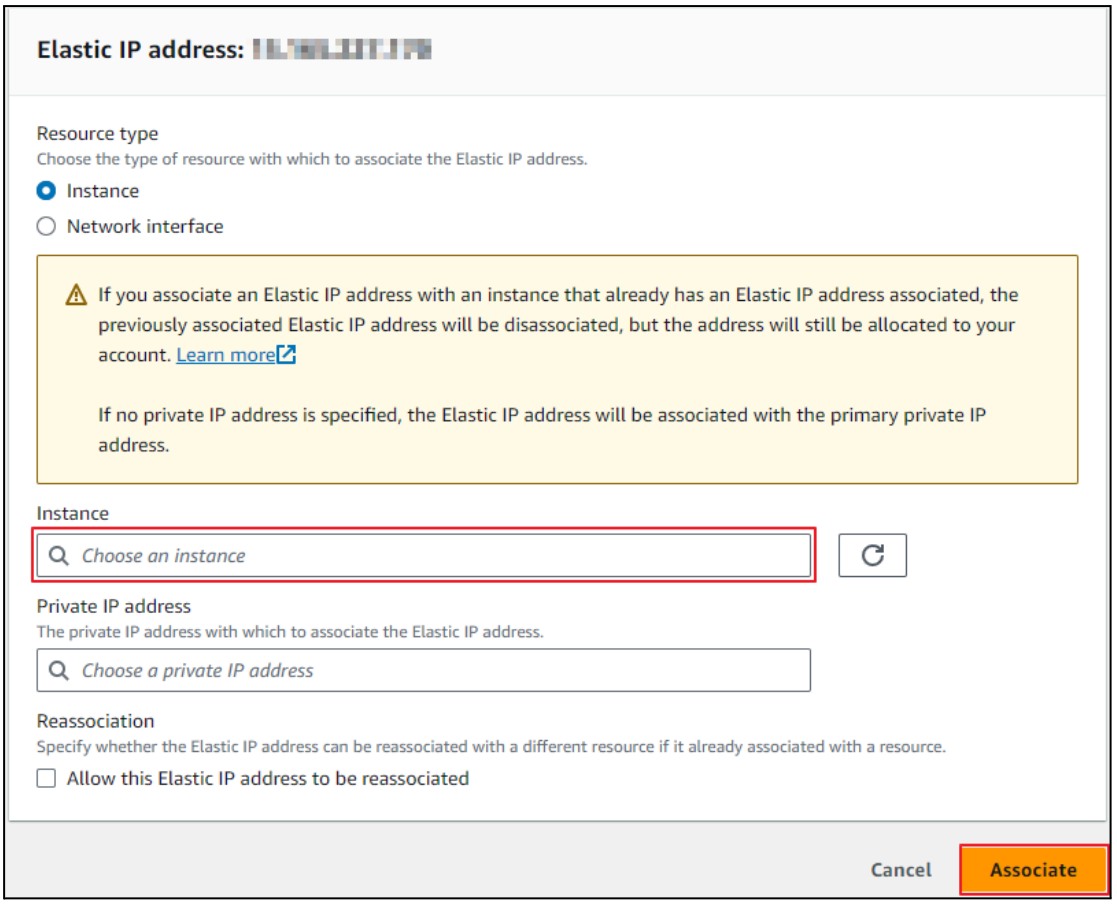
3. Click “Instances” in the left menu and stop the MDRM EC2 instance.
   At this time, confirm that the “Status check” of the instance is “2/2 checks passed”, right-click on the instance, and click “Stop instance.”



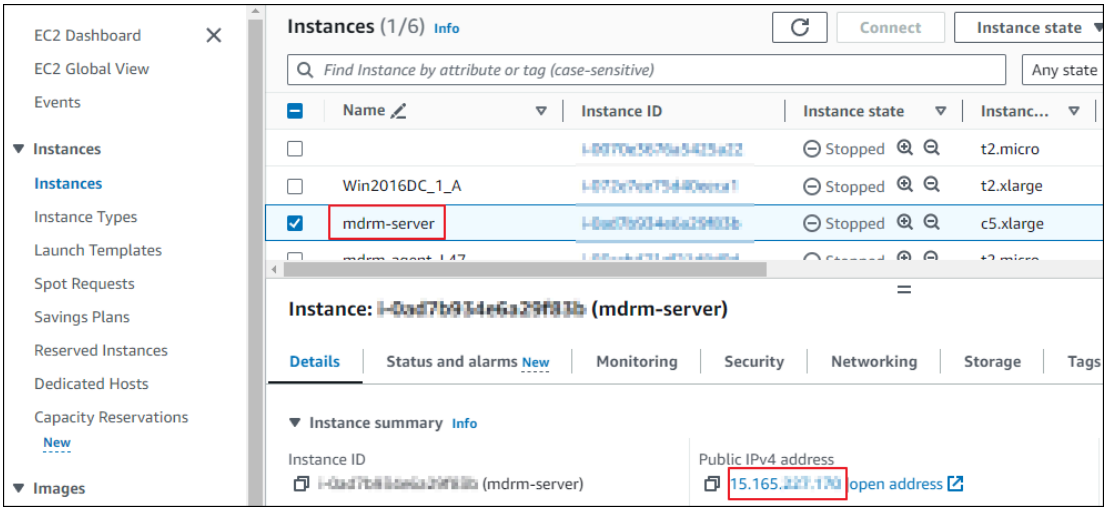
4. On the "Elastic IPs" screen, select the IP you want to associate with and click [Actions] > [Associate Elastic IP address].



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



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



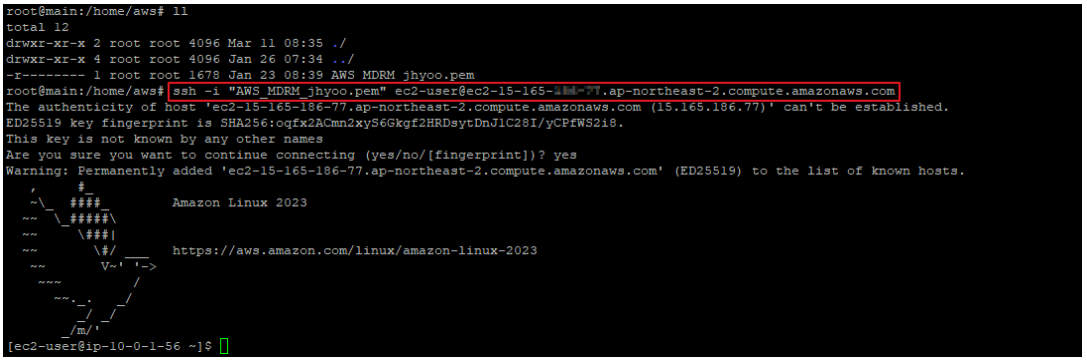
3.2 Install MDRM

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.

```
# 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
```



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]

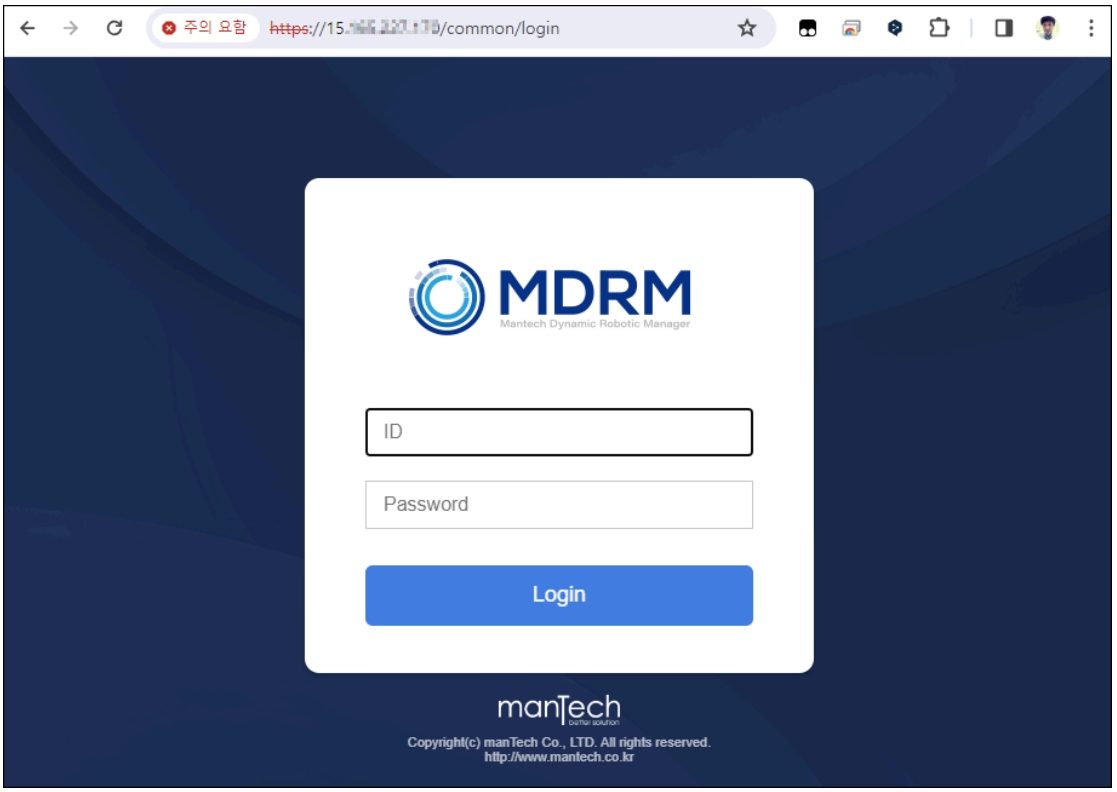
The following are frequently used commands when managing containers.
Run the docker-compose command from where the docker-compose.yml file is located.

```
# 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.

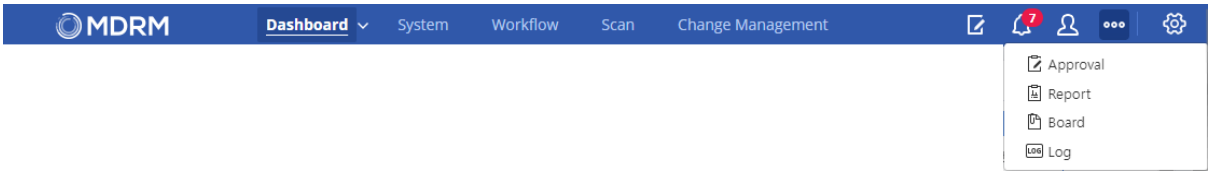
[Change password every 90 days]

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.

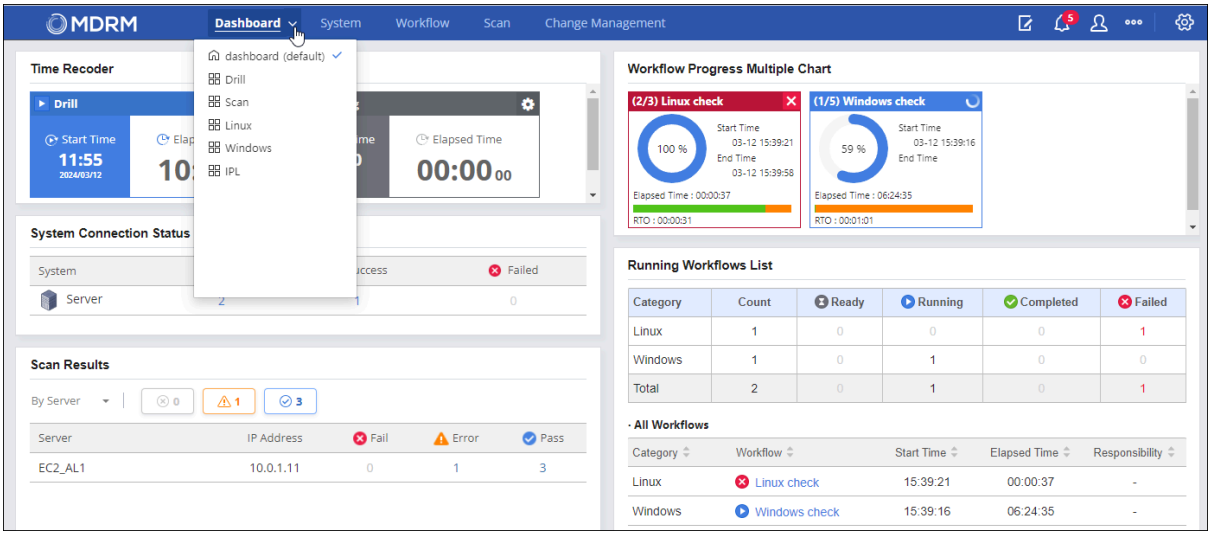
4.2.1 Menu bar



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.

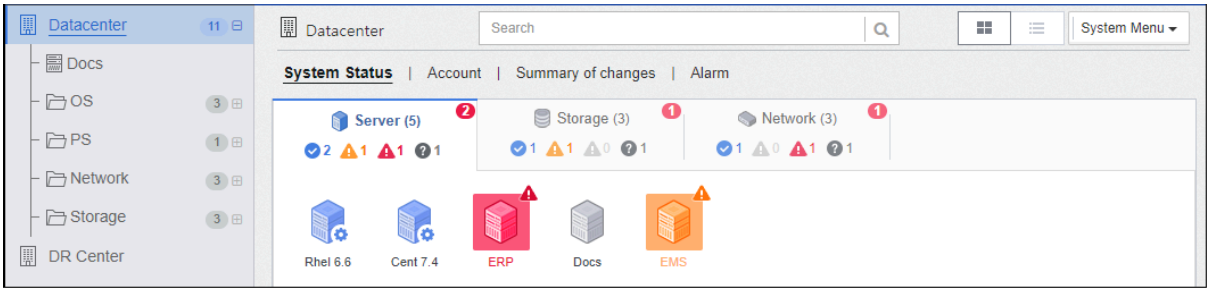
4.2.2 Dashboard

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.



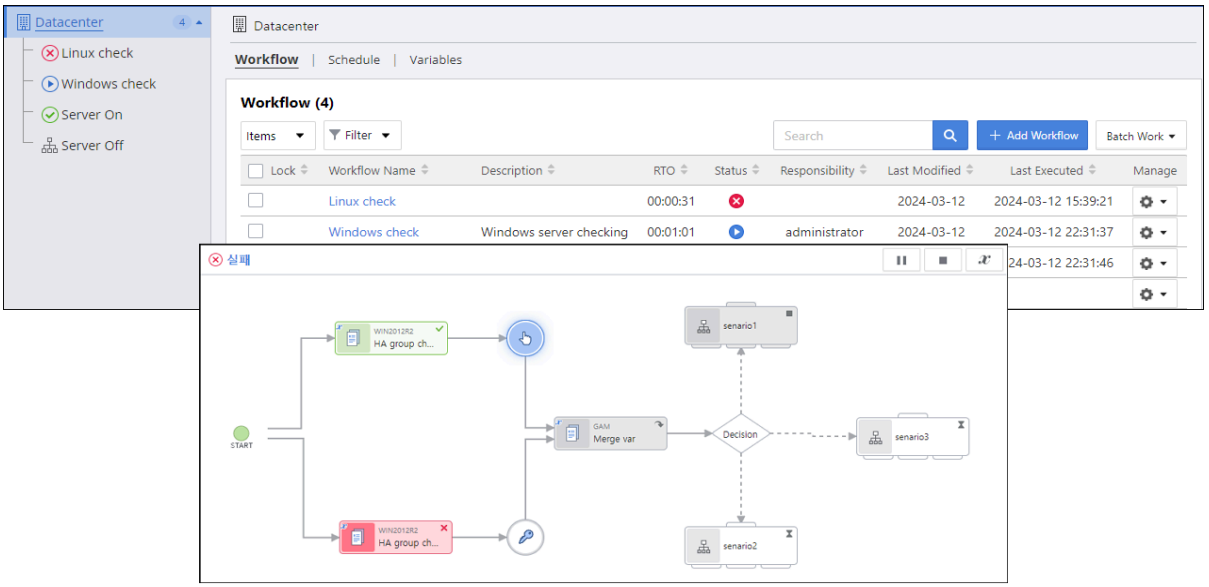
4.2.3 System

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



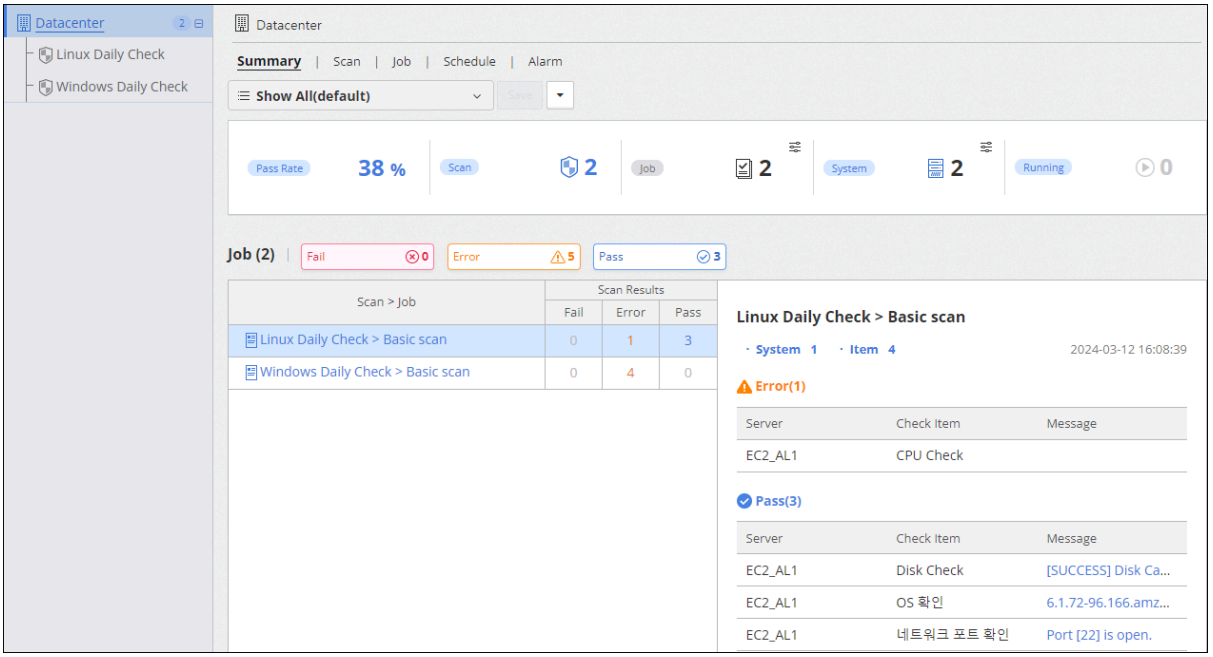
4.2.4 Workflow

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



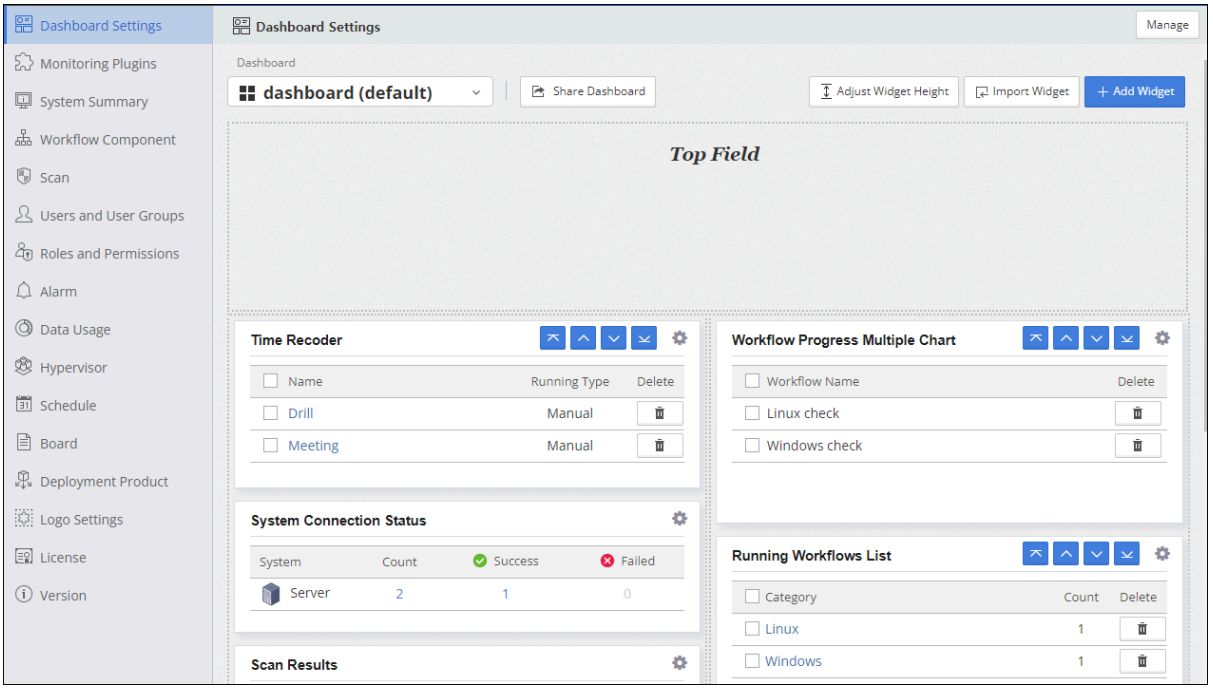
4.2.5 Scan

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.



4.3 License management

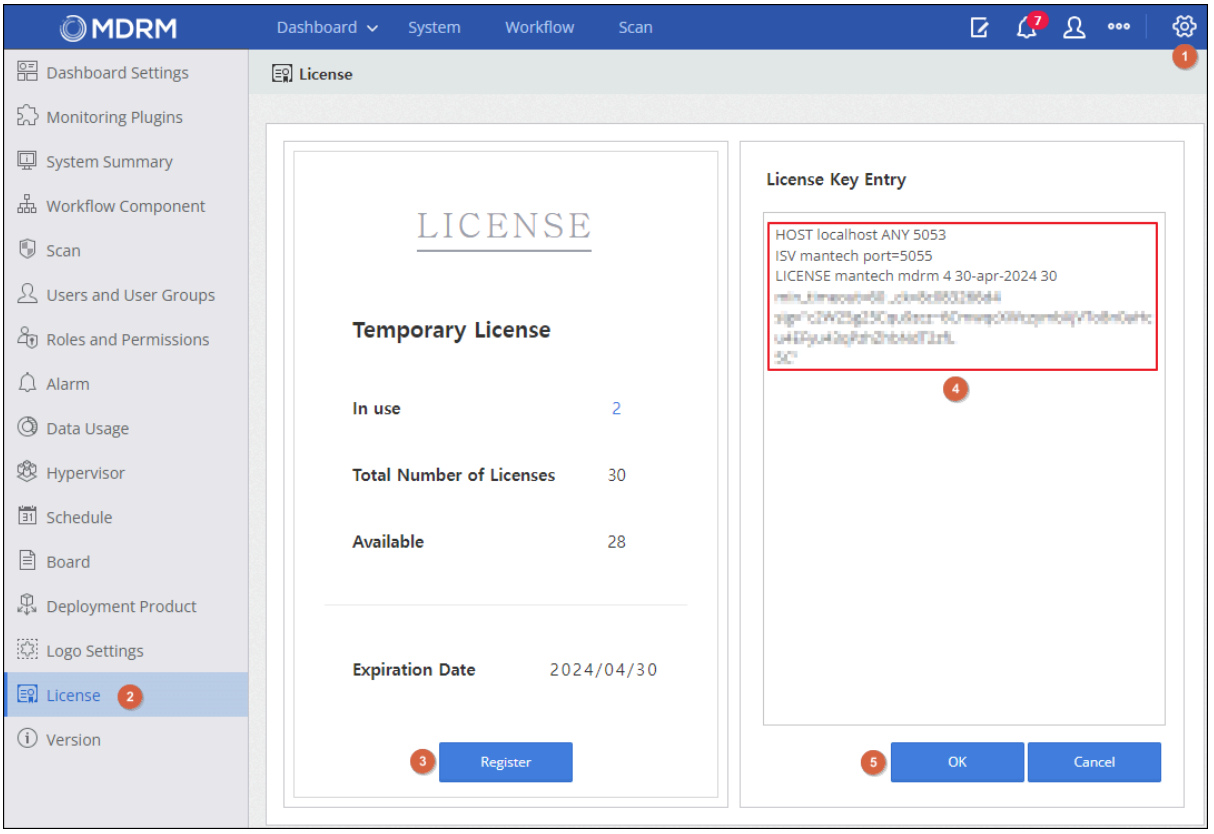
4.3.1 License type

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

Category	Characteristic
Temporary license	• 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	• 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.



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.