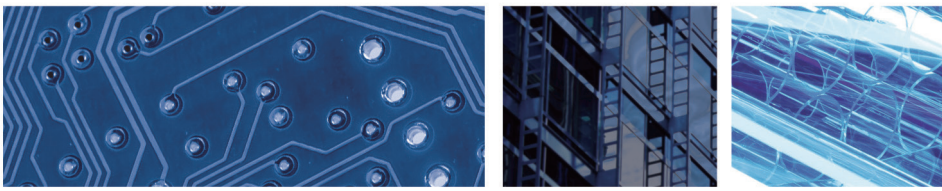
manTech
better solution



MCCS 4

Mantech Continuous Cluster Server

1. Product Overview

This document assumes previous use of AWS and familiarity with AWS services. See the Getting Started section of the AWS documentation for what's new in AWS. You should also be familiar with the following AWS technologies:

This document assumes that you have used AWS before and are familiar with AWS services. If you are new to AWS, see the Getting Started section of the AWS documentation. You should also be familiar with the following AWS technologies:

- Amazon VPC - The Amazon Virtual Cloud service allows you to provision an isolated, dedicated section of the AWS Cloud into which you can launch AWS services and other resources in a virtual network that you define. You have full control over your virtual networking environment, including choosing your own IP address range, creating subnets, and configuring route tables and network gateways.

- Amazon EC2 - The Amazon Elastic Compute Cloud service allows you to launch virtual machine instances on a variety of operating systems. You can choose from existing Amazon Machine Images (AMIs) or bring your own virtual machine images.

1.1 Introduction

MCCS(Mantech Continuous Cluster Server) is a high availability (HA) redundancy solution for continuous service of corporate computer systems.
Service disruptions due to natural disasters, system failures, and operator errors incur huge cost losses and affect a company's social image and economic value. In addition, costs are incurred for planned service outages, such as system changes and backups.
MCCS provides infrastructure stability that maximizes service availability by minimizing downtime and automatically restoring the same level of service in the event of a failure.

1.1.1 Requirements

This topic describes prerequisites and requirements for using AWS with MCCS.

MCCS Requirements
System specifications for MCCS installation are as follows.

System	Requirements
CPU	● 64bit (x64) processor with at least 2GHz or faster ● 4 cores or more recommended

- Instance Requirements
  The system requirements for using the instance are as follows.
  [Windows]

Network	Minimum of 3 network interfaces required
Storage	Requires multiple volumes to configure volume replication

[Linux]

Network	Minimum of 3 network interfaces required
Storage	Requires multiple volumes to configure volume replication
More details	GUI configuration required

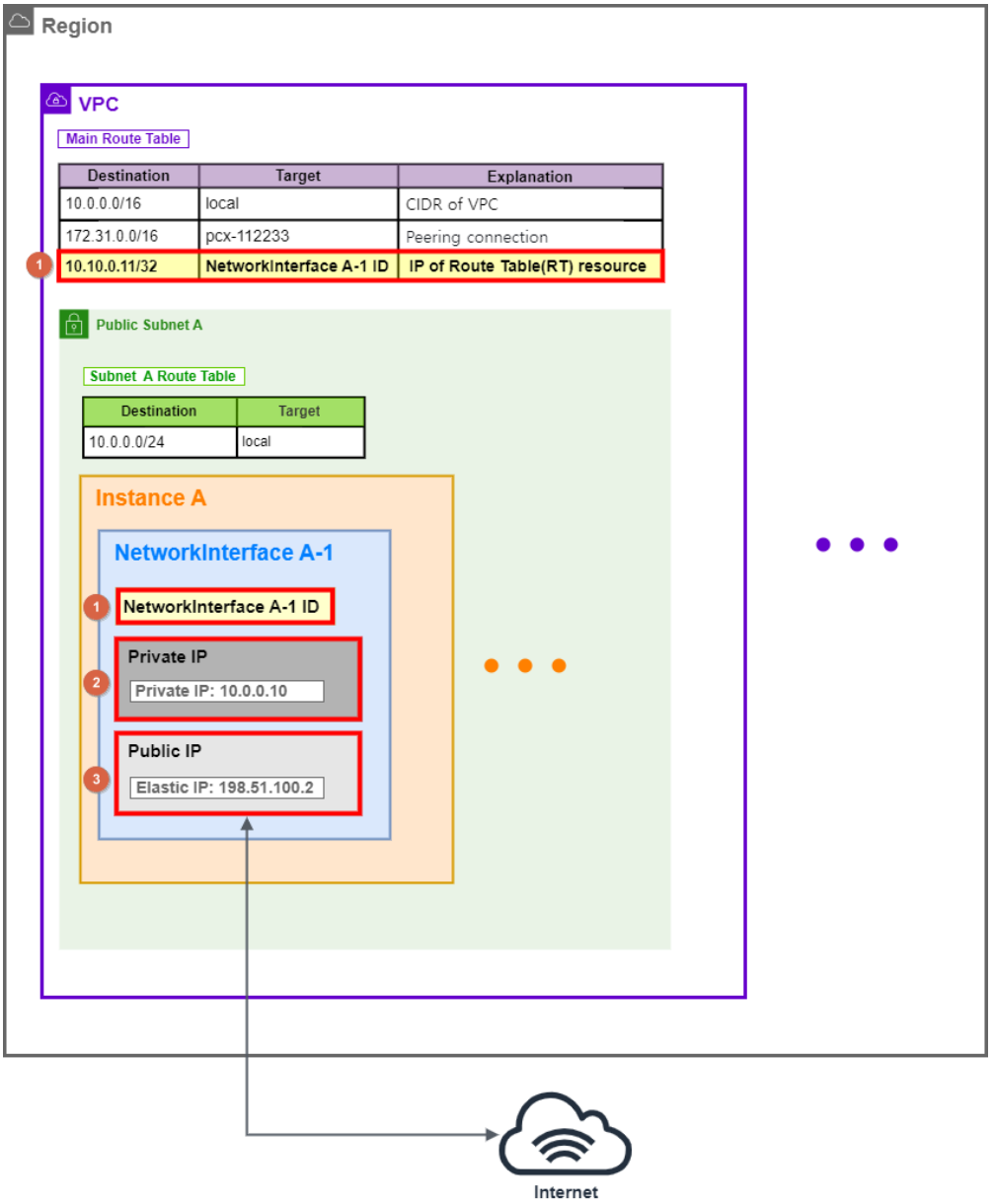
[Max number of network interfaces]

Number of vCPUs	Number of vNICs
2 or less	2
2~8	2~8
8 or more	8

1.1.2 Supported Regions

All regions are supported

1.1.3 Architecture



1	AWS Overlay IP(OIP) Resource	A resource that allows MCCS to manage AWS by creating a routing destination on the AWS network interface with a specified virtual IP address. Route tables are IP addresses that are only available inside AWS. When you create a virtual private cloud (VPC) in AWS, a route table is automatically created for you. You can set a custom route destination address in an automatically generated route table or an additionally created route table.

		If you want to specify a route destination address, you must set the route destination address to a band other than the CIDR band declared in the VPC. For example, if the CIDR of the VPC is 10.0.0.0/16, the route destination IP address cannot be in the range 10.0.0.0 to 10.0.255.255. Overlay IP resources must be configured with network card resource and network address resource of MCCS. The route destination address added to the route table is set to the virtual IP address of the network address resource. MCCS allows you to connect to your AWS instance's network interface at a user-specified virtual IP address. When using that resource, source/destination resolution of the network interface is disabled.
2	AWS Secondary Private IP (SIP) Resource	A resource that allows MCCS to manage AWS by assigning a secondary private IP address for an AWS network interface to a specified virtual IP address. A secondary private IP address is an IP address that can only be used inside AWS. Set the secondary private IP address to an IP address that falls within the CIDR band declared by the subnet. For example, if the subnet's CIDR is 10.0.0.0/24, the secondary private IP address should be set in the range 10.0.0.0 to 10.0.0.255. The secondary private IP resource must be configured with network card resource and network address resource of MCCS. Specify the virtual IP address of your network address resource as a secondary private IP address so that it is recognized by the AWS instance's network interface.
3	AWS Elastic IP (EIP) Resource	A resource that allows MCCS to manage AWS by assigning an Elastic IP address allocated using the AWS Elastic IP feature to a network interface. Elastic IP addresses are static IPv4 addresses designed for dynamic cloud computing that consist of public, externally accessible IPv4 addresses. To use an Elastic IP address, you must first allocate an IP address for use in your account, and once assigned, it remains until you release it. An elastic IP address must be configured as a required network card resource in MCCS.

2. Planning Guidelines

2.1 Security

List	Port
MCCS web console port	11080
Heartbeat port	14321

All that is required to install and control MCCS is SSH access and does not use AWS root credentials.

2.2 Costs and Licenses

MCCS supports BYOL licenses. BYOL is offered by your partner or distributor and offers the same ordering method across all private and public clouds, regardless of platform. You must activate your license the first time you access your instance from the GUI or CLI before using the various features.

License	Price (per 1 set)
MCCS ASP	300,000 won per month
MCCS Permanent License	35 million won

✔ Full List of Billable AWS Services
Full list of billable AWS services You are responsible for the cost of AWS services. Depending on the size of the cluster you plan to use, the cost of your resources will vary. For more information, see the page for each AWS service you will use in this guide: https://aws.amazon.com/pricing/.

A. EC2 instance (required)

2.3 Instance Size

The MCCS AMI supports the following size instance specifications on AWS.
For Node AMIs, specify the instance type according to the node type you want to use. Please refer to the following link (https://aws.amazon.com/ko/ec2/instancetypes/) for the latest information.

3. Deployment Procedures

3.1 Advance procedure

3.1.1 IAM Policy Setting

In AWS Identity and Access Management (IAM) settings, you create a policy for each AWS resource and set that policy to a group of users.
Create permissions for each AWS resource as a policy.

1. Log in to the AWS Management Console (https://console.aws.amazon.com/iam/).
2. Click “Policy” > [Create Policy] button in “Access Management”.

3. Create policy creation.
   To manage AWS resources in MCCS, the following permissions must be set as policies for each resource.

List	Permissions
AWS Overlay IP(OIP) Resource	"ec2:DescribeNetworkInterfaces" "ec2:DescribeVpcs" "ec2:CreateRoute" "ec2:DeleteRoute" "ec2:ReplaceRoute" "ec2:ModifyNetworkInterfaceAttribute" "ec2:DescribeRouteTables
AWS Secondary Private IP Resource	"ec2:DescribeNetworkInterfaces" "ec2:UnassignPrivateIpAddresses" "ec2:DescribeSubnets" "ec2:AssignPrivateIpAddresses"
AWS Elastic IP Resource	"ec2:DisassociateAddress" "ec2:DescribeAddresses" "ec2:DescribeNetworkInterfaces" "ec2:AssociateAddress"

If you create more than one kind of AWS resource, you can add them all with one policy including their permissions.

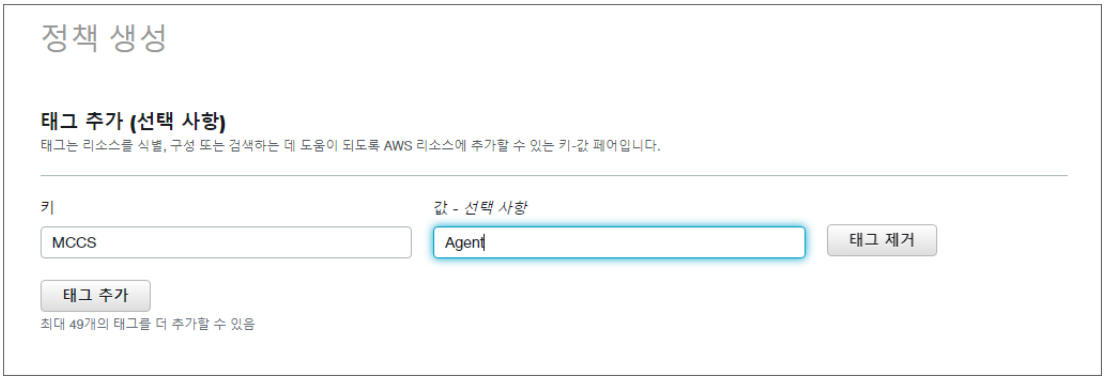
List	Permissions
When the permissions of all AWS resources are included	"ec2:AssociateAddress" "ec2:AssignPrivateIpAddresses" "ec2:CreateRoute" "ec2:DeleteRoute" "ec2:DescribeAddresses" "ec2:DescribeNetworkInterfaces" "ec2:DescribeRouteTables" "ec2:DescribeSubnets" "ec2:DescribeVpcs" "ec2:DisassociateAddress" "ec2:ModifyNetworkInterfaceAttribute" "ec2:ReplaceRoute" "ec2:UnassignPrivateIpAddresses"

You can set permissions after selecting all applicable services in "Visual Editor" or directly set permissions in "JSON".

[Example of configuration format when all permissions of AWS resources are included]

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:AssociateAddress",
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DeleteRoute",
                "ec2:DescribeAddresses",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DisassociateAddress",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ReplaceRoute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": "*"
        }
    ]
}
```

4. Add tagging (optional)
   Adding tags is optional and, if set, can help identify or search for resources.



5. Review policy creation.
   Review the settings and complete.

3.1.2 VPC Creation

1. After searching for VPC services, click the [Create VPC] button.

2. Create a VPC after specifying a name (tag) and CIDR block.

3.1.3 Subnet Creation

1. Click the [Create Subnet] button.

2. Select the VPC you created earlier.

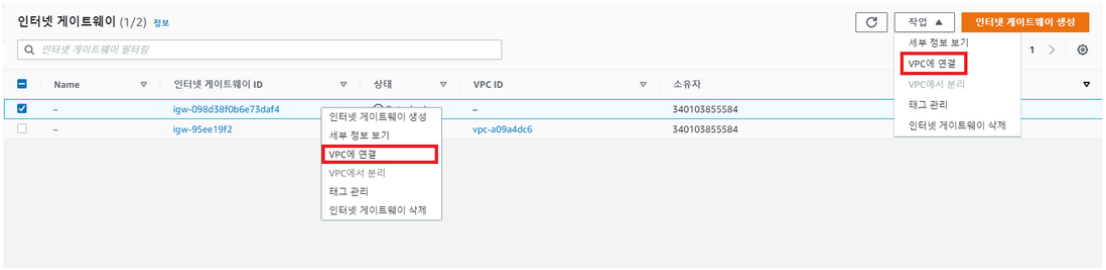
3. Create a subnet after specifying the subnet name, Availability Zone, and CIDR block.
   ※ When using multiple subnets in one instance, the Availability Zones must be matched.

3.1.4 Gateway Settings

1. Click the [Create Internet Gateway] button.

2. After creating a name (tag), create an internet gateway.

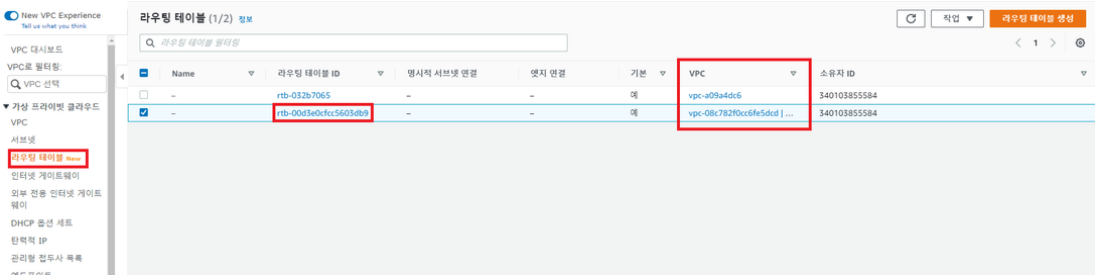
3. After confirming the VPC ID, click the corresponding “Route Table ID”.
   Alternatively, click [Connect to VPC] on the Tasks tab.



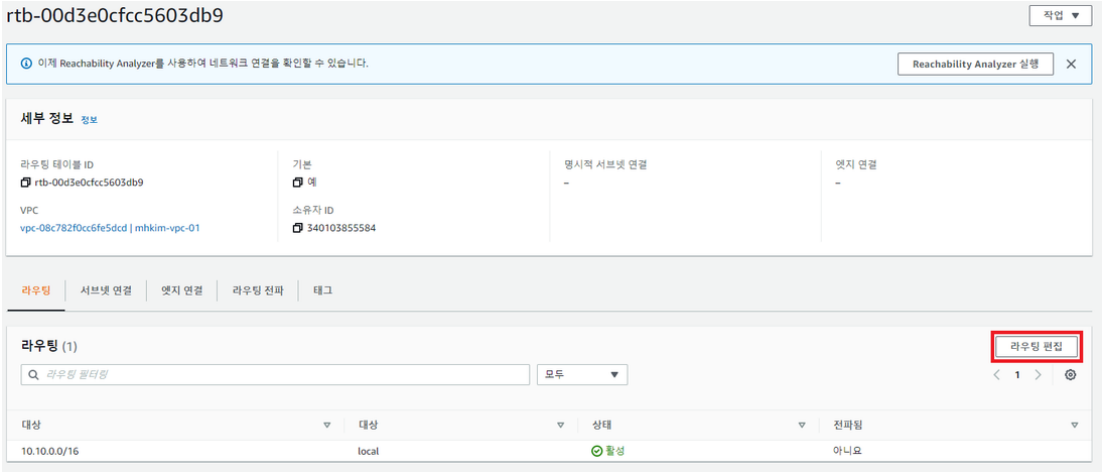
   After selecting a VPC, click [Internet Gateway Connection].

4. Add an internet gateway to the route table of the VPC you created in step 1.

   After confirming the VPC ID, click the corresponding “Route Table ID”.

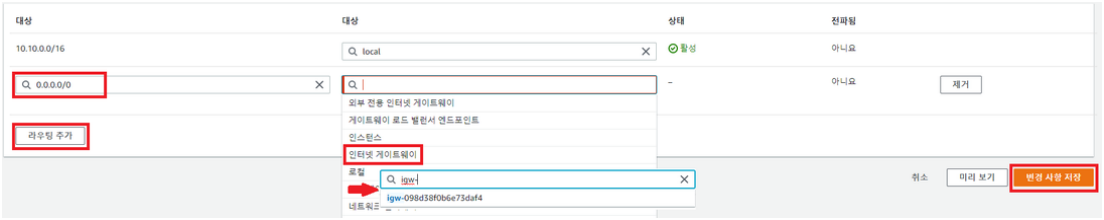


5. Click [Edit Routing].



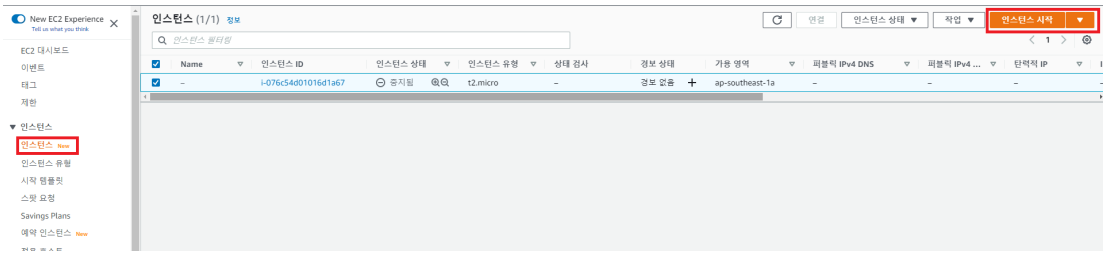
6. After clicking [Add route], specify the destination (0.0.0.0\0) and select the created Internet gateway.

   After confirming the contents, click [Save Changes]



3.1.5 Instance Creation

1. After searching for EC2 service, click the [Start Instance] button.



2. Specify the instance name and select the OS type and detailed version to use.
   MCCS AWS supports both Windows and Linux.

3. Select the type that matches the performance of the instance you want to use, and create or select a key pair for the user who will use that instance

4. Click [Edit] in Network Settings and select the information below.

5. After selecting Advanced Network Configuration, enter the required information in “Network Interface 1” and click [Add Network Interface].

6. Enter the same information in “Network Interface 2”.

7. Set the storage in “Storage Configuration” and click [Start Instance] after setting “Number of Instances”.

3.1.6 AWS CLI Installation

To manage AWS resources in MCCS, the AWS CLI must be installed in advance.
When installing the MCCS program, the installation of the AWS CLI (AWS Command Line Interface) is supported. However, users must manually install it if they have not previously installed it or if the installation fails.
If you manually install the AWS CLI, see "Install or update the latest version of the AWS CLI" in the AWS Manual.

To use the AWS CLI, you must be connected to the regional endpoint and the Internet. Also, since you use the AWS CLI, you need a profile of the AWS CLI and setting information to configure the profile.

Required information
AWS Access Key ID
AWS Secret Access Key
Region name

Finally, the output format should be specified in the default json format.
Since the AWS CLI operates as a service execution account, the AWS CLI profile must be configured in the home directory of the service execution account or an environment variable specifying the location of the config file must be added.
We do not support using the AWS CLI without a profile because each setting in the profile must be specified as an environment variable.

3.1.7 User Settings

3.1.7.1 User Access Type

When adding a user or adding a user to a user group created to manage AWS resources, the user's access type must be set to "Access Key - Programmatic Access".

3.1.7.2 User Security Credentials

When adding a user, the settings below are required.

1. Check your access key ID and secret access key, and download the ".csv" file.

2. Certify user security credentials.
   Set the access key using the "aws configure --profile" command in the cmd window.

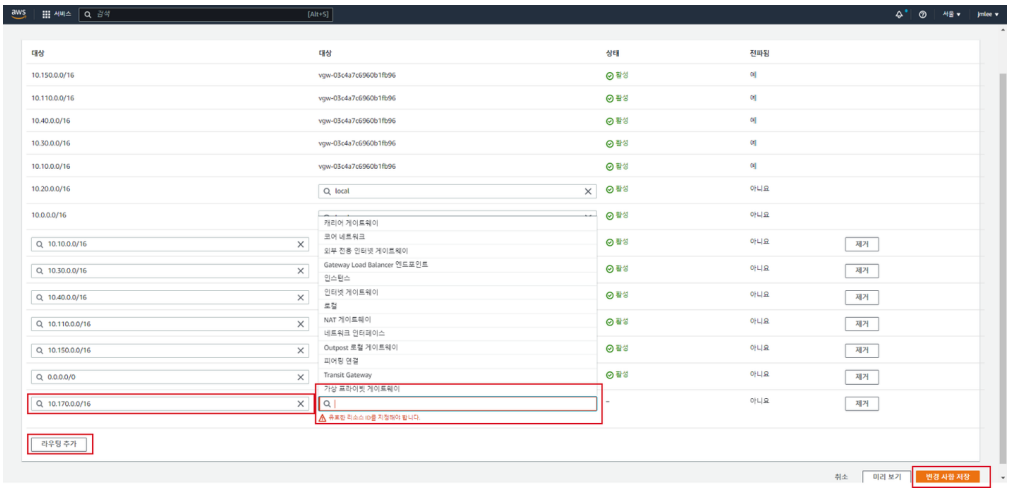
```
C:\Users\Administrator>aws configure --profile Username
```

```
AWS Access Key ID [NONE]: Access key ID
AWS Secret Access Key [**********************]: Secret access key
Default region name [지역명]: Area name
Default output format [None]:
```

3.1.8 Overlay IP(OIP) Settings

When adding an Overlay IP resource of MCCS, a routing table IP must be set.

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose “Routing Tables” and then choose your route table
3. Select Actions > “Edit Routing”.
4. To add a route, click [Add Route]. In Destination, enter the ID of the destination CIDR block, single IP address, or prefix list.



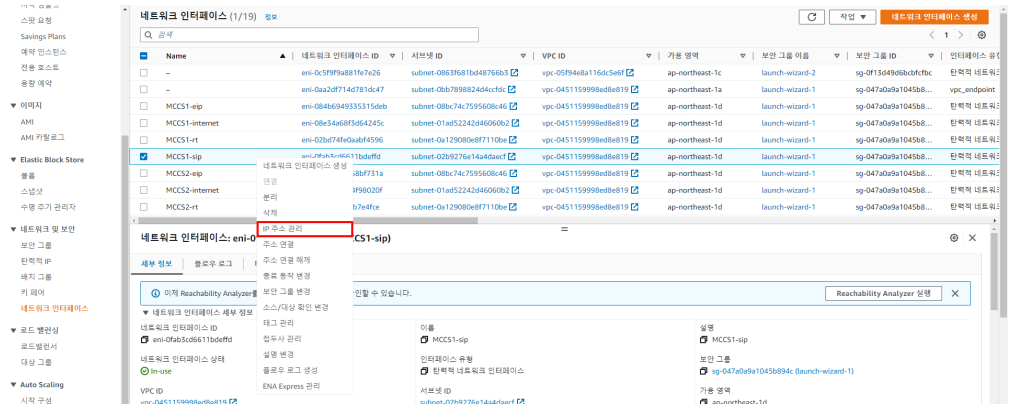
5. To modify the routing, replace the destination CIDR block or single IP address in Destination. Select a target in Target.
6. Click [Remove] to delete the route
7. Click [Save Changes].

3.1.9 Secondary private IP (SIP) Settings

When adding Secondary private IP resources of MCCS, you need to set secondary private IP.

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose “Network Interfaces” and then choose the [Network Interface] connected to your instance.

3. Select Actions > “Manage IP Addresses”.

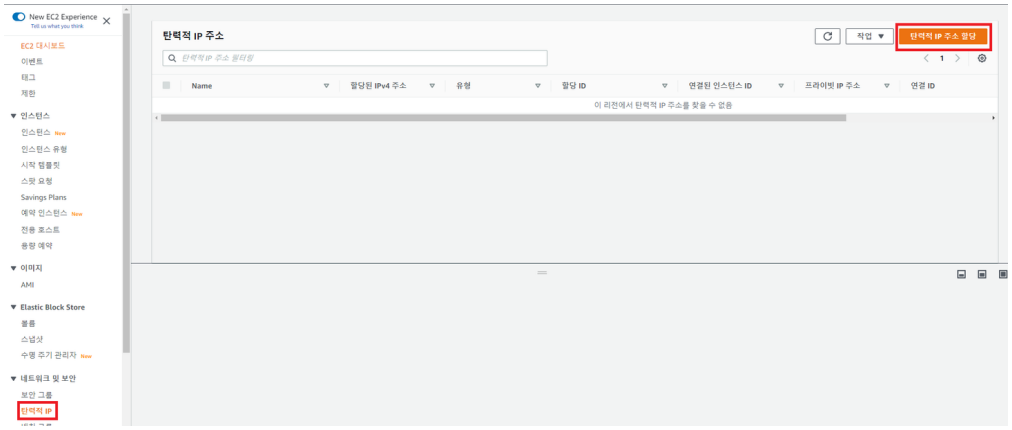


4. Select Allocate New IP from IPv4 Address.
5. Enter a specific IPv4 address within the range of your instance's subnet. Alternatively, leave the field blank and Amazon will automatically select an IP address for you.
6. (Optional) If you select Allow reassignment, the secondary private IP address will be reassigned if another network interface is already assigned.
7. Choose [Yes, Update].

3.1.10 Elastic IP (EIP) Settings

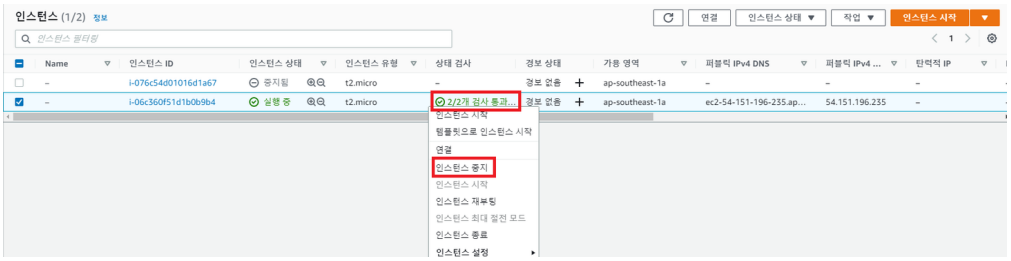
When adding an Elastic IP resource in MCCS, you need to create an Elastic IP.

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. Select “Elastic IP” in the navigation pane and click [Assign Elastic IP Address].

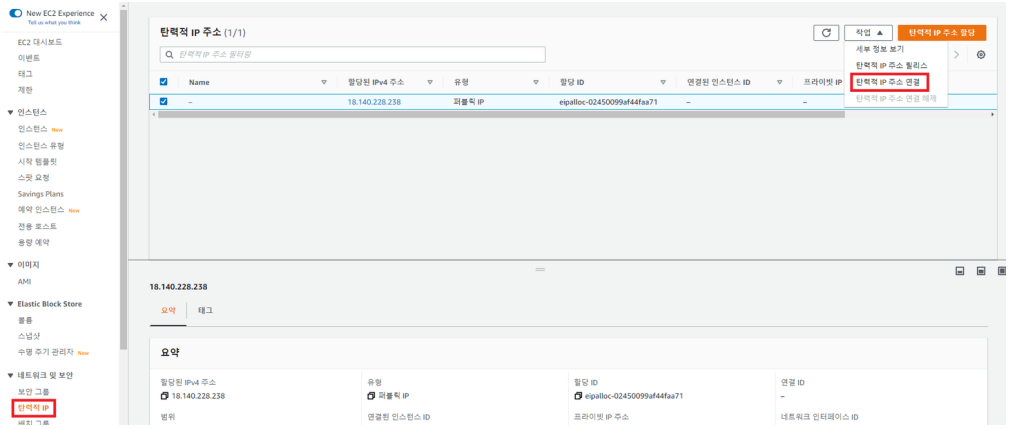


3. Click the [Assign] button.

4. Click [Stop Instance] and attach an Elastic IP to the created network interface. After confirming that “Check Status” is in the initialization state, select the instance, right-click and stop the instance.

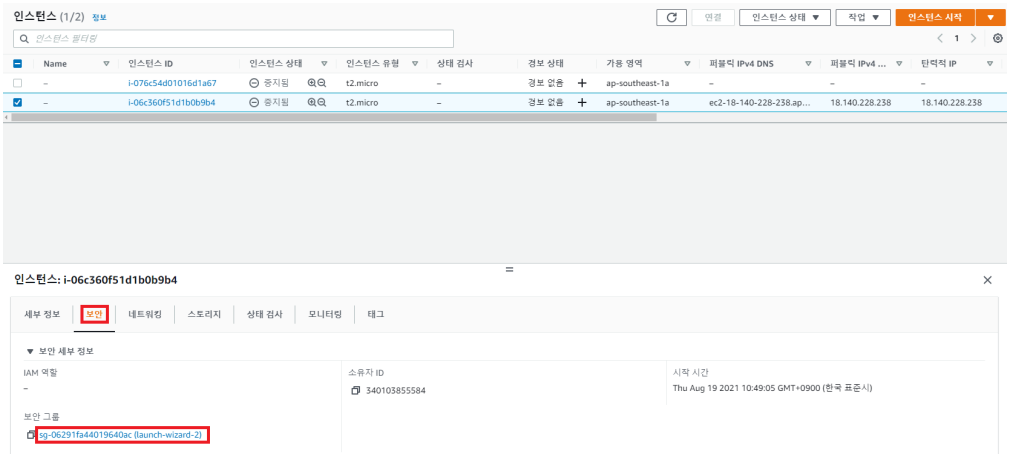


연결할 IP를 체크 후 작업 탭에서 [탄력적 IP 주소 연결]을 클릭합니다.

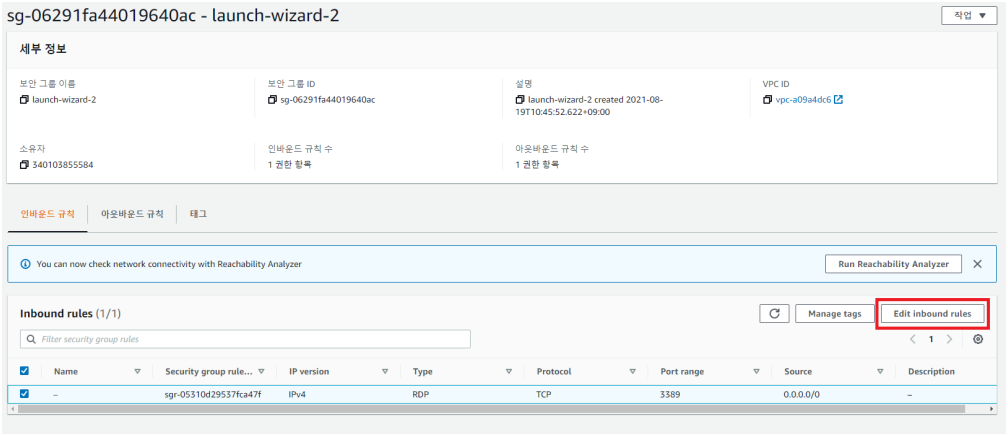


5. After selecting an instance, click [Connect].

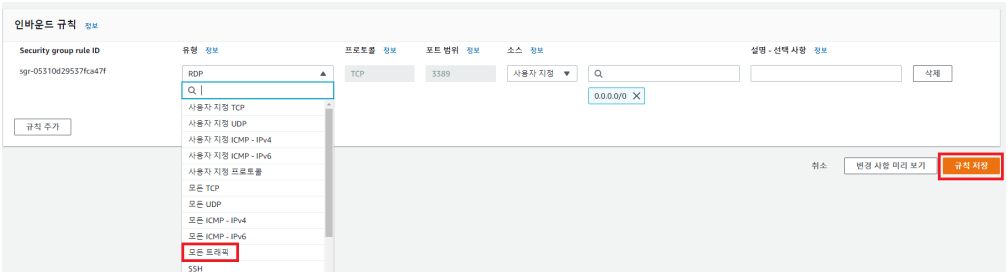
6. Set the inbound rule of the instance “security group” to all traffic, 0.0.0.0/0.
After selecting the instance, click “Security Group” in the Security tab.



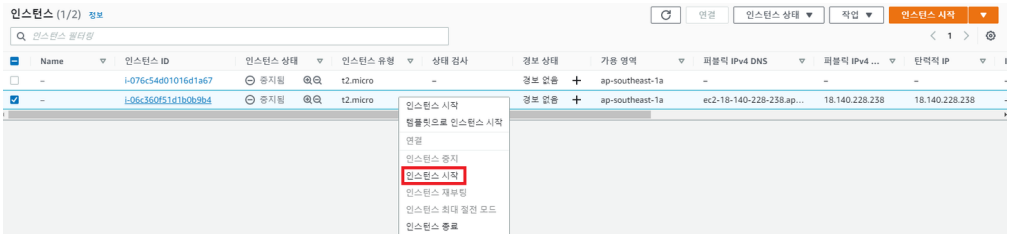
.Click the [Edit Inbound Rules] button.



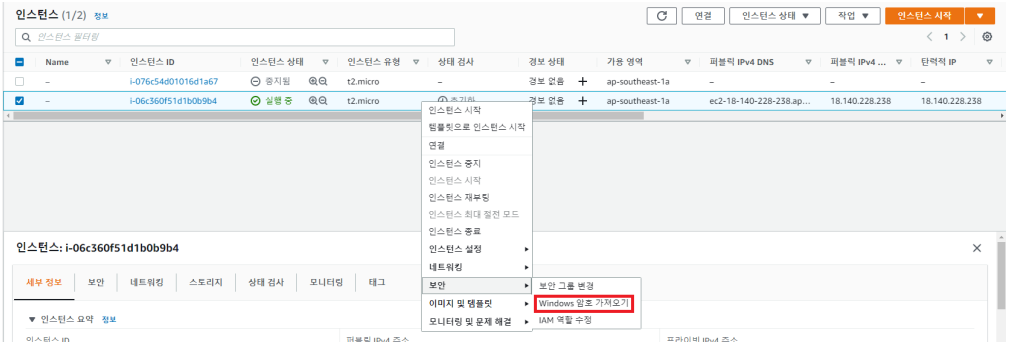
Change the type of inbound rule to “All Traffic” and save the rule.



7. (Windows) Right-click the instance > Security > Obtain the password of the administrator through [Get windows password] and connect remotely.
Right-click the instance and click [Launch Instance].



Right-click the instance > click [Get Windows Password] in the Security tab.



After selecting the downloaded key pair, click [Code-breaking].

Remotely access the connected elastic IP using the printed account information.

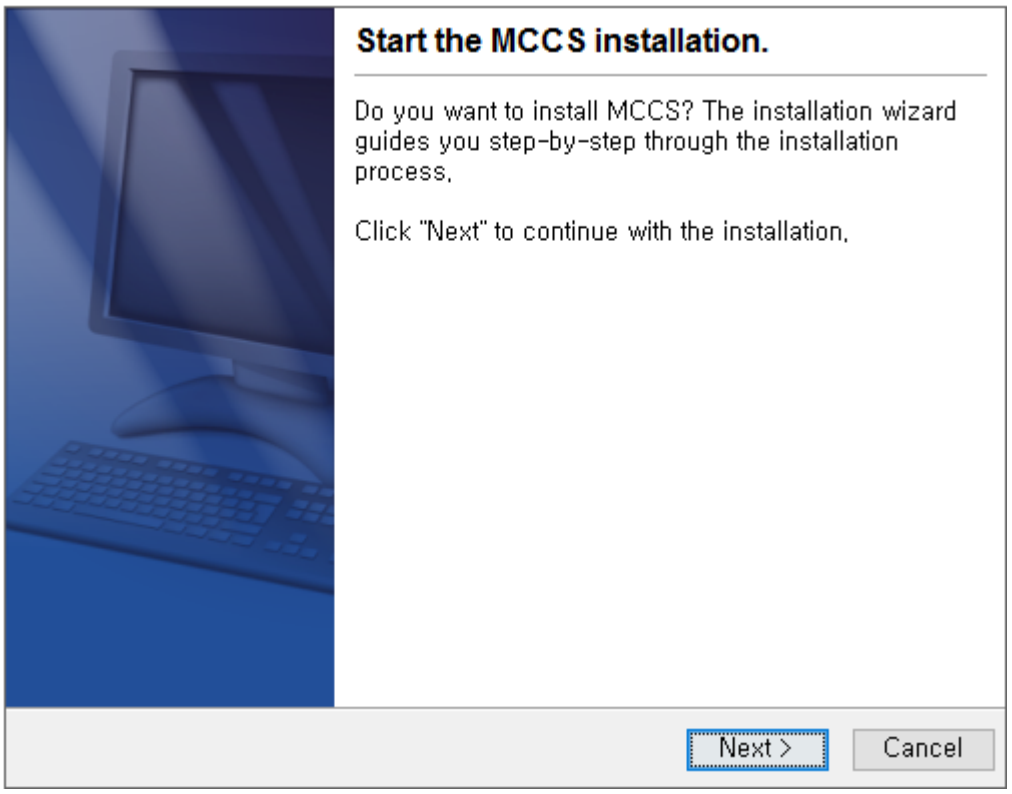
3.2 MCCS Installation Settings

3.2.1 MCCS Installation

1. Insert installation media
   After inserting the MCCS installation media, run the file.
   The installation file varies depending on the version of the operating system.

2. language selection
   When you run the installation file, the installation language selection screen appears..
   Language can be selected between "Korean" and "English". The selected language will be used as the default language of MCCS.
   The default is "Korean".

3. Install start
   The initial screen of the installation wizard is displayed.
   Click the [Next] button to move to the next screen.



4. license agreement
   The product's license is displayed.
   This step asks whether to agree to the license agreement.

5. Select installation folder
   This is the step to set the folder to install MCCS.
   You can select another path after clicking [Browse]. The default is "C:\Program Files\MCCS".

6. Select start menu folder
   If you check "Create shortcut for all users", MCCS shortcut start menu is set for all Windows users.

7. Single node cluster setup
   You can choose to set up a single node cluster.
   When selecting a single node cluster, MCCS will operate on one server.
   Do not select if you are configuring a cluster with two nodes.

8. Install redundancy program and data replication program
   You can choose whether or not to install the data replication program while installing the MCCS redundancy program.
   When configuring a mirror disk resource, be sure to install "Data Replication Program".

3.2.2 Network card, Network address Resource Settings

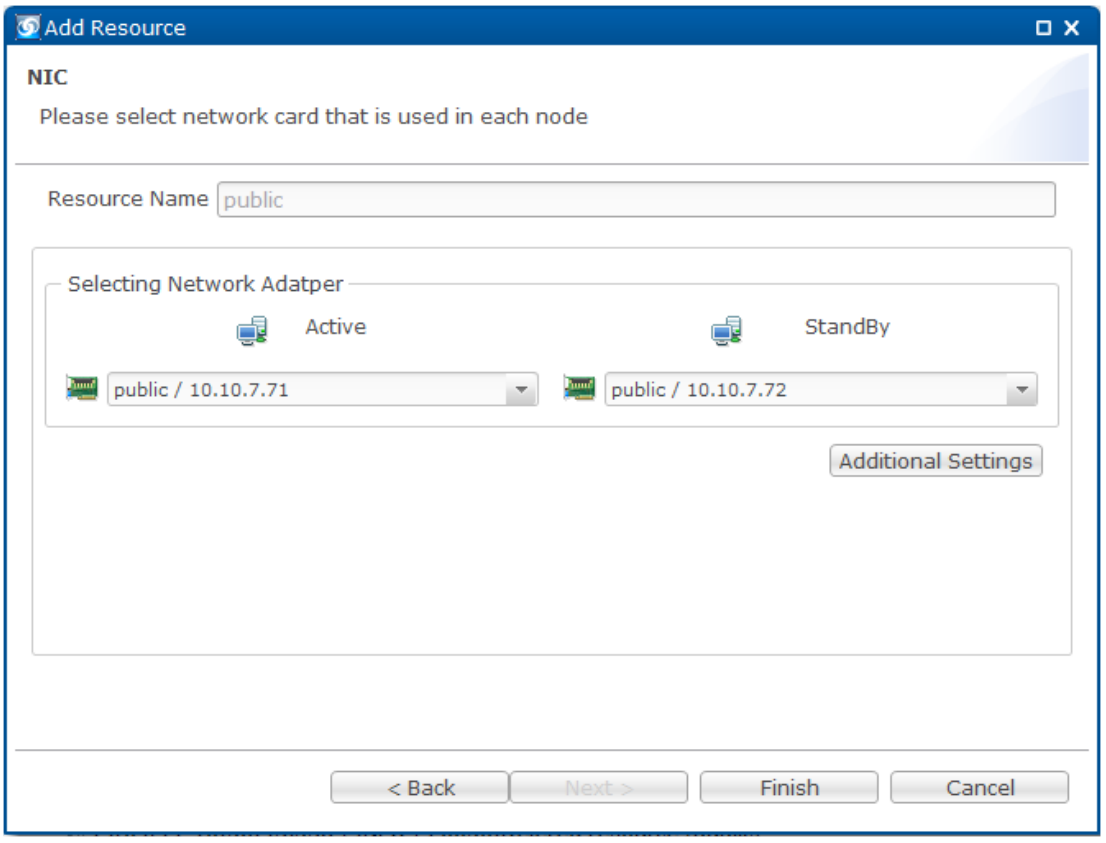
Add a preconfigured network card resource and add a network address resource to set the virtual IP.

3.2.2.1 Add Network Card Resources

1. Select a resource group → right-click → select [Add Resource]

2. Select “Network Card” in the Resource Wizard and click the [Next] button.

3. Enter a resource name and select a network adapter.
   Selecting a network adapter provides a suggested name. You can create a new name in addition to the suggested name.
   If the name is already used by another resource or is a reserved keyword, such as network card (NIC) or process, you cannot use it as a resource name.

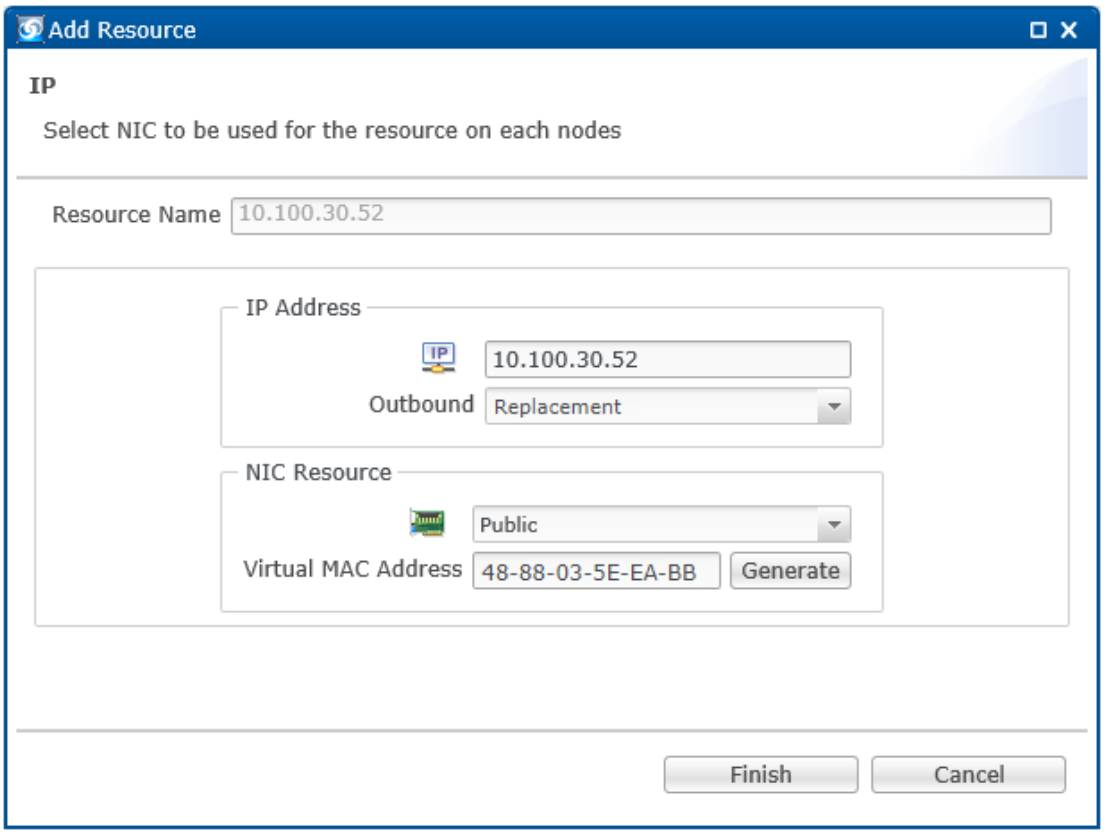


3.2.2.1 Add Network Address Resources

1. Select a resource group → right-click → select [Add Resource]

2. Select “Network Address” in the Resource Wizard and click the [Next] button.

3. Enter the resource name, virtual address and select the network card.



List		Explanation
Virtual address	Virtual IP Address	When configuring AWS, it can only be configured with IPv4.
	Outbound	Changes all source addresses used in communication to virtual addresses specified in the network address resource. Even if a different network address is set on the network card, it communicates with the virtual address according to the Outbound setting. - None (default): No outbound is applied. - Replacement: Deletes the address set in the network card and assigns the virtual address set in the network address resource to the network card. If you take the network address resource offline, it will be restored again. - SkipAsSource: Maintains the address set in the network card and communicates with the outside only with the virtual address set in the network address resource.
Network Card	Network Card	Select the network card added first in Network Card Resources.

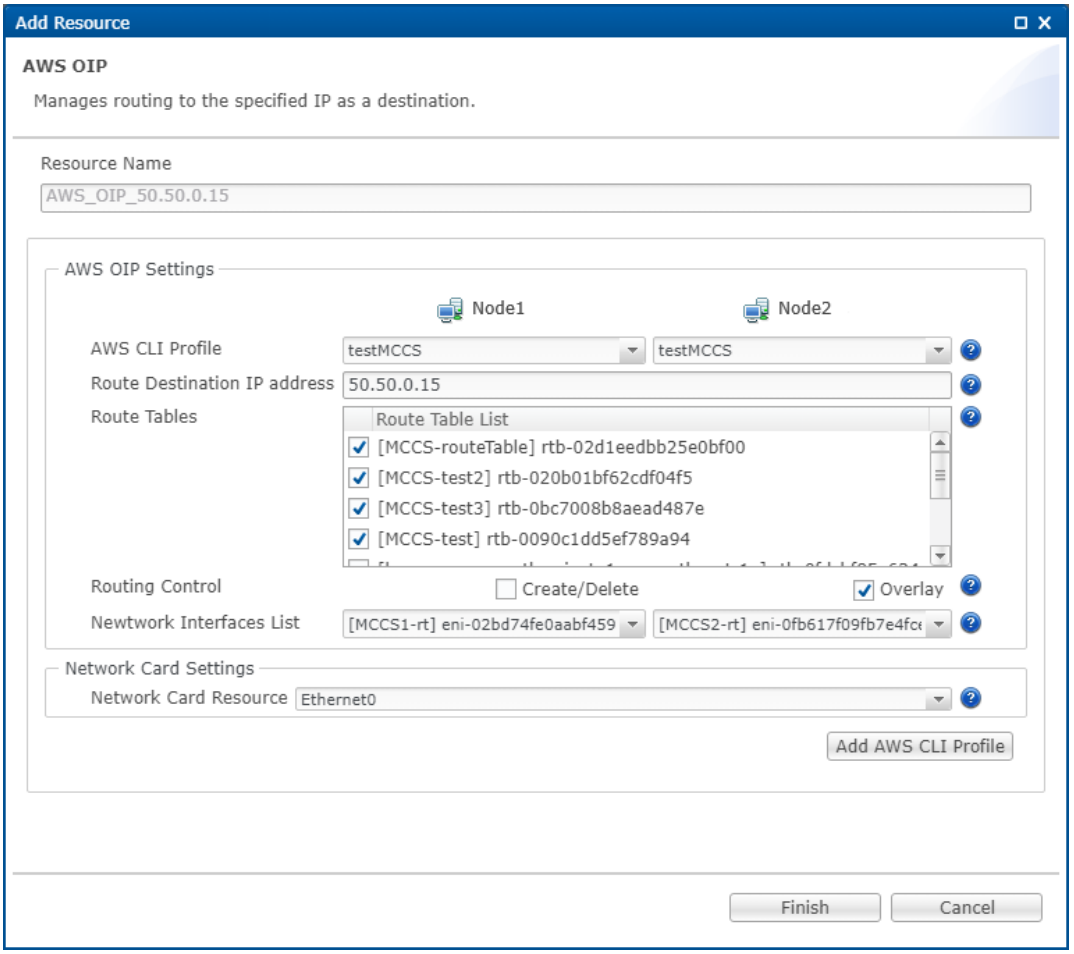
Resource	Virtual MAC Address Setting	Set the MAC addresses of the network cards of both nodes to one virtual MAC address. If communication is possible with only one MAC address, this must be set. If you select a network card and click the [Generate] button, the first 6 digits (48-88-03) and the remaining 6 digits of the Organization Unique Identifier (OUI) are randomly assigned to "48-88-03-XX-XX-XX" " to create a virtual MAC address.

3.2.3 Add Overlay IP Resources

1. Select a resource group → right-click → select [Add Resource]

2. Select “AWS Overlay IP Resource” in the resource wizard and click the [Next] button.

3. Select and enter the settings of the pre-configured AWS routing table.
   ※ AWS CLI profile settings added to AWS resources in MCCS must not be changed in AWS.



List	Explanation
AWS CLI Profile	A list of pre-configured AWS CLI profiles for both nodes is output. Validate AWS CLI profiles on both nodes.

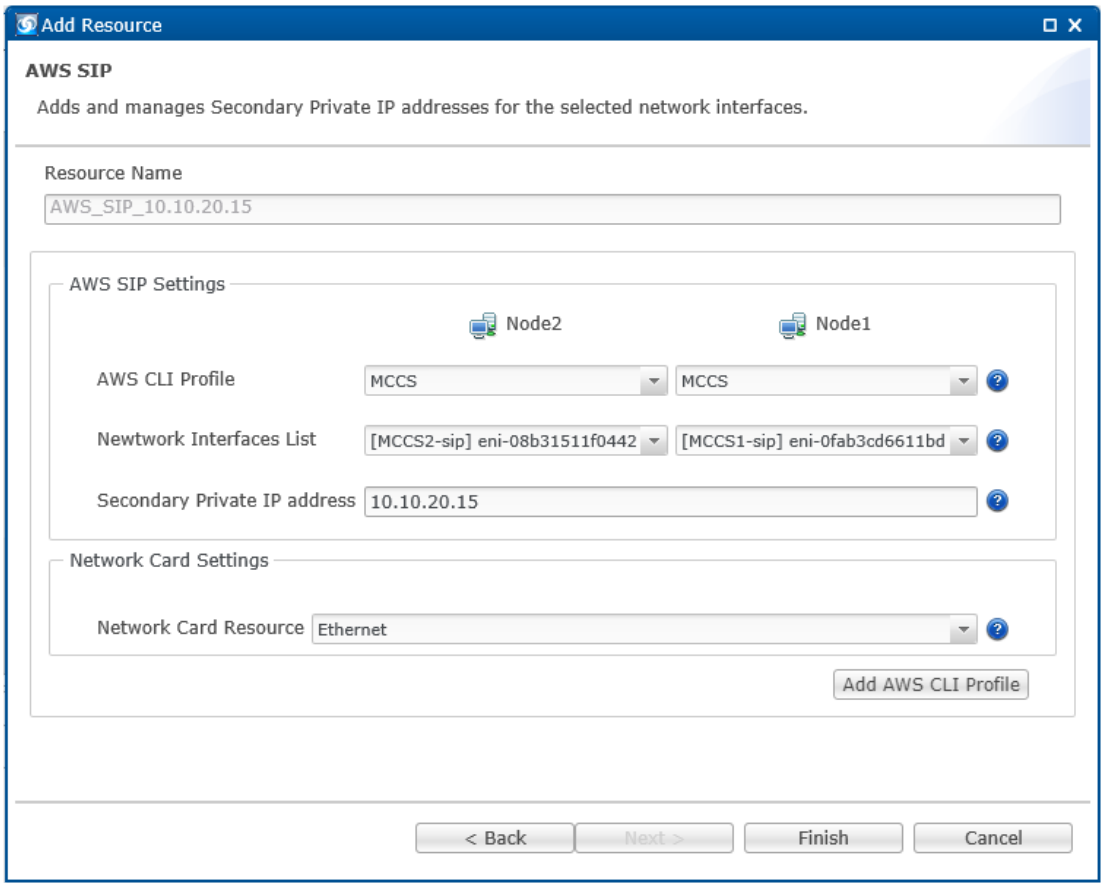
Route Destination IP Address		This is the Virtual IP address to be registered as a routing table destination when the resource is online. When adding a virtual IP address of an existing network address resource or adding a new virtual IP address, you must add a network address resource with the IP address after adding the AWS Overlay IP resource. When you enter a routing destination address, it is compared to the network band within the CIDR declared in the VPC to verify that it is an appropriate IP address. Set the routing destination address to a band outside of the CIDR band you declared in your VPC. For example, if the CIDR of your VPC is 10.10.0.0/16, the route to address cannot use the band 10.10.~.~/32.
Route Tables		A list of pre-configured routing tables is output.
Routing management	Overlay	Manage routing through Replace.(ec2:ReplaceRoute) Default is Overlay. Online: Change route destination via Replace Offline: nothing works
	Create/Delete	Manage routing through "create/delete" of routing. ("ec2:CreateRoute", "ec2:DeleteRoute") Online: Create a route Offline: remove routing
Network Interfaces List		A list of pre configured network interfaces on both nodes is printed. Verify that you have selected different network interfaces on both nodes.

3.2.4 Add Secondary Private Resources

1. Select a resource group → right-click → select [Add Resource]

2. Select “AWS Secondary Private IP Resource” in the resource wizard and click the [Next] button.

3. Select and enter the pre-configured AWS secondary private IP settings.
   ※ AWS CLI profile settings added to AWS resources in MCCS must not be changed in AWS.



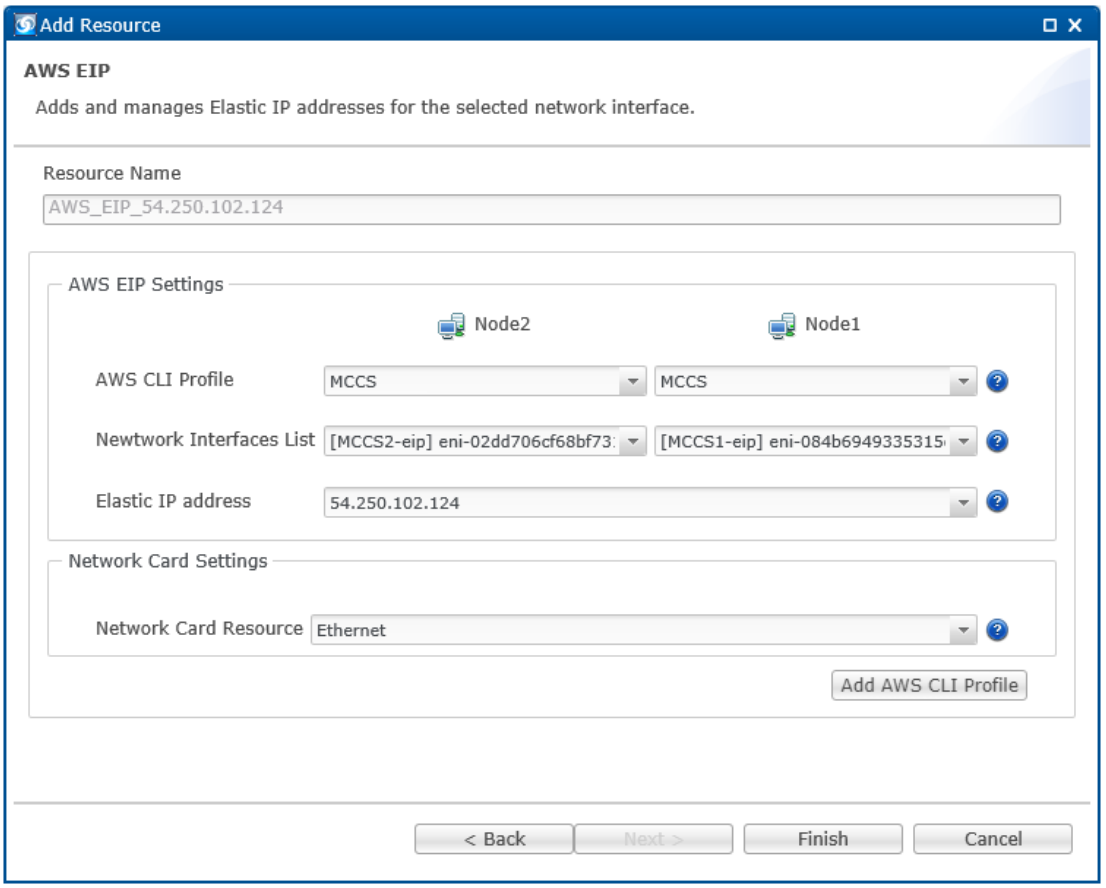
List	Explanation
AWS CLI Profile	A list of pre-configured AWS CLI profiles for both nodes is output. Validate AWS CLI profiles on both nodes.
Network interface list	A list of pre-configured AWS network interface IDs for both nodes is output. Verify that different network interfaces on both nodes are selected.
Secondary private IP address	The virtual IP address that will be registered as a secondary private IP address when the resource comes online. If you add a virtual IP address of an existing network address resource or add a new virtual IP address, you must add a network address resource with the corresponding IP address after adding the AWS secondary private IP resource. When you enter a secondary private IP address, it is compared to the subnet CIDR of the AWS network interface to validate that it is a valid IP address. Set a secondary private IP address that falls within the subnet CIDR band. For example, if the subnet's CIDR is 10.10.0.0/24, the secondary private IP address should be set in the range 10.10.0.~/32.
Network Card Resource	A list of pre-configured network card resource information is output.

3.2.5 Adding Elastic IP Resources

1. Select a resource group → right-click → select [Add Resource]

2. Select “AWS Elastic IP Resource” in the resource wizard and click the [Next] button.

3. Select and enter the preconfigured AWS Elastic IP settings.
   ※ AWS CLI profile settings added to AWS resources in MCCS must not be changed in AWS.



List	Explanation
AWS CLI Profile	A list of pre-configured AWS CLI profiles for both nodes is output. Validate AWS CLI profiles on both nodes.
Network interface list	A list of pre-configured AWS network interface IDs for both nodes is output. Verify that different network interfaces on both nodes are selected.
Elastic IP address	The IP address that will be registered to the Elastic IP address when the resource comes online.
Network Card Resource	A list of pre-configured network card resource information is output.

3.2.6 Dependency Settings

After completing the configuration of AWS-related resources, set network card resources, network address resources and dependencies.

Type	Configuration example	Resource Name	Explanation
AWS OIP Resource		Network address resource AWS OIP Resource Network Card Resource	AWS Overlay IP resource must configure network card resource and network address resource. Also, since IP addresses are additionally assigned inside the instance, dependencies must be set for the network card resource, network address resource, and AWS overlay IP resource in the order shown in the example. If the AWS overlay IP resource becomes the parent resource and the network address resource becomes the child resource, communication may not be possible even though the IP address is assigned.
AWS SIP Resource		Network address resource AWS SIP Resource Network Card Resource	AWS Secondary Private IP resource must configure network card resource and network address resource. In addition, since additional IP addresses are assigned inside the instance, dependencies must be set for the network card resource, network address resource, and AWS secondary private IP resource in the order shown in the example. If the AWS secondary private IP resource becomes the parent resource and the network address resource becomes the child resource, communication may not be possible even though the IP address is assigned.
AWS EIP Resource		AWS EIP Resource Network Card Resource	The AWS Elastic IP address must configure the network card resource, and the network card resource and AWS secondary private IP resource must set dependencies in the order shown in the example.

4. Operational Support

4.1 Regular maintenance management

Get the most out of your product with the latest releases and technical support services.
Maintenance fees are determined by the developer's policy and include services related to development and upgrades to the latest release.
Details of maintenance and technical support may vary according to the license agreement.
Maintenance is broadly divided into:
- Regular maintenance
- Emergency maintenance

※ Maintenance is performed according to the contract.
▸Service center) 1833 - 7790

The scope of regular maintenance is as follows.
- Periodic product inspection
- Certificate management
- Patches and upgrades

4.2 Emergency maintenance management

In the event of a sudden MCCS failure, the failure is resolved according to the maintenance contract.

Describes simple product control methods, failure types and solutions.

4.2.1 Service Control

This is a command to stop and start the MCCS service when recovering from an MCCS failure.

1) Start MCCS service

OS	Explanation	Command
Window	Start MCCS service.	“services.msc” > MCCS service start
	Start MCCS service.	service mccs_agent start
Linux	Start MCCS service.	- service mccs_agent start - systemctl start mccs_agent

2) Stop MCCS service

OS	Explanation	Command
Window	Stop MCCS service.	“services.msc” > MCCS service stop
	Stop MCCS service.	service mccs_agent stop

Linux	Stop MCCS service.	- service mccs_agent stop - systemctl stop mccs_agent

4.2.2 Status Check

This command checks the MCCS service status.

1) MCCS Status Check

OS	Explanation	Command
Window	Check the MCCS service status.	“services.msc” > Check MCCS service status
	Check the MCCS service status.	service mccs_agent status
Linux	Check the MCCS service status.	- service mccs_agent status - systemctl status mccs_agent

4.2.3 Failure Type

1) If communication fails due to network card or network IP change, etc.
2) If MCCS initial heartbeat setting fails in the environment where the security solution is installed

4.2.4 Failure Recovery Procedure

Case1. When changing network-related settings or firewalls

→ In case of advance change

1. resource group offline
2. Delete related dependencies
3. Delete network related resources (network card, network address)
4. Re-add that resource with changes
5. reset dependencies

→ In case of sudden change

If network disconnection occurs for any reason in the operating node (A node) of the cluster, B node, which was a standby node (B node), is changed to an operating node and operated again.

Case2. If MCCS initial heartbeat setting fails in the environment where the security solution is installed

→ The security solution handles the following exceptions.

[Directory]

OS	Directory	Explanation
Windows	C:\program Files\MCCS	MCCS service for operation of redundancy solution
Linux	/opt/MCCS	MCCS service for operation of redundancy

		solution

[File]

OS	File	Explanation
Windows	C:\program Files\MCCS\bin\mccsserver.exe	An engine process that monitors and controls nodes and resources.
	C:\program Files\MCCS\bin\MccsAgentService.exe	MCCSServer.exe is a management process that monitors whether it is running.
	C:\program Files\MCCS\bin\dskdrv.vbs	You can check the list of disks in dskdrv.vbs.
Linux	/opt/MCCS/bin/mccsserver.exe	An engine process that monitors and controls nodes and resources.
	/opt/MCCS/bin/MccsAgentService.exe	MCCSServer.exe is a management process that monitors whether it is running.
	/opt/MCCS/bin/dskdrv.vbs	You can check the list of disks in dskdrv.vbs.dskdrv.vbs에서 디스크 리스트 확인할 수 있습니다.

4.2.5 Recovery procedure in case of failure recovery

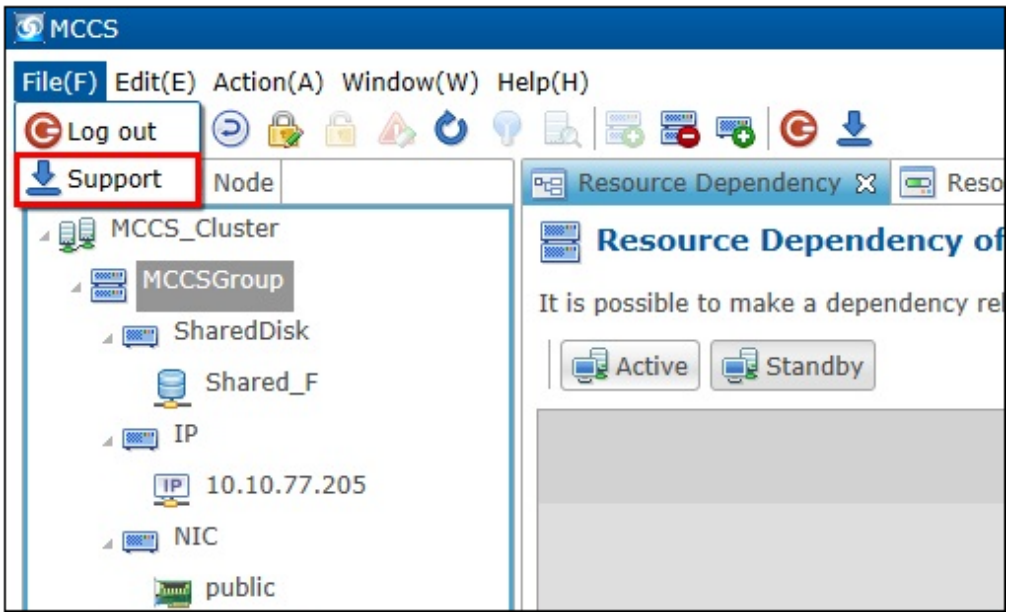
After collecting support files, upgrade the MCCS version.

4.2.5.1 Collecting Support Files

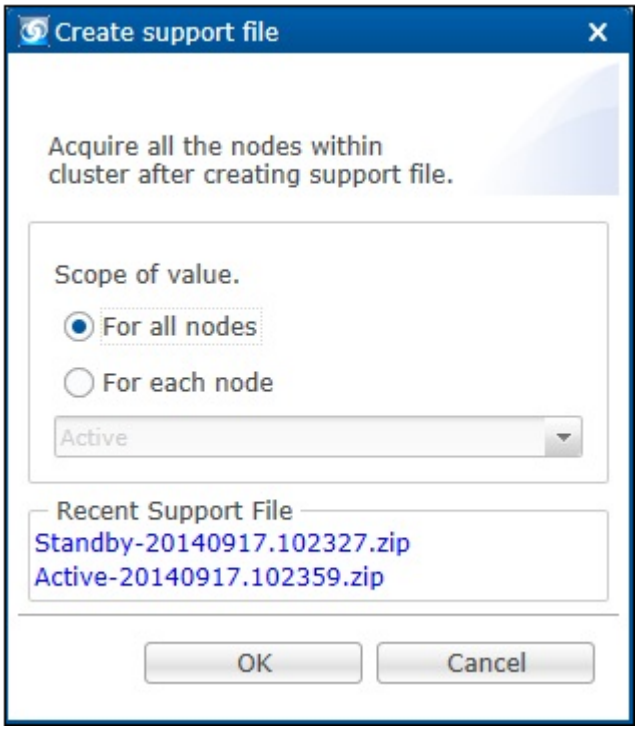
1) Collecting support files

When a problem occurs in MCCS, log information and environment information can be collected through support files.

1. In the MCCS web console, click [Support] in [File (F)] of the menu bar to collect support files.



2. You can choose to receive support files from all nodes or per node.
   You can also re-download previously received support files.



3. Click the [OK] button to start collecting support files.

[Support file contents]

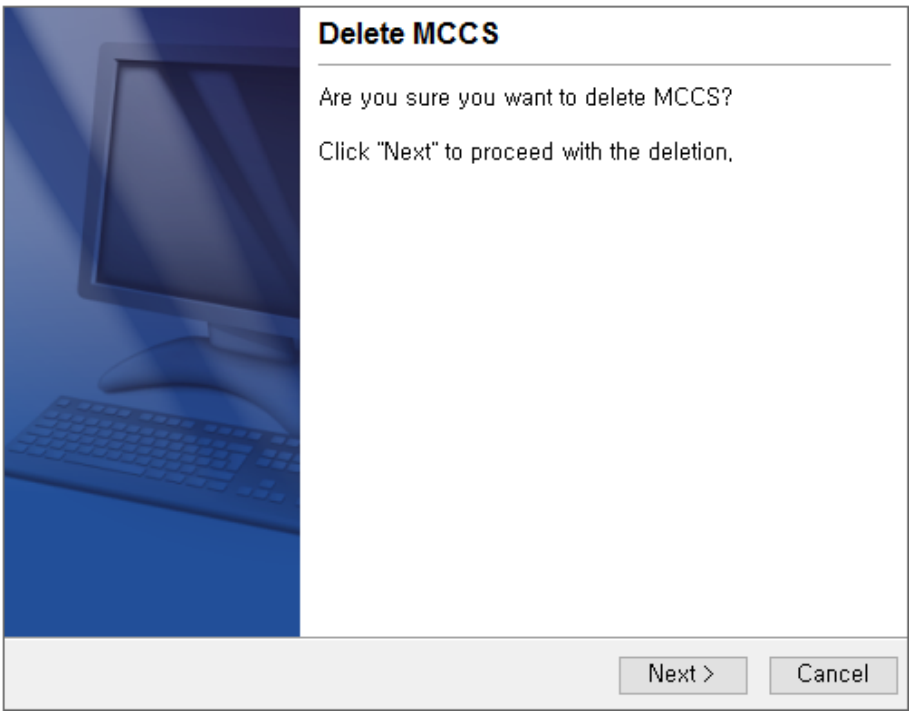
MCCS directory	config	Directory containing configuration files for MCCS installation and operation - main.json: resource, resource group information - hb.json: heartbeat information
	ini	Information required for initial setup of an application or window

	jvmdump	java dump file
	logs	MCCS log file
	script	Script files required when configuring MCCS
ProcessInfo	Provide process items used in the operating system	
System	System information	
Systeminfo	Provide system information through Windows commands	

4.2.5.2 MCCS version upgrade

1. Delete MCCS
    a. Windows: Execute "uninstall.exe" in the directory (folder) where MCCS is installed.
    Linux: Go to the home directory where MCCS is installed (cd $MCCS_HOME) and run the uninstaller (./uninstall).

    b. This is the initial screen for MCCS program deletion..
    To proceed with deletion, click the [Next>] button.
    After selecting and deleting the relevant items according to the environment configuration, the MCCS deletion is completed.



2. MCCS version upgrade installation
    Proceed with reinstallation according to [3.2 MCCS Installation Settings].
    Reflect the necessary content among the contents in the support file.

4.3 RTO

Once a single configuration is deployed, an RTO will occur if an admin error occurs. You will need to recreate the AMI using a snapshot of the existing installer and reinstall the AMI. Occurs from a minimum of 10 minutes to a maximum of 30 minutes.

5. System Management

5.1 Connect to the GUI using VNC

1. Install the TigerVNC software on your local computer if it is not already installed. TigerVNC is available for Windows, Linux and macOS. To access downloads, see the TigerVNC website.

   Linux: The “tigervnc” package is available in the repositories of many distributions and can be installed using their respective package managers.
   macOS: Download and install “TigerVNC-x.y.z.dmg”. where x.y.z represents the latest version.
   Windows: Download and install “tigervnc64-x.y.z.exe” (64-bit) or “tigervnc-x.y.z.exe” (32-bit). where x.y.z represents the latest version.

2. Connect to the instance using SSH while creating a tunnel from your local computer that forwards all traffic on local port 5901/TCP (VNC) to the instance's VNC server.

   Linux 와 macOS

   Enable port forwarding by adding the -L parameter when connecting to your instance using SSH. Replace PEM_FILE with your private key and INSTANCE_IP with the instance's public or private IP, as appropriate.

   ```
   >> ssh -L 5901:localhost:5901 -i PEM_FILE ec2-user@INSTANCE_IP
   ```

   Windows

   Configure port forwarding and open a connection when opening a connection with PuTTY.

   a. Choose [SSH] from the [Connection] menu, then choose [Tunnels].
   b. Enter 5901 in the Source Port field.
   c. Enter localhost:5901 in the Target field.
   d. Choose Add.
   e. From the [Connection] menu, choose [SSH], then choose [Auth].
   f. Enter the pem file in Private key file for authentication.
   g. Open a connection and connect as ec2-user.

3. Open TigerVNC Viewer on your local computer. When prompted for the hostname of the VNC server, enter localhost: 1 then connect to it.

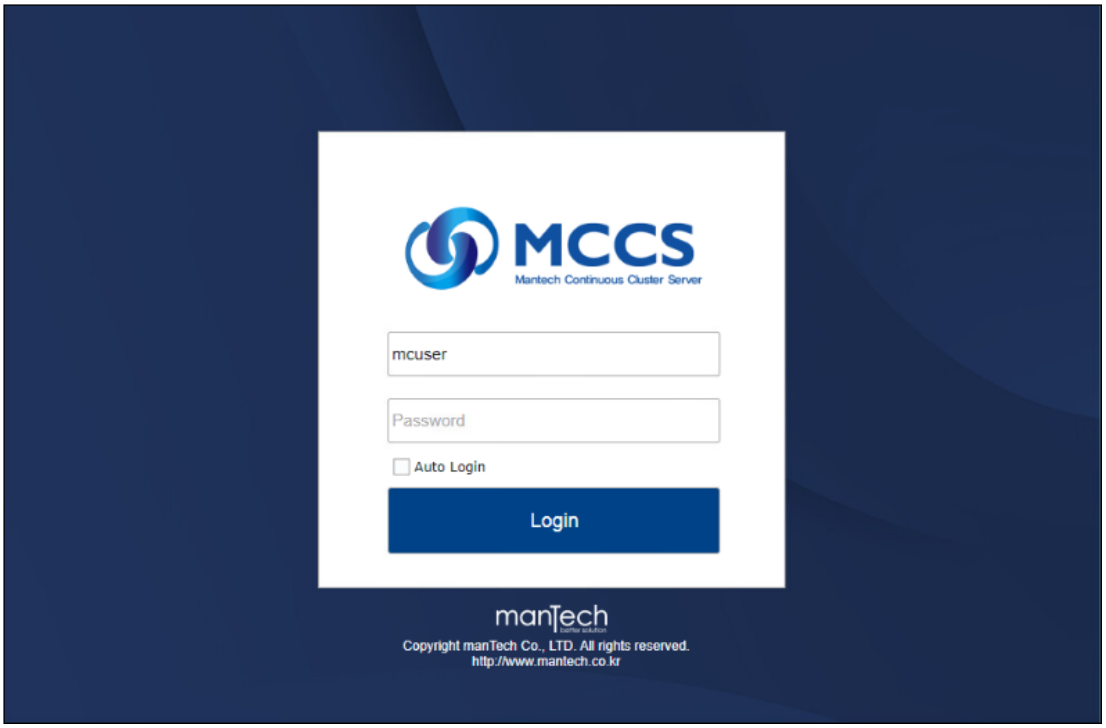
4. Enter the VNC password you set in Step 2 of the Installing TigerVNC section. If you receive a notification that your connection is not secure, ignore it. You are accessing

the VNC server using an encrypted SSH tunnel.

5. The MATE desktop environment is displayed.

5.2 Login

Run a web browser (Firefox, Chrome) on your PC.
Enter 'https://serverIP:11080/main' in the address bar of the web browser and access the MCCS login screen.



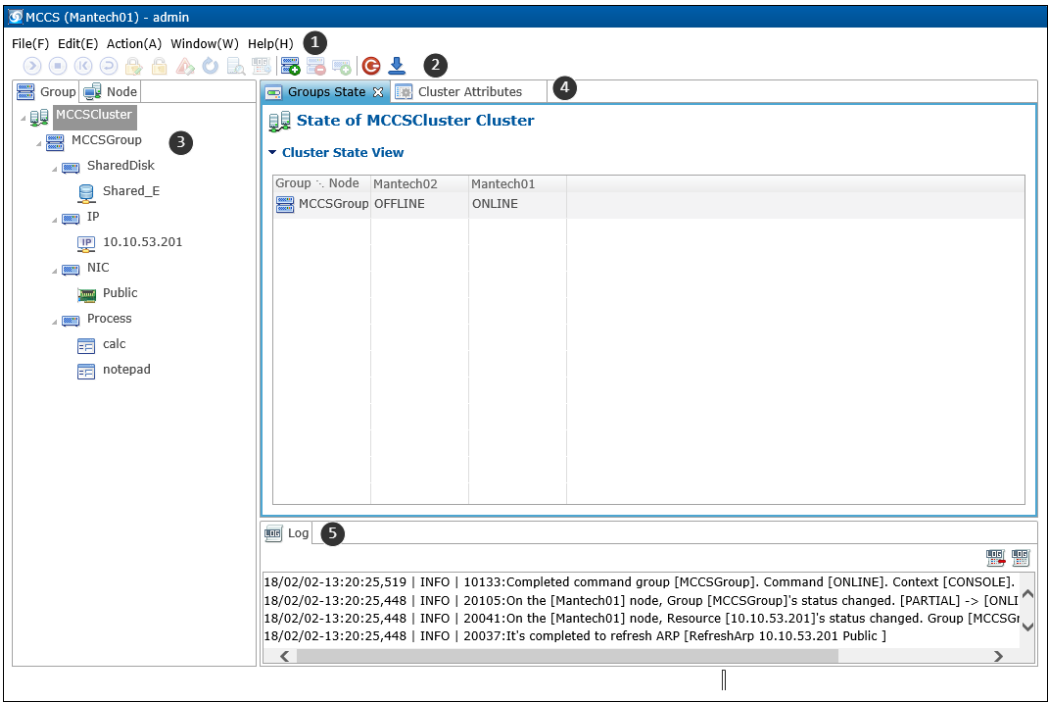
List	Explanation
Default User ID	mcuser
password	mccs

Change your password when logging in for the first time.
The password can be set to 12 or more digits or 14 or more digits according to the rules below.
Passwords must be changed periodically, every 90 days.
A password once used cannot be used again.
If you click "Change next time", the password change pop-up window will appear again after 90 days.

Number of digits in password	Password rules
more than 12 digits	Must contain lowercase letters, numbers, and special characters (~!@#$%^&*( )+\).

more than 14 digits	Lowercase letters and numbers are required.

5.3 Screen Composition



List	Explanation
1 Menu Bar	This is the menu bar that lists MCCS functions.
2 Tool Bar	Frequently used functions are provided in the toolbar. Depending on the resource group, resource type, and resource status, items that can be executed are enabled, and items that cannot be executed are disabled.
3 Management Tree	You can check resource groups and nodes.
4 Detail Screen	Provides status and property information for objects selected in the management tree.
5 Log Web Console	Logs for MCCS operation are output.

5.3.1 Menu Bar

This is a detailed description of the menu bar.

Main menu	Sub menu	Explanation
File(F)	Logout	Sign out of the web console.

	 Collecting support files	Collects system information, environment information, etc. where MCCS is installed.
Edit(E)	 Add group	Add new resource groups.
	 Delete group	Delete the resource group.
	 Add resource	Add new resources.
	 Delete resource	Delete the resource.
	Resource activation	Start monitoring the selected resources.
	Monitoring all resources	Start monitoring all resources.
	Group failover on failure	Set whether to fail over the resource group in case of resource failure.
	 Edit heartbeat configuration	Edit cluster name, heartbeat port, heartbeat configuration.
	Node name change	Rename the selected node.
Action(F)	 Online	Start the selected resource group, resource.
	 Offline	Shut down the selected resource group, resource.
	 Group Manual Failover	The resource group is failed over by the user.
	 Group Lock	Temporarily lock or lock the resource group.
	 Unlock	Unlock the resource group.
	 Remove fault indication	Removes the failed resource group and resource failure indication.
	 command initialization	Cancels all commands in progress on the resource group and resets the state of the resource.
	 manual detection	Manually detect if a resource is up or not.
	 View Manual Operation Logs	Manual operation logs are output for each node.
Window(W)	Environment settings	Edit the configuration of the MCCS management web console.
Help(H)	Help	This is the MCCS manual.
	About MCCS	MCCS version information.

5.3.2 Toolbar

Frequently used functions are provided in the toolbar. Depending on the resource group, resource type, and resource status, items that can be executed are enabled, and items that cannot be executed are disabled.

5.3.3 Management Tree

You can check resource groups and nodes.

Main menu	Sub menu	Explanation
Cluster	Resource group state	You can check the status of resource groups and nodes configured in the cluster.
	Cluster attribute	You can view or change the cluster attributes, log attributes, and quorum attributes.
	Quorum state	A tap is active only when a quorum is set. You can check the connection status of the quorum server and quorum clients.
Node	Node attribute	You can view or change node attributes, self-fencing attributes, and remote fencing attributes.
Resource group	Resource dependency	You can establish dependencies between resources or control resources.
	Resource state	You can check the status of resource groups and resources by node.
	Resource group property	Add new resources.
Resource type	Resource state	You can check the status of resources belonging to a resource type.
	Resource type attribute	You can check or change resource type attributes. Changes to resource type attributes apply to all resources belonging to the resource type.
Resource	Resource state	You can check the status of resources by node.
	Resource attribute	You can check or change the attributes of each resource.

5.3.4 Detailed Screen

State and property information of the object selected in the management tree.

5.3.5 Log Web Console

This is a description of the log web console icon.

Icon	Function	Explanation

	Clear the log	Delete log messages displayed on the web console screen. Log files stored in the MCCS folder are not deleted.
	View full log	Displays the entire log of the node in a new window.

5.4 License Management

5.4.1 License Type

License Type	Category	Explanation
Temporary license - There is a deadline for the license expiration date	Term license	This is the license when MCCS is installed alone. - HostID: ANY
	Floating license	This license is used when configuring MCCS and Enterprise products together. - Include hostname or IP address - Port settings - Including the number of installed MCCS (eg: 30) ※Caution※ If the node is restarted while unable to connect to the floating license server, failover does not work because it is recognized as an invalid license.
Full License - No license expiration date.	Node Lock License	This is the license when MCCS is installed alone. - HostID: one of the node's MAC addresses
	Floating license	This license is used when configuring MCCS and Enterprise products together. - Include hostname or IP address - Port settings - Including the number of installed MCCS (eg: 30) ※Caution※ If the node is restarted while unable to connect to the floating license server, failover does not work because it is recognized as an invalid license.
	Dongle license	The dongle license works in conjunction with the dongle USB and the existing text file license. It is authenticated through the physical serial (rlmid) of the hardware dongle (HASP). - HostID: rlmid (Example: rlmid1=32783e7d)

License

▸ If the license file does not exist or the temporary license expires, it changes to limited mode and does not fail over in case of failure.

▸ In the case of "node-locked license" that refers to the MAC address, if the network card is changed, the license must be reissued.

▸ In the case of a full license, if the license is verified within 7 days when the MCCS service is restarted, the license authentication is maintained. If it exceeds 7 days, it changes to restricted mode and does not failover in case of failure.

5.4.2 How to set up license

5.4.2.1 License settings when installing MCCS

You can set the license at the last stage of MCCS installation.

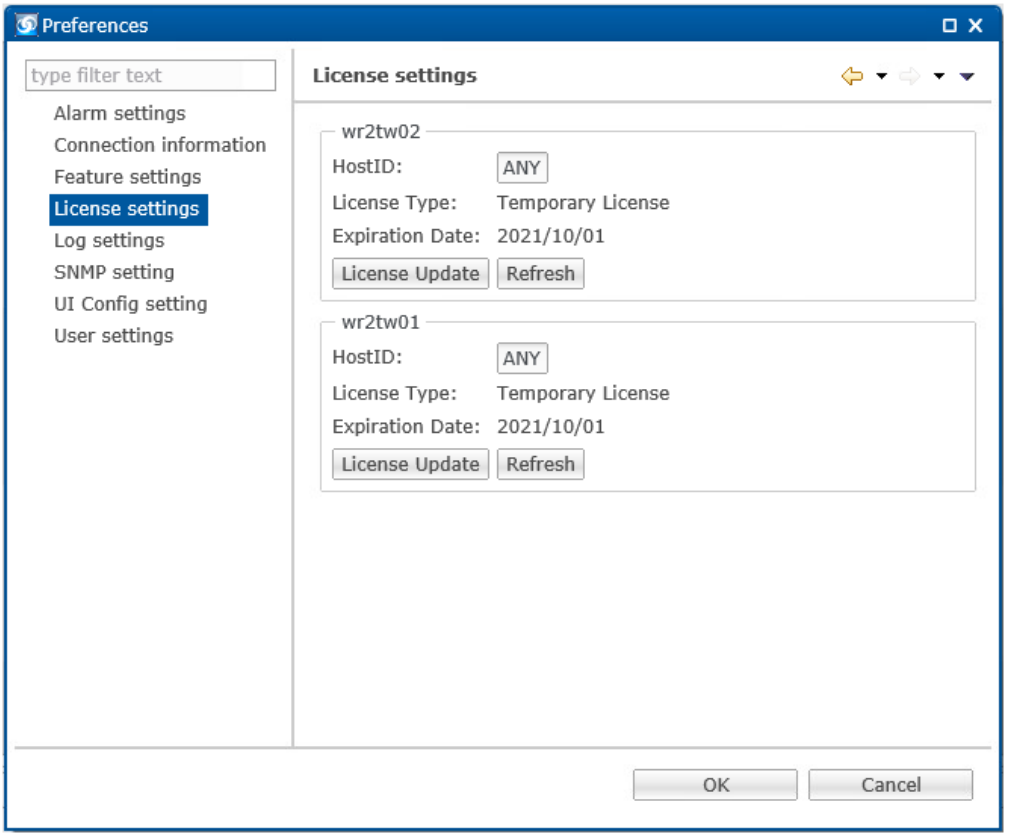
If you do not enter the license in the installation stage, you can set the license in environment settings.

5.4.2.2 License Registration in Environment Settings

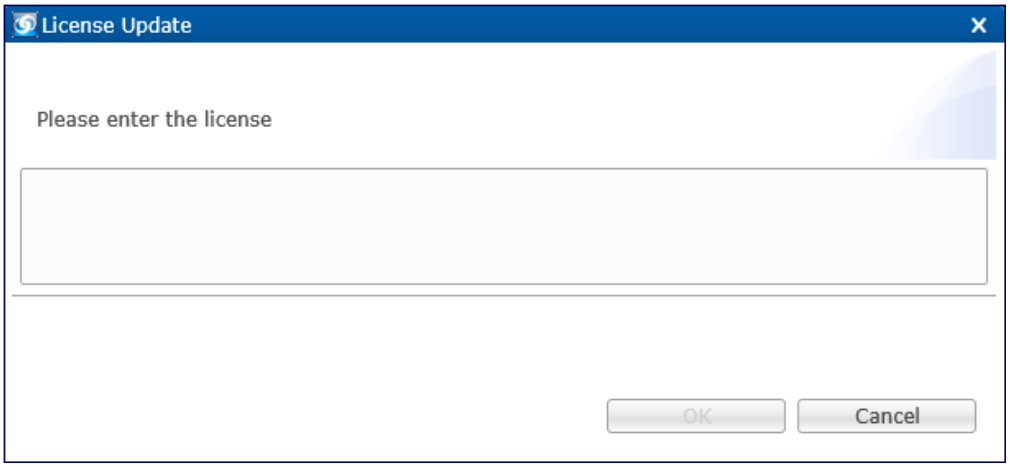
In Preferences, you can check licenses by node.

In the case of a “temporary license”, you can renew it in Preferences when the period expires.

1. Connect to the MCCS web console.
2. Select Window → "Preferences".
3. After selecting "License Settings" in the left area, click the [Renew License] button of the node to be updated in the right area.



4. Enter the MCCS license in the blank field.
   After entering the license, click the [OK] button to complete.



5.5 Patch and Update Management

Previous version	How to upgrade
MCCS 3.1 ~ MCCS 4.4.2	It is recommended to reinstall after deleting the MCCS program and MCCS folder. Proceed with the version upgrade in the order below. 1. Delete MCCS. For details, refer to "6. Delete Open Link in New

	Window" in MCCS Installation Manual. 2. Delete the MCCS folder in "C:\Program Files". 3. Install the newly issued MCCS. For details, refer to "3. InstallationOpen a link in a new window" in the installation manual. 4. After installation is complete, reconfigure MCCS.
MCCS 4.4.3 ~ MCCS 4.4.11	Deleting the MCCS program and MCCS folder, installing a new one, and upgrading MCCS are both possible. Upgrade is a method of installing after backing up "support files", deleting only the MCCS program and not deleting the MCCS folder. <Support File> ● MSCS configuration files (main.json, hbjson, etc.) ● Files that store other user-defined scripts, etc. ● MCCS license file (mccs.lic) Proceed with the version upgrade in the order below. 1. Download the support file. For details, refer to "9.4 How to collect support files". 2. Delete MCCS. For details, refer to "6. Delete Open Link in New Window" in MCCS Installation Manual. 3. Install the newly issued MCCS. For details, refer to "3. InstallationOpen a link in a new window" in the installation manual. 4. Reflect the necessary content among the contents in the support file.

6. Support

6.1 Technical Support

The scope of technical support is limited to the functions specified in documents such as manuals.

The scope of technical support is as follows:

24 X 7 Disability / Technical Support

Installation support (installation manual and user manual are also provided)

Technical support contacts are:

cs@mantech.co.kr / 1833-7790

6.2 Support Cost

Technical support is provided under the License Agreement.

6.3 SLA

SLAs are provided under the license agreement.