EXPRESSCLUSTER X 5.2
HA Cluster Configuration Guide for Amazon Web Services (Linux)

Release 2

NEC Corporation

Nov 29, 2024

TABLE OF CONTENTS:

CHAPTER

ONE

PREFACE

1.1 Who Should Use This Guide

This guide is intended for administrators who configure cluster systems, and system engineers and maintenance staff who support the users. They must also have knowledge of Amazon EC2, Amazon VPC, and IAM provided by Amazon Web Services.

1.2 Scope of Application

For information on the system requirements, see "Getting Started Guide" -> "Installation requirements for EXPRESSCLUSTER".

This guide contains product- and service-related information (e.g., screenshots) collected at the time of writing this guide. For the latest information, which may be different from the content in this guide, refer to corresponding websites and manuals.

1.3 How This Guide is Organized

- 2. *Overview*: Describes the functional overview.
- 3. *Operating Environment*: Describes the tested operating environment of this function.
- 4. *Notes*: Describes the notes on constructing a cluster.
- 5. *Constructing an HA cluster based on VIP control*: Describes how to create an HA cluster based on VIP control.
- 6. *Constructing an HA cluster based on EIP control*: Describes how to create an HA cluster based on EIP control.
- 7. *Constructing an HA cluster based on DNS name control*: Describes how to create an HA cluster based on DNS name control.
- 8. *Troubleshooting*: Describes the problems and their solutions.

1.4 EXPRESSCLUSTER X Documentation Set

The EXPRESSCLUSTER X manuals consist of the following five guides. The title and purpose of each guide is described below:

EXPRESSCLUSTER X Getting Started Guide

This guide is intended for all users. The guide covers topics such as product overview, system requirements, and known problems.

EXPRESSCLUSTER X Installation and Configuration Guide

This guide is intended for system engineers and administrators who want to build, operate, and maintain a cluster system. Instructions for designing, installing, and configuring a cluster system with EXPRESSCLUSTER are covered in this guide.

EXPRESSCLUSTER X Reference Guide

This guide is intended for system administrators. The guide covers topics such as how to operate EXPRESSCLUSTER, function of each module and troubleshooting. The guide is supplement to the Installation and Configuration Guide.

EXPRESSCLUSTER X Maintenance Guide

This guide is intended for administrators and for system administrators who want to build, operate, and maintain EXPRESSCLUSTER-based cluster systems. The guide describes maintenance-related topics for EXPRESSCLUSTER.

EXPRESSCLUSTER X Hardware Feature Guide

This guide is intended for administrators and for system engineers who want to build EXPRESSCLUSTER-based cluster systems. The guide describes features to work with specific hardware, serving as a supplement to the Installation and Configuration Guide.

1.5 Conventions

In this guide, Note, Important, See also are used as follows:

Note: Used when the information given is important, but not related to the data loss and damage to the system and machine.

Important: Used when the information given is necessary to avoid the data loss and damage to the system and machine.

See also:

Used to describe the location of the information given at the reference destination.

The following conventions are used in this guide.

Convention	Usage	Example
Bold	Indicates graphical objects, such as text boxes, list boxes, menu selections, buttons, labels, icons, etc.	Click Start. Properties dialog box
Angled bracket within the command line	Indicates that the value specified inside of the angled bracket can be omitted.	`clpstat -s[-h host_name]`
#	Prompt to indicate that a Linux user has logged on as root user.	`# clpstat`
Monospace	Indicates path names, commands, system output (message, prompt, etc.), directory, file names, functions and parameters.	`/Linux`
bold	Indicates the value that a user actually enters from a command line.	Enter the following: **# clpcl -s -a**
italic	Indicates that users should replace italicized part with values that they are actually working with.	`# ping <IP address>`

In the figures of this guide, this icon represents EXPRESSCLUSTER.

1.6 Contacting NEC

For the latest product information, visit our website below:

https://www.nec.com/en/global/prod/expresscluster/

CHAPTER

TWO

OVERVIEW

2.1 Functional overview

The settings described in this guide allow you to construct an HA cluster with EXPRESSCLUSTER in the Amazon Virtual Private Cloud (VPC) environment provided by Amazon Web Services (AWS).

Because more important applications can be performed by constructing an HA cluster, a wider range of system configuration options are available in the AWS environment. The AWS has a robust configuration made up of multiple availability zones (hereafter referred to as AZ) in each region. The user can select and use an AZ as needed. EXPRESSCLUSTER realizes highly available applications by allowing the HA cluster to operate between multiple AZs in a region (hereafter referred to as Multi-AZ).

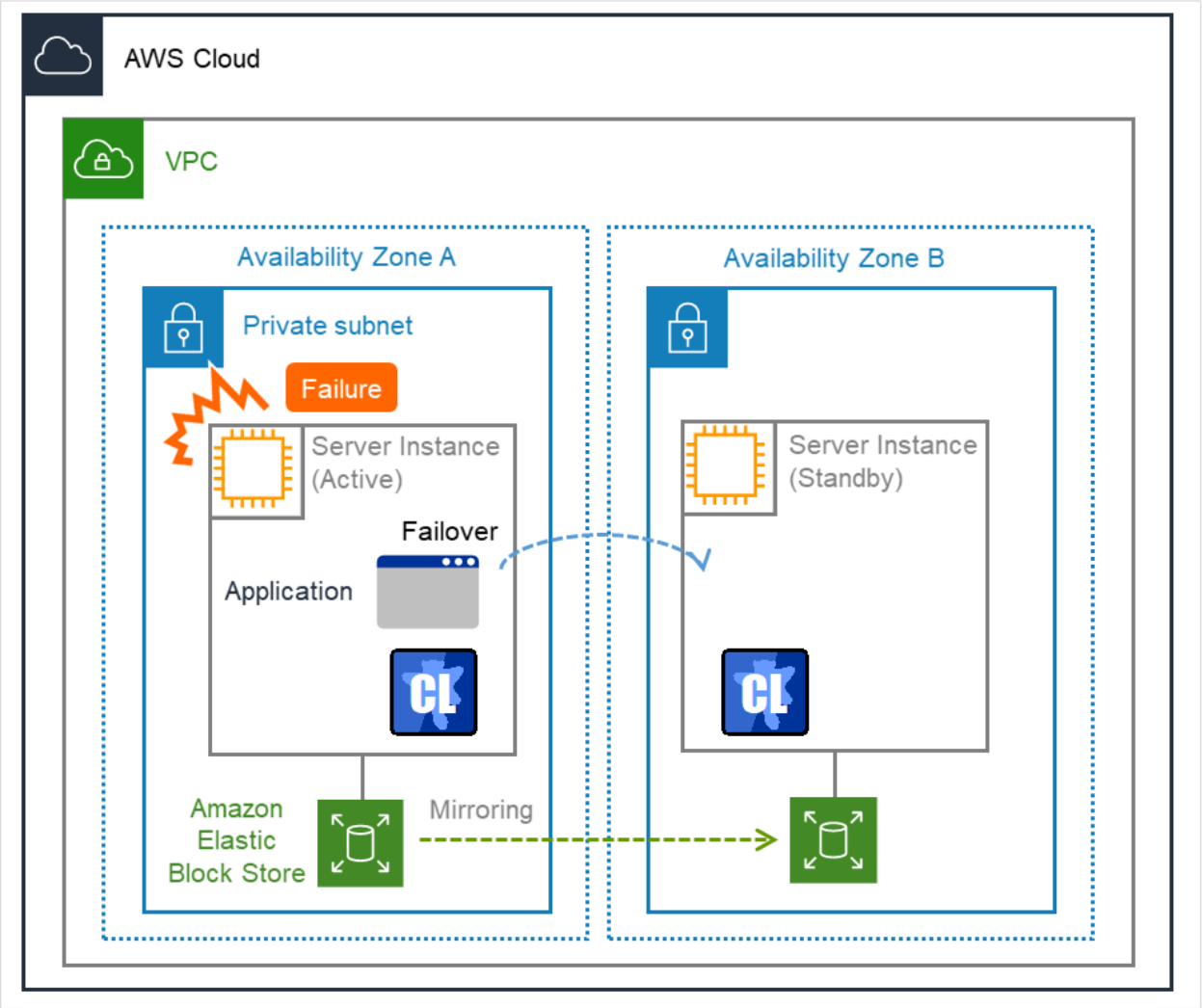


Fig. 2.1: Mirror Type HA Cluster in Multi-AZ Configuration

In the AWS environment, a virtual IP can be used to connect to the cluster server. The AWS Virtual IP resource and AWS Elastic IP resource and AWS DNS resource enable the client not to be aware of switching the destination server even if a "failover" or "group transition" occurred.

2.2 HA cluster configuration

This guide describes three types of HA cluster configurations: HA cluster based on virtual IP (VIP) control, HA cluster based on elastic IP (EIP) control and HA cluster based on DNS name control. This section describes a single AZ configuration. For a multi-AZ configuration, refer to "2.3. *Multi-AZ*"

Location of a client accessing an HA cluster	Resource to be selected	Reference in this chapter
In the same VPC	AWS Virtual IP resource	HA cluster based on VIP control
Internet	AWS Elastic IP resource	HA cluster based on EIP control
Voluntary location	AWS DNS resource	HA cluster based on DNS name control

2.2.1 HA cluster based on VIP control

This guide assumes the configuration in which a client in the same VPC accesses an HA cluster via a VIP address. For example, a DB server is clustered and accessed from a web server via a VIP address.

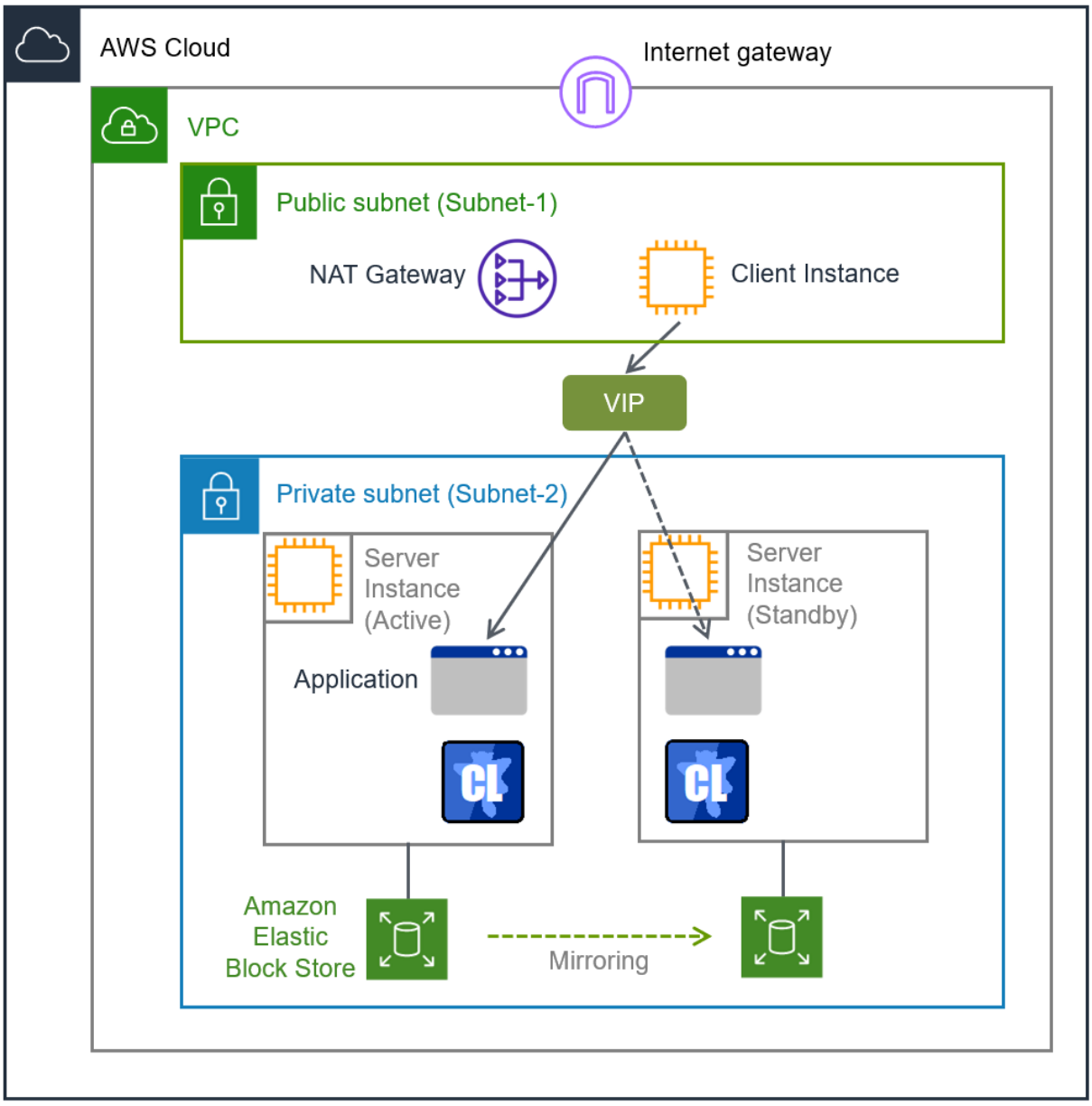


Fig. 2.2: HA Cluster Based on VIP Control

In the above figure, the server instances are clustered and placed on the private subnet. The AWS Virtual IP resource of EXPRESSCLUSTER sets a VIP address to the active server instance and rewrites the VPC route table. This enables the client instance placed on any subnet in the VPC to access the active server instance via the VIP address. The VIP address must be out of the VPC CIDR range.

To enable a client outside the VPC to access the server instance, establish the communication by using the route table in the VPC in some way. For example, using AWS Transit Gateway enables the communication from outside the VPC to be transferred to the VPC via the Transit Gateway route table and then to be established with the server instance via the route table in the VPC.

When executing the AWS CLI or referencing the DNS, each server instance accesses the regional endpoint or the Internet via a NAT gateway placed on the public subnet as needed.

* With the AWS CLI running, each instance must connect to the regional endpoint. For this connection, various ways are available such as a proxy server, NAT, a public IP, an EIP, and a VPC endpoint. This guide is based on using a NAT gateway for a VIP-controlled HA cluster configuration.

The following resources and monitor resources are required for an HA cluster based on VIP control configuration.

Resource type	Description	Setup
AWS Virtual IP resource	Assigns a VIP address to an active server instance, changes the route table of the assigned VIP address, and publishes operations within the VPC.	Required
AWS Virtual IP monitor resource	Periodically monitors whether the VIP address assigned by the AWS Virtual IP resource exists in the local server and whether the VPC route table is changed illegally. (This monitor resource is automatically added when the AWS Virtual IP resource is added.)	Required
AWS AZ monitor resource	Periodically monitors the health of the AZ in which the local server exists by using Multi-AZ.	Recommended
Other resources and monitor resources	Depends on the configuration of the application, such as a mirror disk, used in an HA cluster.	Optional

2.2.2 HA cluster based on EIP control

This guide assumes the configuration in which a client accesses an HA cluster via a global IP address assigned to the EIP through the Internet.

Clustered instances are placed on a public subnet. Each instance can access the Internet via the Internet gateway.

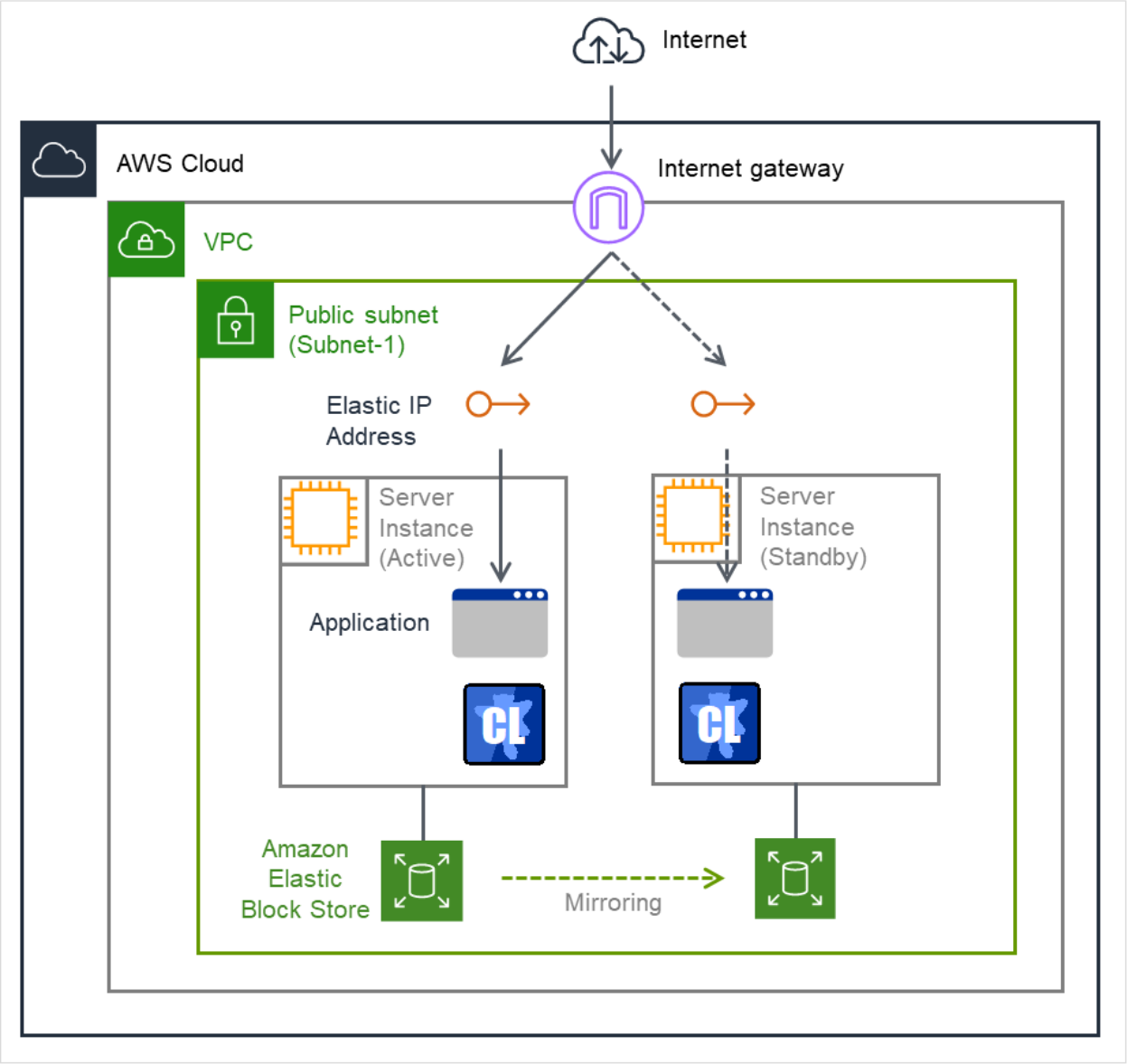


Fig. 2.3: HA Cluster Based on EIP Control

In the above figure, the server instances are clustered and placed on the public subnet. The AWS Elastic IP resource of EXPRESSCLUSTER attaches the EIP to the active server instance. This enables a client on the Internet to access the active server instance via the EIP address.

* With the AWS CLI running, each instance must connect to the regional endpoint. For this connection, various ways are available such as a proxy server, NAT, a public IP, an EIP, and a VPC endpoint. This guide is based on using a public IP address assigned to the instance for an EIP-controlled HA cluster configuration.

The following resources and monitor resources are required for an HA cluster based on EIP control configuration.

Resource type	Description	Setup
AWS Elastic IP resource	Assigns an EIP address to an active server instance and publishes operations to the Internet.	Required
AWS elastic IP monitor resource	Periodically monitors whether the EIP address assigned by the AWS Elastic IP resource exists in the local server. (This monitor resource is automatically added when the AWS Elastic IP resource is added.)	Required
AWS AZ monitor resource	Periodically monitors the health of the AZ in which the local server exists by using Multi-AZ.	Recommended
Other resources and monitor resources	Depends on the configuration of the application, such as a mirror disk, used in an HA cluster.	Optional

2.2.3 HA cluster based on DNS name control

This guide assumes the configuration in which a client accesses an HA cluster via the same DNS name. For example, a DB server is clustered and accessed from a web server via a DNS name.

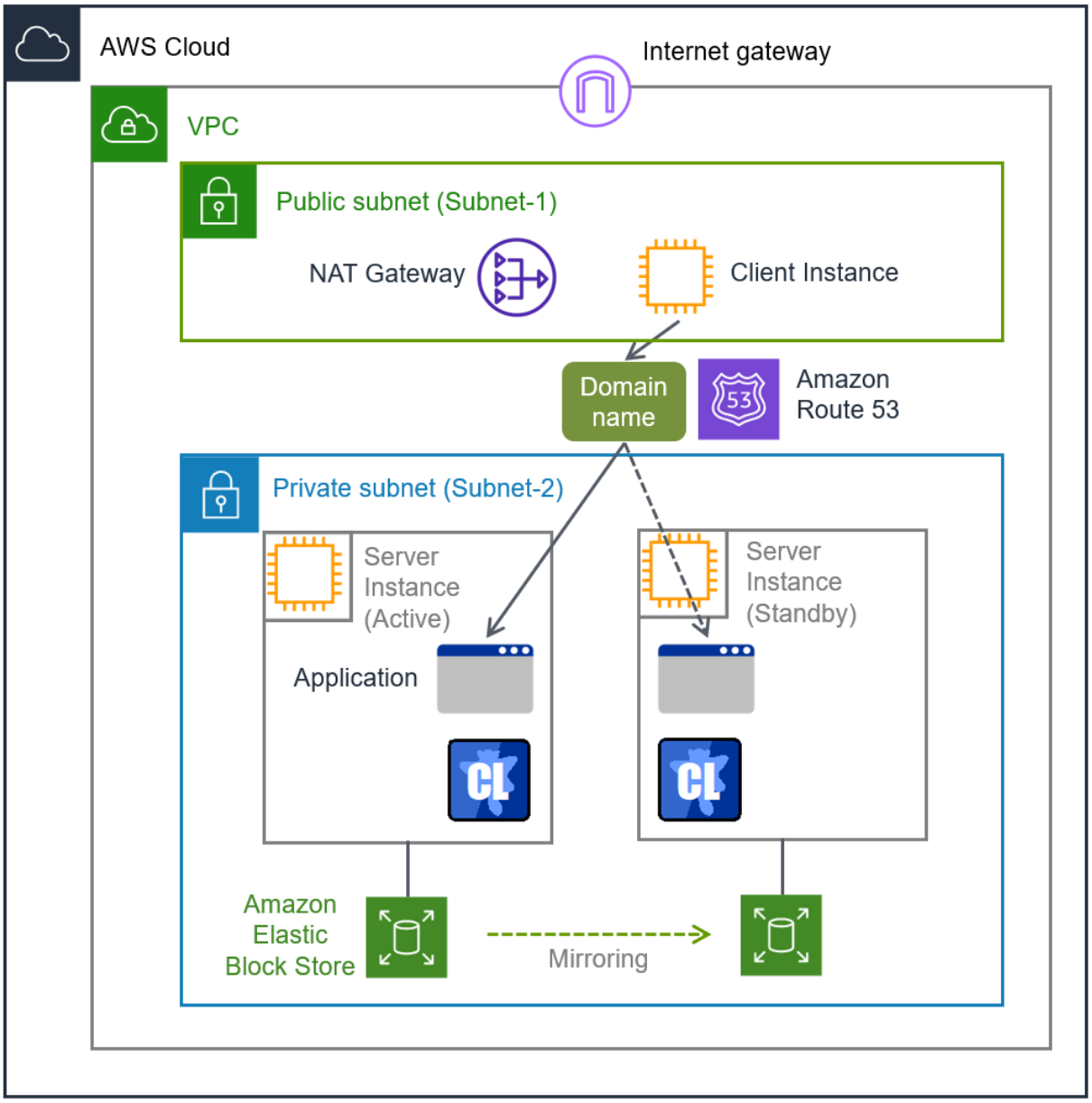


Fig. 2.4: HA cluster based on DNS name control

In the above figure, the server instances are clustered and placed on the private subnet. The AWS DNS resource of EXPRESSCLUSTER registers resource record set including the DNS name and the IP address of the active server into the Private Hosted Zone of Amazon Route 53. This enables the client instance placed on any subnet in the VPC to access the active server instance via the DNS name.

In this guide, clustered server instances are placed on the private subnet. However, the instances can be also placed on a public subnet. In this case, this enables a client on the Internet to access the active server instance via the DNS name by registering the resource record set including the DNS name and the public IP address of the active server into the Public Hosted Zone of Amazon Route 53. Furthermore, in order that the query to the domain of the Public Hosted Zone can refer to the Amazon Route 53 name server, it is required to set the name server (NS) record of the registrar in advance.

Moreover, for a configuration in which the cluster and client exist in different VPCs, use a VPC peering connection. Preliminary create a peering connection between the VPCs and associate the VPCs with the private hosted zone of Amazon Route 53. And then register the resource record set including the DNS name and the IP address of the active server into the private hosted zone. This enables the client in the different VPC to access the active server instance via DNS name.

* With the AWS CLI running, each instance must connect to the regional endpoint. For this connection, various ways are available such as a proxy server, NAT, a public IP, and an EIP. This guide is based on using a NAT gateway for a DNS-name-controlled HA cluster configuration.

The table below shows the necessary resources and monitor resources for constructing a HA cluster based on DNS name control.

Resource Type	Description	Configuration
AWS DNS resource	Registers the resource record sets including the DNS name and the IP address of the active server instance into the hosted zone of Amazon Route 53, and publishes operations within the VPC or to the Internet.	Required
AWS DNS monitor resource	AWS DNS resource periodically monitors whether the registered resource record set exists in the hosted zone of Amazon Route 53 and whether the resolution of the DNS name is available. (This monitor resource is automatically added when the AWS DNS resource is added.)	Required
AWS AZ monitor resource	Periodically monitors the health of the AZ in which the local server exists by using Multi-AZ.	Recommended
Other resources and monitor resources	Depends on the configuration of the application, such as a mirror disk, used in an HA cluster.	Optional

2.3 Multi-AZ

In the AWS environment, the instances configuring an HA cluster can be distributed to AZs. This provides the instance redundancy for a failure occurrence in an AZ, and increases the system availability.

The AWS AZ monitor resource monitors the health of each AZ. If the monitor resource detects a failure, it makes EXPRESSCLUSTER to issue a warning or perform a recovery operation.

For details, refer to the following:

Reference Guide

-> Understanding AWS AZ monitor resources

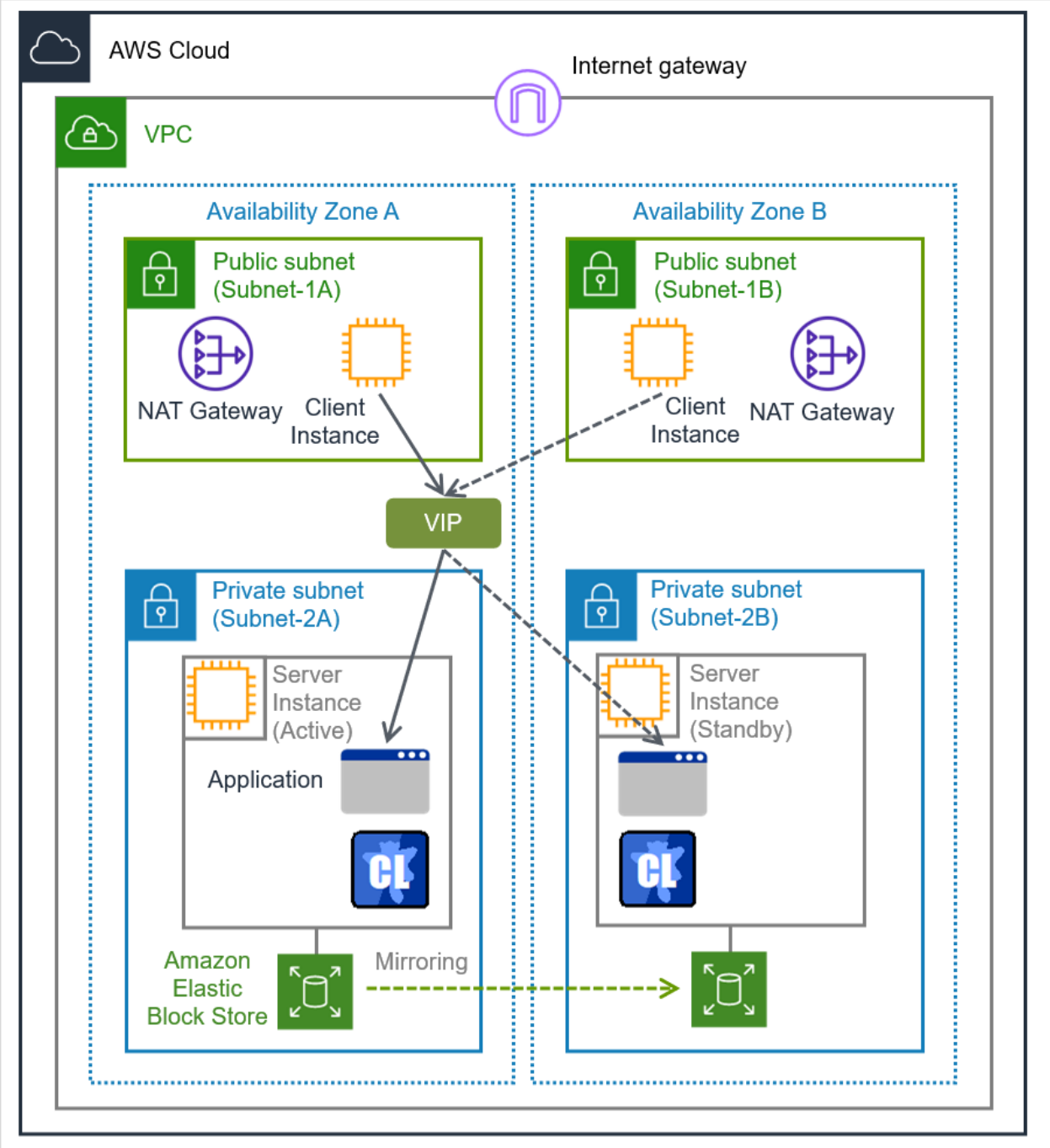


Fig. 2.5: HA Cluster Using Multi-AZ

2.4 Network partition resolution

In network partition resolution (NP resolution), each server checks whether it can access a shared device or not, and then determines whether the server has been isolated from the network or other servers have been down.

The following table shows NP resolution configured for examples in this guide (unspecified settings mean that their default values are used):

Item	Setting	Remark
Type	HTTP	
Target Host (Target)	aws.amazon.com	Specify a device which responds to an HTTP HEAD request with the status code 200.
Service Port	443	
Use SSL	On	To specify the 443 port of aws.amazon.com as the target, set this setting to **On**. Some environments may require setting **SSL Library** and **Crypto Library** (see **Cluster properties** -> the **Encryption** tab).

For more information on NP resolution, refer to the following documents:

- "Getting Started Guide"-"Network partition resolution"
- "Reference Guide"-"Network partition resolution resources details"

2.5 On-premises and AWS

The following table describes the EXPRESSCLUSTER functional differences between the on-premises and AWS environments.

- ✓: Available
- n/a: Not available

Function	On-premises	AWS
Creation of a shared disk type cluster	✓	✓
Creation of a mirror disk type cluster	✓	✓
Using the management group	✓	n/a
Floating IP resource	✓	n/a
Virtual IP resource	✓	n/a
AWS Elastic IP resource	n/a	✓
AWS Virtual IP resource	n/a	✓
AWS DNS resource	n/a	✓

The following table describes the creation flow of a 2-node cluster that uses a mirror disk and various resources in the on-premises and AWS environments.

- Before installing EXPRESSCLUSTER

	Step	On-premises	AWS
1	Configure the VPC environment.	Not required	- When using the AWS Virtual IP resource, refer to "5.1. *Configuring the VPC Environment*" in this guide. - When using the AWS Elastic IP resource, refer to "6.1. *Configuring the VPC Environment*" in this guide. - When AWS DNS resource is used, refer to "7.1. *Configuring the VPC Environment*" in this guide.

Continued on next page

Table 2.7 – continued from previous page

	Step	On-premises	AWS
2	Configure the instance.	Not required	- When using the AWS Virtual IP resource, refer to "5.2. *Configuring the instance*" in this guide. - When using the AWS Elastic IP resource, refer to "6.2. *Configuring the instance*" in this guide. - When AWS DNS resource is used, refer to "7.2. *Configuring the instance*" in this guide.
3	Configure a partition for a mirror disk resource.	Refer to the following: - Installation and Configuration Guide -> Determining a system configuration -> Settings after configuring hardware - Reference Guide -> Understanding Mirror disk resources	Same as the on-premises environment
4	Adjust the OS startup time.	Refer to the following: - Installation and Configuration Guide -> Determining a system configuration -> Settings after configuring hardware	Same as the on-premises environment
5	Check the network.	Refer to the following: - Installation and Configuration Guide -> Determining a system configuration -> Settings after configuring hardware	Same as the on-premises environment

Continued on next page

Table 2.7 – continued from previous page

	Step	On-premises	AWS
6	Check the root file system	Refer to the following: - Installation and Configuration Guide -> Determining a system configuration -> Settings after configuring hardware	Same as the on-premises environment
7	Check the firewall.	Refer to the following: - Installation and Configuration Guide -> Determining a system configuration -> Settings after configuring hardware	Same as the on-premises environment
8	Synchronize the server time.	Refer to the following: - Installation and Configuration Guide -> Determining a system configuration -> Settings after configuring hardware	Same as the on-premises environment
9	Install EXPRESSCLUSTER.	Refer to the following: - Installation and Configuration Guide -> Installing EXPRESSCLUSTER	Same as the on-premises environment

- After installing EXPRESSCLUSTER

	Step	On-premises	AWS
10	Register the EXPRESSCLUSTER license.	Refer to the following: - Installation and Configuration Guide -> Registering the license	Same as the on-premises environment

Continued on next page

Table 2.8 – continued from previous page

	Step	On-premises	AWS
11	Construct a cluster - Set up the heartbeat method.	Refer to the following: - Installation and Configuration Guide -> Creating the cluster configuration data -> Creating the configuration data of a 2-node cluster	COM heartbeat, BMC heartbeat and DISK heartbeat cannot be used.
12	Construct a cluster: Set up the NP resolution.	Use an NP resolution resource. Refer to the following: - Installation and Configuration Guide -> Creating the cluster configuration data -> Creating the cluster configuration data - Reference Guide -> Network partition resolution resources details	Use an NP resolution resource. Refer to the following section of this guide: - " 2.4. *Network partition resolution* "

Continued on next page

Table 2.8 – continued from previous page

	Step	On-premises	AWS
13	Construct a cluster: Create a failover group Create a monitor resource.	Refer to the following: - Installation and Configuration Guide -> Creating the cluster configuration data -> Creating the cluster configuration data	In addition to the reference for the on-premises environment, refer to the following: - When using the AWS Virtual IP resource - "5.3. *Setting up EXPRESSCLUSTER*" in this guide - Reference Guide -> Understanding AWS Virtual IP resources - When using the AWS Elastic IP resource, refer to the following: - "6.3. *Setting up EXPRESSCLUSTER*" in this guide - Reference Guide -> Understanding AWS Elastic IP resources - When AWS DNS resource is used, refer to below documents: - "7.3. *Setting up EXPRESSCLUSTER*" in this guide. - Reference Guide -> Understanding AWS DNS resources

CHAPTER

THREE

OPERATING ENVIRONMENT

For details, refer to the following:

- Getting Started Guide
  -> Installation requirements for EXPRESSCLUSTER
  -> Operation environment for AWS Elastic IP resource, AWS Elastic IP monitor resource, AWS AZ monitor resource
- Getting Started Guide
  -> Installation requirements for EXPRESSCLUSTER
  -> Operation environment for AWS Virtual IP resource, AWS Virtual IP monitor resource
- Getting Started Guide
  -> Installation requirements for EXPRESSCLUSTER
  -> Operation environment for AWS DNS resource, AWS DNS monitor resource

CHAPTER

FOUR

NOTES

4.1 Notes on Using EXPRESSCLUSTER in the VPC

Note the following points when using EXPRESSCLUSTER in the VPC environment.

Access from the Internet or different VPC

NEC has verified that the AWS specifications do not allow clients on the internet or different VPC to access the server instance via the VIP address assigned by the AWS Virtual IP resource. In case of accessing from the client on Internet, specify the EIP address assigned by the AWS Elastic IP resource. In case of accessing from the client on different VPC, specify the DNS name registered to Amazon Route 53 with AWS DNS resource and then make an access via VPC Peering Connection.

Access from different VPC via VPC peering connection

AWS virtual IP resources cannot be used if access via a VPC peering connection is necessary. This is because it is assumed that an IP address to be used as a VIP is out of the VPC range and such an IP address is considered invalid in a VPC peering connection. If access via a VPC peering connection is necessary, use the AWS DNS resource that use Amazon Route 53.

Using VPC endpoint

By using VPC endpoint, it is able to control Amazon EC2 services of AWS CLI without preparing proxy server or NAT, even on the private network. Therefore, in the case of "5. *Constructing an HA cluster based on VIP control*", it is able to use VPC endpoint instead of NAT. When the VPC endpoint is created, the name which ends in ".ec2" must be selected.

Moreover, even when VPC endpoint is used, NAT gateway etc. will be required if internet access (for online update of instance, module download etc.) or access to AWS cloud service which is not supported by VPC endpoint are needed.

For EXPRESSCLUSTER, the VPC endpoint cannot be explicitly specified.
Use the VPC endpoint automatically selected by the AWS CLI.

Restrictions on the group resource and monitor resource functions

Refer to the following:

- Getting Started Guide

  -> Notes and Restrictions
  -> Setting up AWS elastic ip resources

-> Setting up AWS virtual ip resources
-> Setting up AWS DNS resources
-> Setting up AWS DNS monitor resources

Mirror disk performance

If an HA cluster is constructed in a Multi-AZ configuration, the instances are located at long distances from each other, causing a TCP/IP response delay. This might affect a mirroring operation.

Also, the usage of other systems affects the mirroring performance due to multi-tenancy. Therefore, the difference in the mirror disk performance in a cloud environment tends to be larger than that in a physical or general virtualized environment (non-cloud environment) (that is, the degradation rate of the mirror disk performance tends to be larger).

Take this point into consideration at the design phase if priority is put on writing performance in your system.

Disk device name to be specified for EXPRESSCLUSTER

In the AWS environment, the device file name of an NVMe EBS volume (e.g. /dev/nvme0n1) may be changed by rebooting, stopping/starting an instance or detaching/attaching an EBS volume, etc.

Therefore, if you set the device file name of an NVMe EBS volume to the device name controlled by Disk Resource (disk resource, mirrored disk resource, etc.), the startup of the Disk Resource may fail because the device file name may be changed when the instance reboots.

One of the following methods is recommended to address this issue.

- Set the LVM logical volume name to the device name of a Disk Resource.
- Set the by-id name (e.g. /dev/disk/by-id/nvme-Amazon_Elastic_Block_Store_vol***) to the device name of a Disk Resource.

If the data partition of a mirror disk is configured with LVM, the data partition can be extended without business suspension.

CHAPTER

FIVE

CONSTRUCTING AN HA CLUSTER BASED ON VIP CONTROL

This chapter describes how to construct an HA cluster based on VIP control.

In the figure below, "Server Instance (Active)" and "Server Instance (Standby)" respectively represent the instance of the active server and that of the standby server.

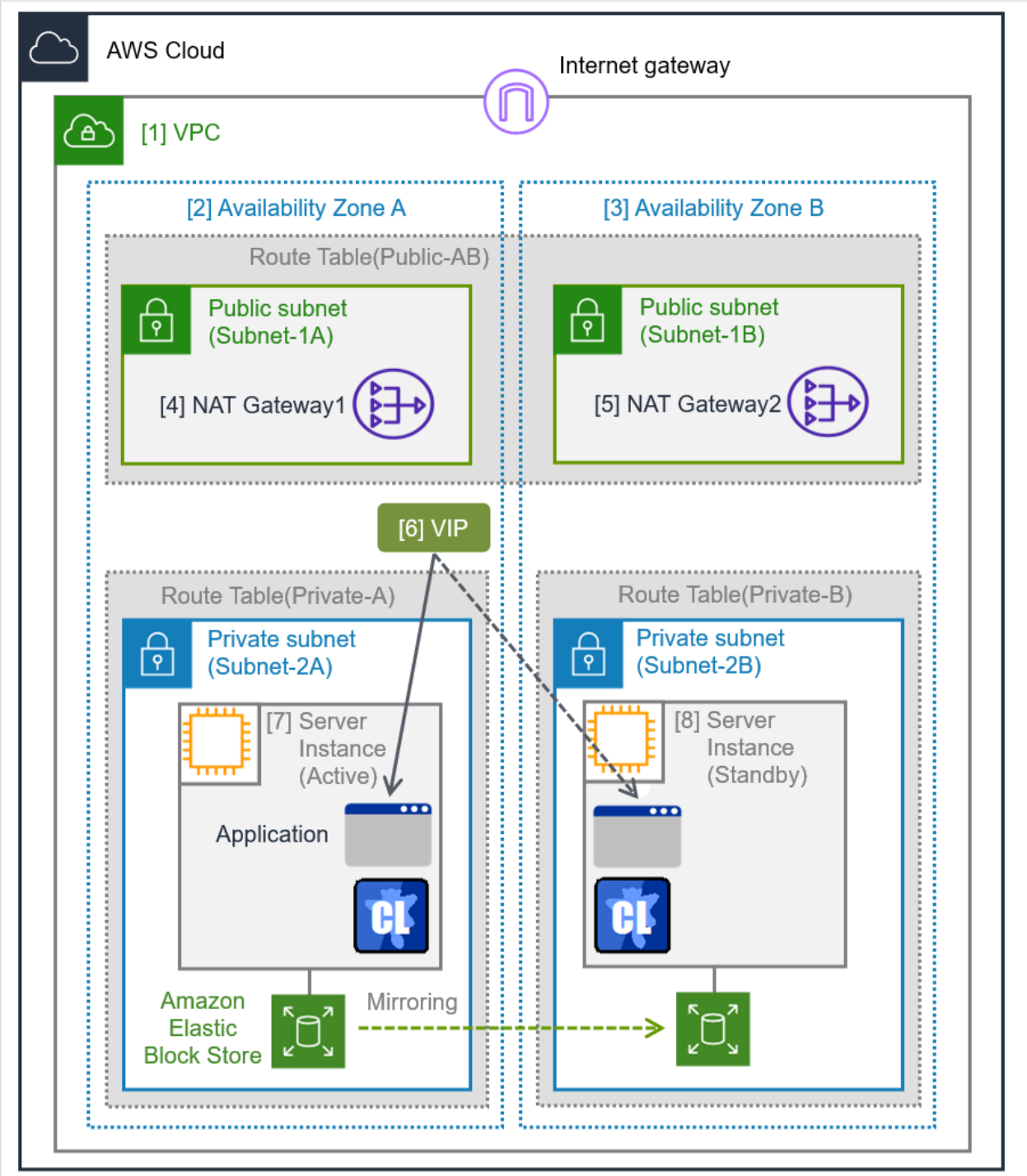


Fig. 5.1: System Configuration of the HA Cluster Based on VIP Control

CIDR (VPC)	10.0.0.0/16
VIP	10.1.0.20
Public subnet (Subnet-1A)	10.0.10.0/24

Continued on next page

Table 5.1 – continued from previous page

Public subnet (Subnet-1B)	10.0.20.0/24
Private subnet (Subnet-2A)	10.0.110.0/24
Private subnet (Subnet-2B)	10.0.120.0/24

5.1 Configuring the VPC Environment

Configure the VPC on the VPC Management console and EC2 Management console.
The IP addresses used in the figures and description are an example. In the actual configuration, use the actual IP addresses assigned to the VPC. When installing EXPRESSCLUSTER in the existing VPC, specify the appropriate settings such as adding a subnet if the number of subnets is insufficient.

1. **Configure the VPC and subnet.**

   Create a VPC and subnet first.

   -> Add a VPC and subnet in **VPC** and **Subnets** on the VPC Management console.

   [1] VPC Write down the VPC ID (vpc-xxxxxxxx), which is needed later for setting up the AWS virtual IP resource.

2. **Configure the Internet gateway.**

   Add an Internet gateway to access the Internet from the VPC.

   -> To create an Internet gateway, select **Internet Gateways > Create internet gateway** on the VPC Management console. Attach the created Internet gateway to the VPC.

3. **Configure the network ACL and security group.**

   Specify the appropriate network ACL and security group settings to prevent unauthorized network access from in and out of the VPC.
   Change the network ACL and security group path settings so that the instances of the HA cluster node can communicate with the Internet gateway via HTTPS, communicate with Cluster WebUI, and communicate with each other. The instances are to be placed on the private networks (Subnet-2A and Subnet-2B).

   -> Change the settings in **Network ACLs** and **Security Groups** on the VPC Management console.

   For the port numbers that are used by the EXPRESSCLUSTER components, refer to the following:

   Getting Started Guide
   -> Notes and Restrictions
   -> Before installing EXPRESSCLUSTER

4. **Add an HA cluster instance.**

   Create an HA cluster node instance on the private networks (Subnet-2A and Subnet-2B).
   To use an IAM role by assigning it to an instance, specify the IAM role.

   -> To create an instance, select **Instances > Launch Instance** on the EC2 Management console.

   -> For details about the IAM settings, refer to the following:

   Getting Started Guide
   -> Notes and Restrictions
   -> Before installing EXPRESSCLUSTER
   -> IAM settings in the AWS environment

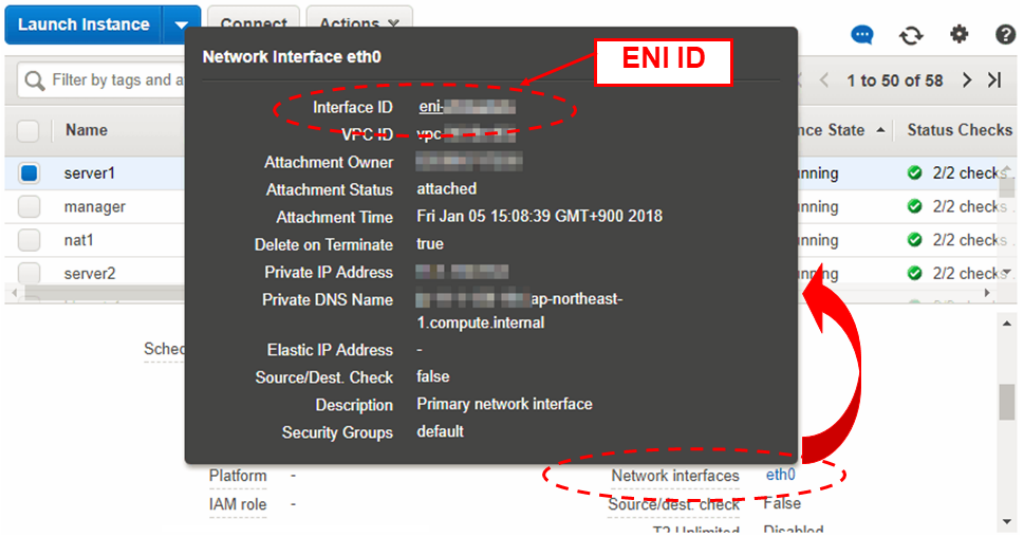
Disable Source/Dest. Check of the elastic network interface (ENI) assigned to each created instance.
To perform the VIP control by using the AWS Virtual IP resource, communication with the VIP address (10.1.0.20 in the above figure) must be routed to the ENI of the instance. It is necessary to disable **Source/Dest. Check** of the ENI of each instance to communicate with the private IP address and VIP address.

-> To change the settings, right-click the added instance in **Instances** on the EC2 Management console, and select Networking > Change Source/Dest. Check.

[7] Server Instance (Active), [8] Server Instance (Standby) The ENIs assigned respectively to the instance of the active server and the instance of the standby server can be identified according to the ENI IDs. **Write down the ENI ID (eni-xxxxxxxx) of each instance, because the ID is needed later for setting up the AWS virtual IP resource.**

Use the following procedure to check the ENI ID assigned to the instance.

1. Select the instance to display its detailed information.
2. Click the target device in **Network Interfaces**.
3. Check **Interface ID** displayed in the pop-up window.



5. **Add a NAT.**

To perform the VIP control by using the AWS CLI, communication from the instance of the HA cluster node to the regional endpoint via HTTPS must be enabled.
To do so, create a NAT gateway on the public networks (Subnet-1A and Subnet-1B).
For more information on the NAT gateway, see the corresponding AWS document.

6. **Configure the route table.**

Add the routing to the Internet gateway so that the AWS CLI can communicate with the regional endpoint via NAT and the routing so that a client in the VPC can access the VIP address. The number of CIDR blocks of the VIP address must always be 32.
The following routings must be set in the route table (Public-AB) of the public networks (Subnet-1A and Subnet-1B in the above figure).

- Route table (Public-AB)

Destination	Target	Remarks
VPC network (Example: 10.0.0.0/16)	local	Existing by default
0.0.0.0/0	Internet gateway	Add (required)
VIP address (Example: 10.1.0.20/32)	eni-xxxxxxxx (ENI ID of the active server instance) (ENI ID of the active server instance represented as "[7] Server Instance (Active)")	Add (required)

The following routings must be set in the route tables (Private-A and Private-B) of the private networks (Subnet-2A and Subnet-2B in the above figure).

- Route table (Private-A)

Destination	Target	Remarks
VPC network (Example: 10.0.0.0/16)	local	Existing by default
0.0.0.0/0	NAT Gateway1	Add (required)
VIP address (Example: 10.1.0.20/32)	eni-xxxxxxxx (ENI ID of the active server instance) (ENI ID of the active server instance represented as "[7] Server Instance (Active)")	Add (required)

- Route table (Private-B)

Destination	Target	Remarks
VPC network (Example: 10.0.0.0/16)	local	Existing by default
0.0.0.0/0	NAT Gateway2	Add (required)

Continued on next page

Table 5.4 – continued from previous page

Destination	Target	Remarks
VIP address (Example: 10.1.0.20/32)	eni-xxxxxxxx (ENI ID of the active server instance) (ENI ID of the active server instance represented as "[7] Server Instance (Active)")	Add (required)

When a failover occurred, the AWS Virtual IP resource switches all routings to the VIP address set in these route tables to the ENI of the standby server instance by using the AWS CLI.

[6] VIP

The VIP address must be out of the VPC CIDR range of the VPC.

Write down the VIP address set to the route table, because the address is needed later for setting up the AWS virtual IP resource.

Configure other routings according to the environment.

7. **Add a mirror disk (EBS).**

   Add an EBS to be used as the mirror disk (cluster partition or data partition) as needed.

   -> To add an EBS, select **Volumes > Create Volume** on the EC2 Management console, and then attach the created volume to an instance.

5.2 Configuring the instance

Log in to each instance of the HA cluster and specify the following settings.
For the AWS CLI versions supported by EXPRESSCLUSTER, refer to the following:

Getting Started Guide
-> Installation requirements for EXPRESSCLUSTER
-> Operation environment for AWS Virtual IP resource, AWS Virtual IP monitor resource

1) **Adjusting the OS startup time, verifying the network settings, verifying the root file system, verifying the firewall settings, synchronizing the server clock, and verifying the SELinux settings**

For information on each of the procedures, refer to the following:
- "Installation and Configuration Guide" -> "Determining a system configuration" -> "Settings after configuring hardware"

2) **Install the AWS CLI.**

Install the AWS CLI.

The installation path of the AWS CLI must be any of the following:

```
/sbin, /bin, /usr/sbin, /usr/bin, /usr/local/bin
```

For details about how to set up the AWS CLI, refer to the following:
https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html

(If EXPRESSCLUSTER has been installed before installing the AWS CLI, be sure to restart the OS before using EXPRESSCLUSTER.)

3) **Register the AWS access key ID.**

Run the following command from the shell.

```
$ sudo aws configure
```

Enter information such as the AWS access key ID to the inquiries.
The settings to be specified vary depending on whether an IAM role is assigned to the instance or not.

- Instance to which an IAM role is assigned.

```
AWS Access Key ID [None]: (Press Enter without entering anything.)
AWS Secret Access Key [None]: (Press Enter without entering anything.)
Default region name [None]: <default region name>
Default output format [None]: text
```

- Instance to which an IAM role is not assigned.

```
AWS Access Key ID [None]: <AWS access key ID>
AWS Secret Access Key [None]: <AWS secret access key>
Default region name [None]: <default region name>
Default output format [None]: text
```

For "Default output format", other format than "text" may be specified.
If you specified incorrect settings, delete the directory `/root/.aws` entirely, and specify the above settings again.

4) **Prepare the mirror disk.**

If an EBS has been added to be used as the mirror disk, divide the EBS into partitions and use each partition as the cluster partition and data partition.

For details about the mirror disk partition, refer to the following:

- Installation and Configuration Guide
  -> Determining a system configuration
  -> Partition settings for Mirror disk resource (when using Replicator)

5) **Install EXPRESSCLUSTER.**

For the installation procedure, refer to "Installation and Configuration Guide".
Store the EXPRESSCLUSTER installation media in the environment to which to install EXPRESSCLUSTER. (To transfer data, use any method such as Remote Desktop and Amazon S3.)

After the installation, restart the OS.

5.3 Setting up EXPRESSCLUSTER

For details about how to set up and connect to Cluster WebUI, refer to the following:

Installation and Configuration Guide
-> Creating the cluster configuration data

This section describes how to add the following resources:

- Mirror disk resource
- AWS Virtual IP resource
- AWS AZ monitor resource
- AWS Virtual IP monitor resource
- NP resolution (HTTP method)

For the settings other than the above, refer to "Installation and Configuration Guide".

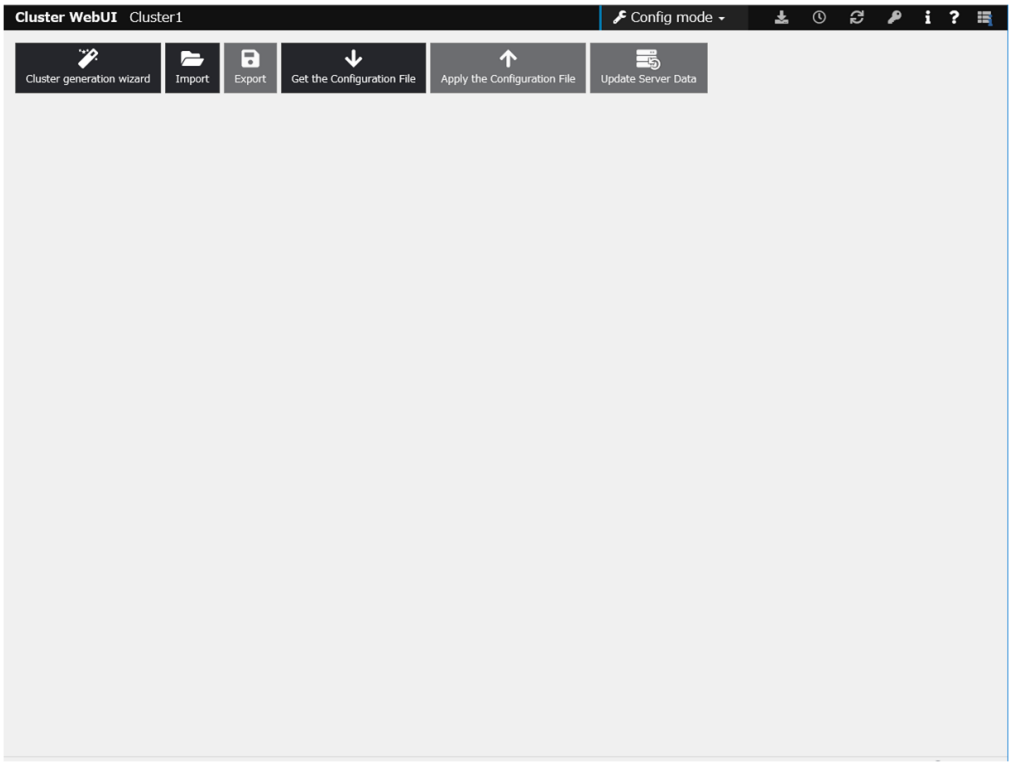
1. **Construct a cluster.**

   Start the Cluster generation wizard to construct a cluster.

   - Construct a cluster.

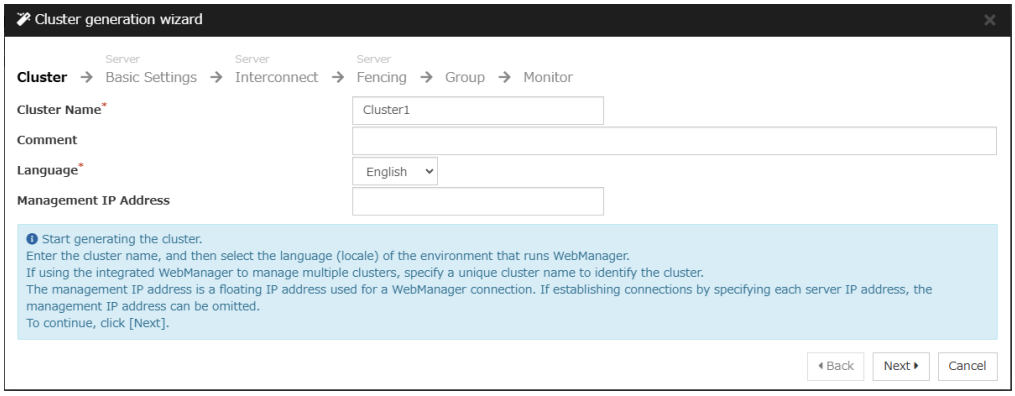
     Steps

     1. Access Cluster WebUI, and click **Cluster generation wizard**.

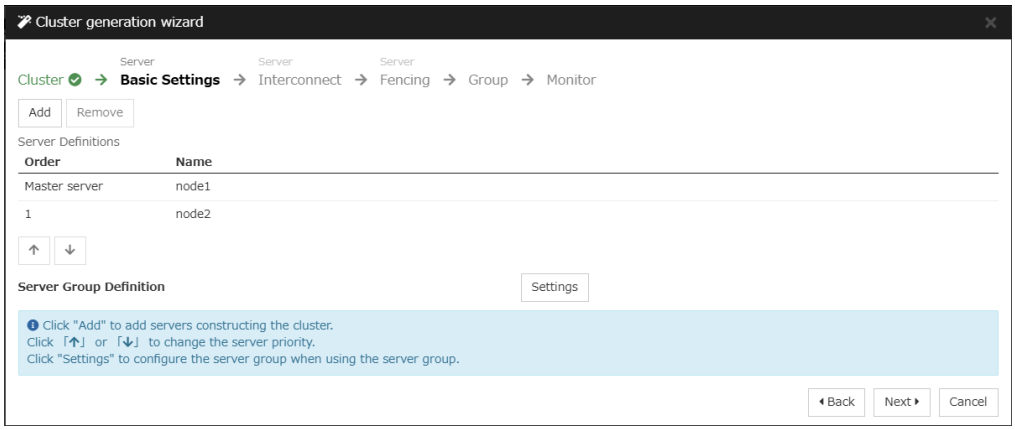


     2. The **Cluster** window on the **Cluster Generation Wizard** is displayed.

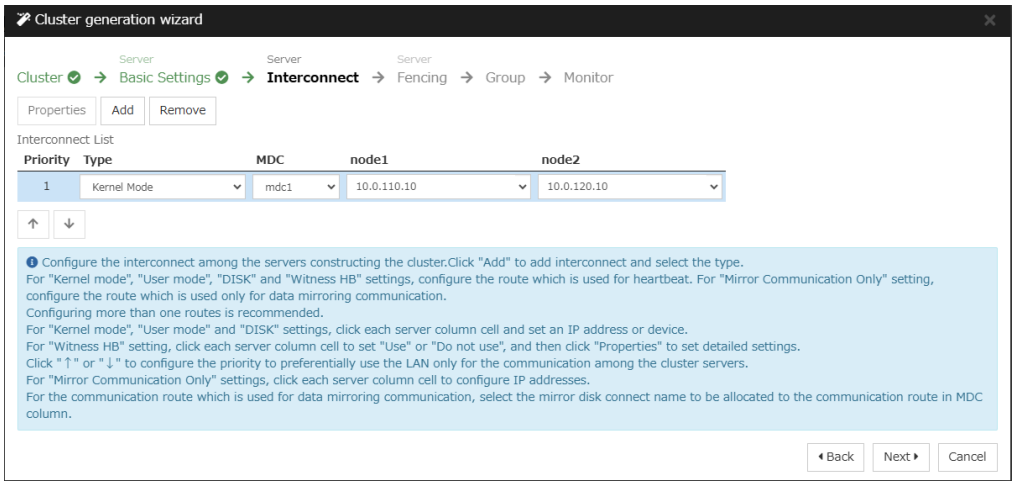
Enter a cluster name in **Cluster Name**.
Select an appropriate language from **Language**. Click **Next**.



3. The **Basic Settings** window is displayed.
   The instance connecting to Cluster WebUI is displayed as the registered master server.
   Click **Add** to add other instances (by specifying their private IP addresses). Click **Next**.



4. The **Interconnect** window is displayed.
   Specify the IP address (private IP address of each instance) to be used for interconnect. Select mdc1 from **MDC** for the communication path of the mirror disk resource to be created later.
   Click **Next**.



5. The **Fencing** window is displayed.
   Set the HTTP NP resolution.
   Click **Next**.

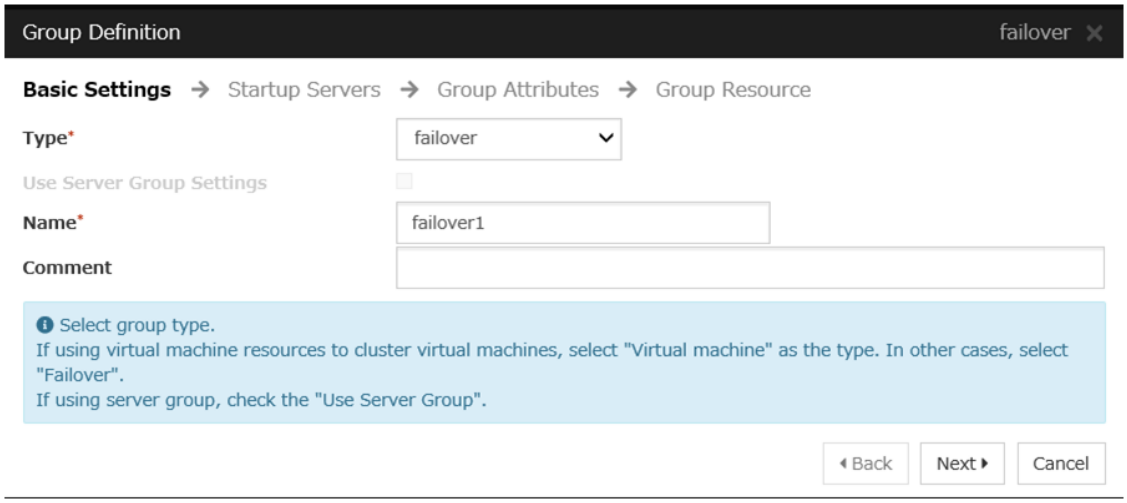
2. **Add a group resource.**

- Group definition

  Create a failover group.

  Steps

  1. The **Group List** window is displayed.
     Click **Add**.
  2. The **Group Definition** dialog box is displayed.
     Enter the failover group name (failover1) in the **Name** box. Click **Next**.



  3. The **Startup Servers** window is displayed.
     Click **Next** without specifying anything.

4. The **Group Attributes** window is displayed.
   Click **Next** without specifying anything.
5. The **Group Resource** window is displayed.
   Add a group resource on this page following the procedure below.

- Mirror disk resource

  Create a mirror disk resource according the mirror disk (EBS) as needed.

  For details, refer to the following:

  Reference Guide
  -> Understanding Mirror disk resources

  Steps

  1. Click **Add** in **Group Resource List**.
  2. The **Resource Definition of Group | failover1 window** is displayed.
     Select the group resource type (Mirror disk resource) from the **Type** box and enter the group resource name (md) in the **Name** box. Click **Next**.
  3. The **Dependency** window is displayed.
     Click **Next** without specifying anything.
  4. The **Recovery Operation** windows is displayed.
     Click **Next**.
  5. The **Advanced Settings** window is displayed.
     Enter the device name for the partition set up in "5.2. *Configuring the instance*" -> "6. **Prepare the mirror disk.**" in **Data Partition Device Name** and **Cluster Partition Device Name**. Specify Mount Point and File System. Click **Finish** to finish setting.

- AWS Virtual IP resource

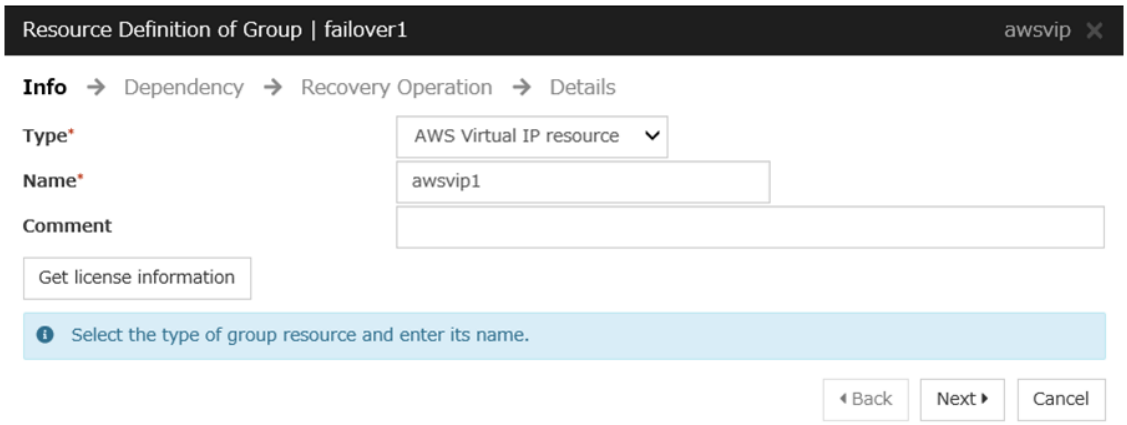
  Add the AWS Virtual IP resource that controls the VIP by using the AWS CLI.

  For details, refer to the following:

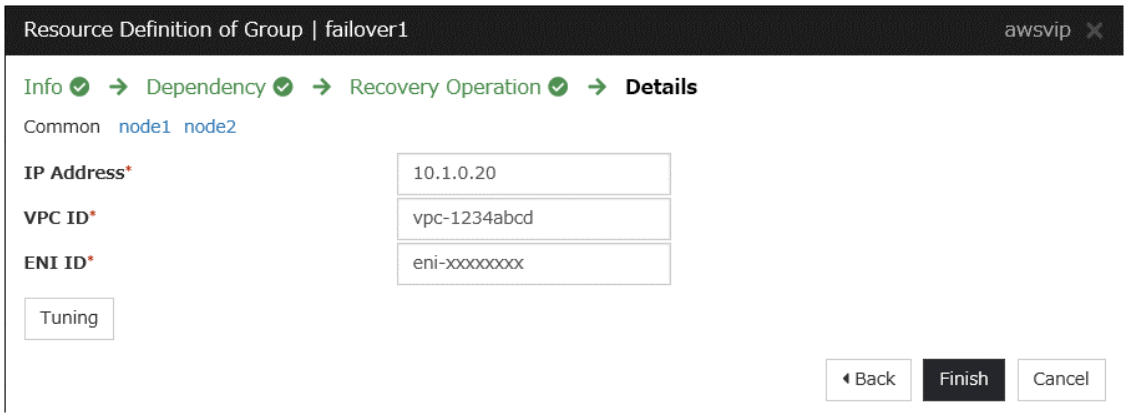
  Reference Guide
  -> Understanding AWS Virtual IP resources

  Steps

  1. Click **Add** in **Group Resource List**.
  2. The **Resource Definition of Group | failover1** window is displayed.
     Select the group resource type (AWS Virtual IP resource) from the **Type** box and enter the group resource name (awsvip1) in the **Name** box. Click **Next**.

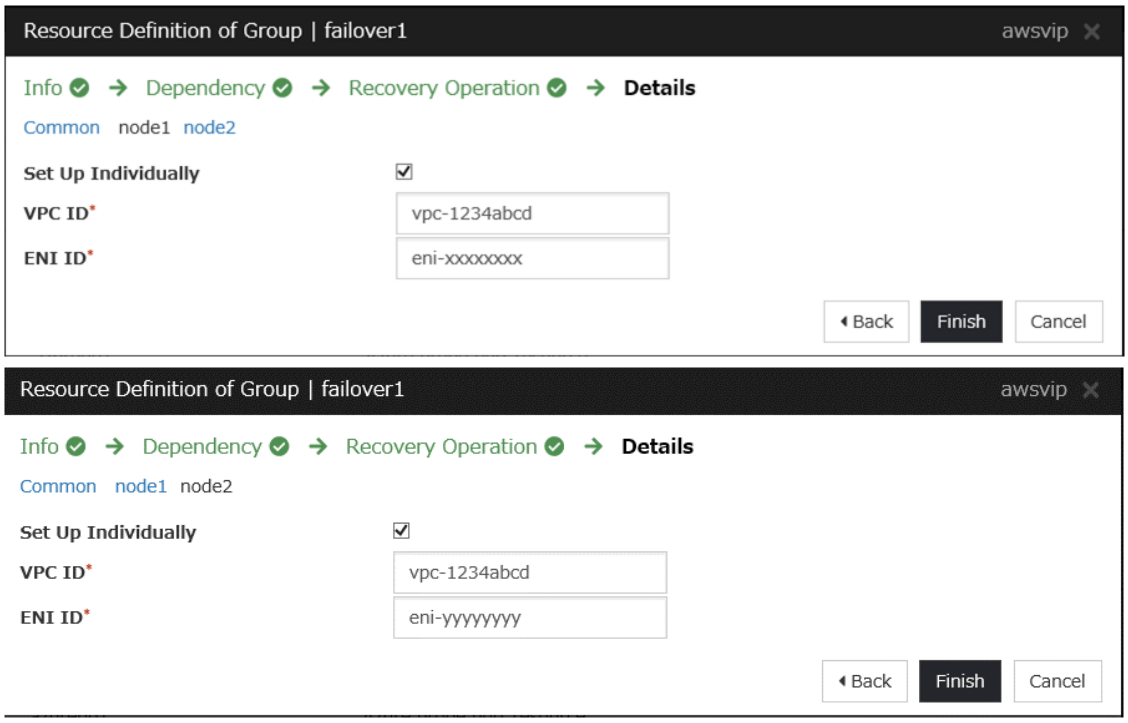


3. The **Dependency** window is displayed. Click **Next** without specifying anything.
4. The **Recovery Operation** window is displayed.
   Click **Next**.
5. The **Details** window is displayed.
   Set a VIP address to be assigned in the **IP Address** box on the **Common** tab (corresponds to [6] in Figure 5.1 System Configuration of the HA Cluster Based on VIP Control).
   Set the ID of the VPC including instances in the **VPC ID** box (corresponds to [1] in Figure 5.1 System Configuration of the HA Cluster Based on VIP Control).
   To set up the servers individually, enter the VPC ID of one server on the **Common** tab and specify the VPC ID of the other server separately.
   Enter the ENI ID of the active server instance to which the VIP address is to be routed in the **ENI ID** box (corresponds to [7] in Figure 5.1 System Configuration of the HA Cluster Based on VIP Control).
   The ENI IDs of the servers must be set up individually. Enter the ENI ID of one server on the **Common** tab and specify the ENI ID of the other server separately.



6. Specify the node settings on each node tab
   Select the **Set Up Individually** check box.
   Confirm that the VPC ID specified on the **Common** tab is entered in the **VPC ID** box (corresponds to [1] in Figure 5.1 System Configuration of the HA Cluster Based on VIP Control).

Enter the ENI ID of the instance corresponding to the node in the **ENI ID** box (corresponds to [7] and [8] in Figure 5.1 System Configuration of the HA Cluster Based on VIP Control).



7. Click **Finish** to complete setting.

3) **Add a monitor resource.**

- AWS AZ monitor resource

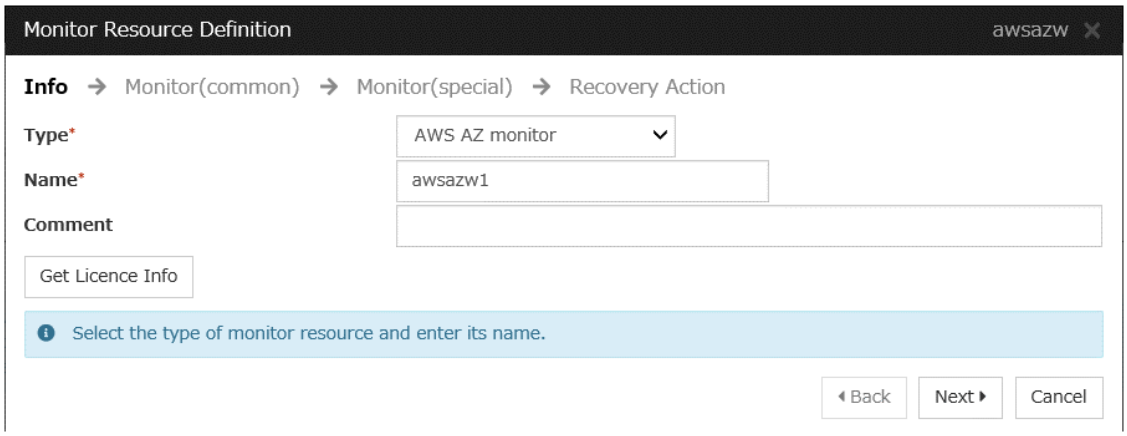
  Create an AWS AZ monitor resource to check whether the specified AZ is usable by using the monitor command.

  For details, refer to the following:

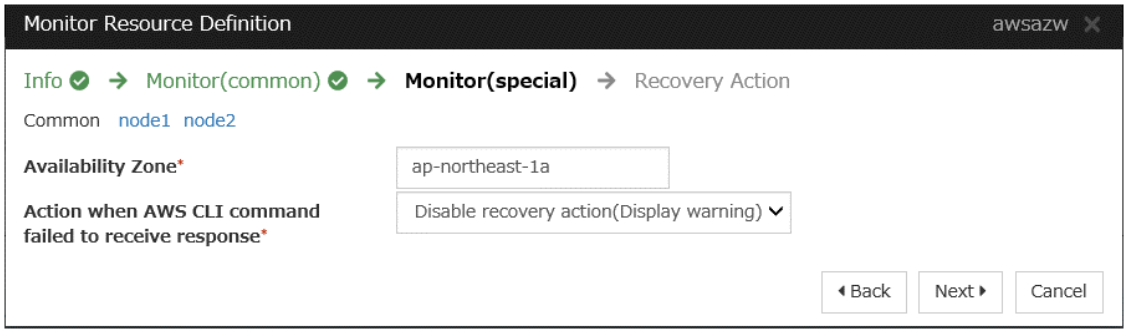
  Reference Guide
  -> Understanding AWS AZ monitor resources

  Steps

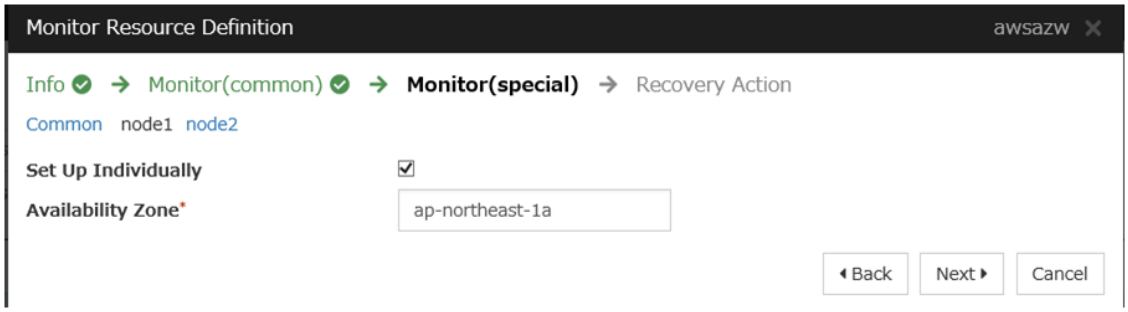
  1. Click **Add** in **Monitor Resource List**.
  2. Select the monitor resource type (AWS AZ monitor) from the **Type** box and enter the monitor resource name (awsazw1) in the **Name** box. Click **Next**.

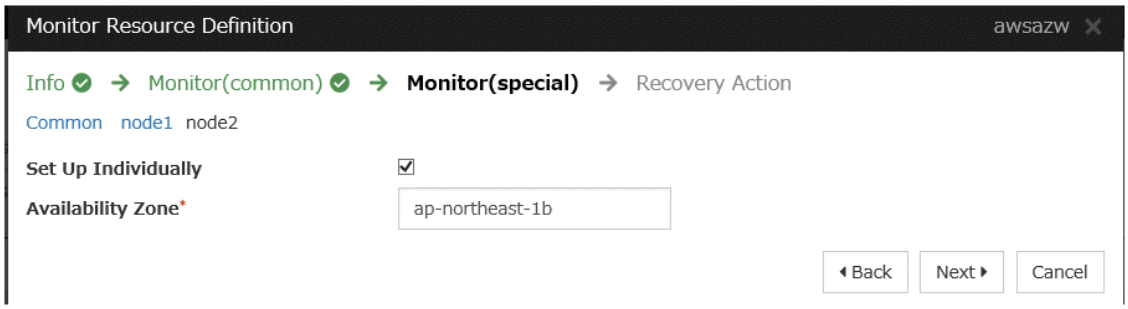


3. The **Monitor (common)** window is displayed.
   Click **Next** without specifying anything.
4. The **Monitor (special)** window is displayed.
   Enter the AZ to be monitored in the **Availability Zone** box on the **Common** tab. (Specify the AZ of the active server instance.) (corresponds to [2] in Figure 5.1 System Configuration of the HA Cluster Based on VIP Control)

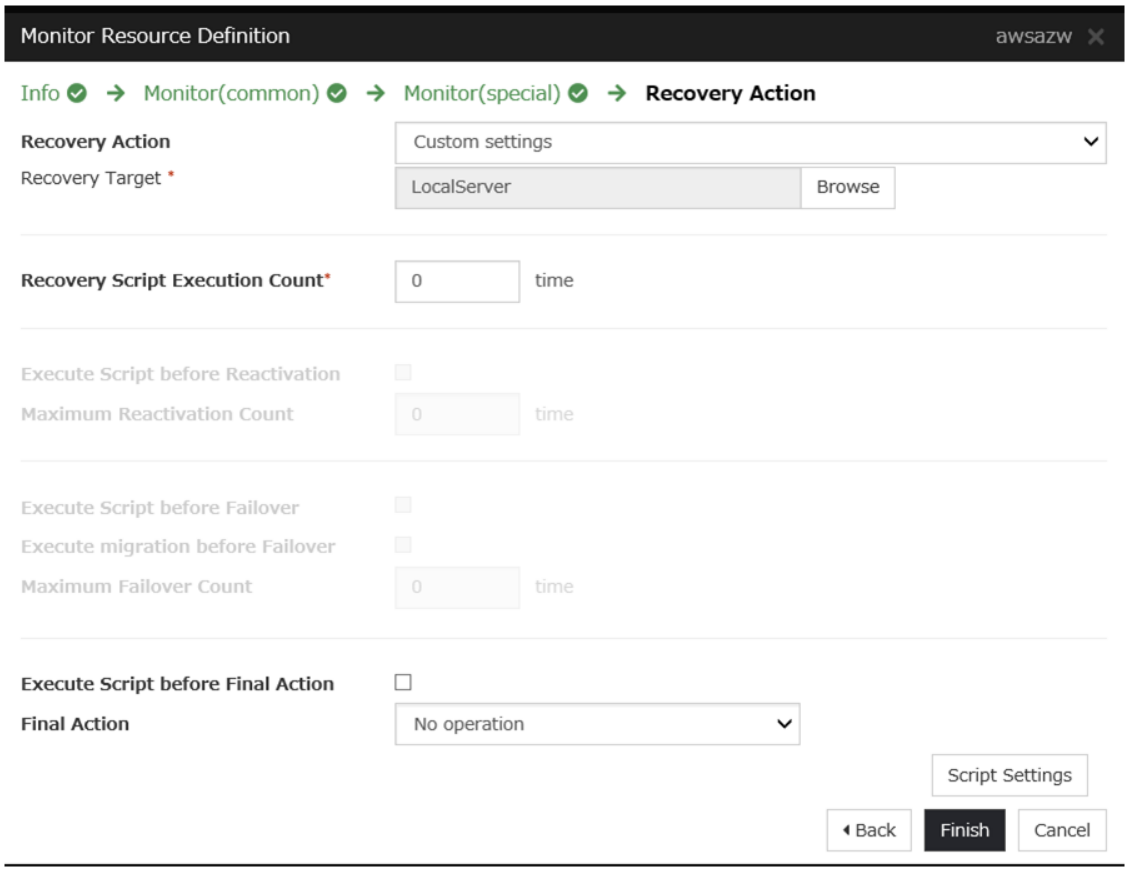


5. Specify the node settings on each node tab.
   Select the **Set Up Individually** check box.
   Enter the AZ of the instance corresponding to the node in the **Availability Zone** box. (corresponds to [2] and [3] in Figure 5.1 System Configuration of the HA Cluster Based on VIP Control) Click **Next**.





6. The **Recovery Action** window is displayed.
   Set LocalServer in the **Recovery Target** box.



7. Click **Finish** to complete setting.

- AWS Virtual IP monitor resource

  This resource is automatically added when the AWS Virtual IP resource is added.

  The resource checks the existence of the VIP address and the health of the route table.

For details, refer to the following:

Reference Guide
-> Understanding AWS Virtual IP monitor resources

4) **Apply the settings and start the cluster.**

1. Click **Apply the Configuration File** on the **File** in the config mode of Cluster WebUI.
   If the upload succeeds, the message saying "The application finished successfully."
2. Select the **Operation Mode** on the drop down menu of the toolbar in Cluster WebUI to switch to the operation mode.
3. The procedure depends on the resource used. For details, refer to the following: Installation and Configuration Guide -> How to create a cluster

CHAPTER

SIX

CONSTRUCTING AN HA CLUSTER BASED ON EIP CONTROL

This chapter describes how to construct an HA cluster based on EIP control.

In the figure below, "Server Instance (Active)" and "Server Instance (Standby)" respectively represent the instance of the active server and that of the standby server.

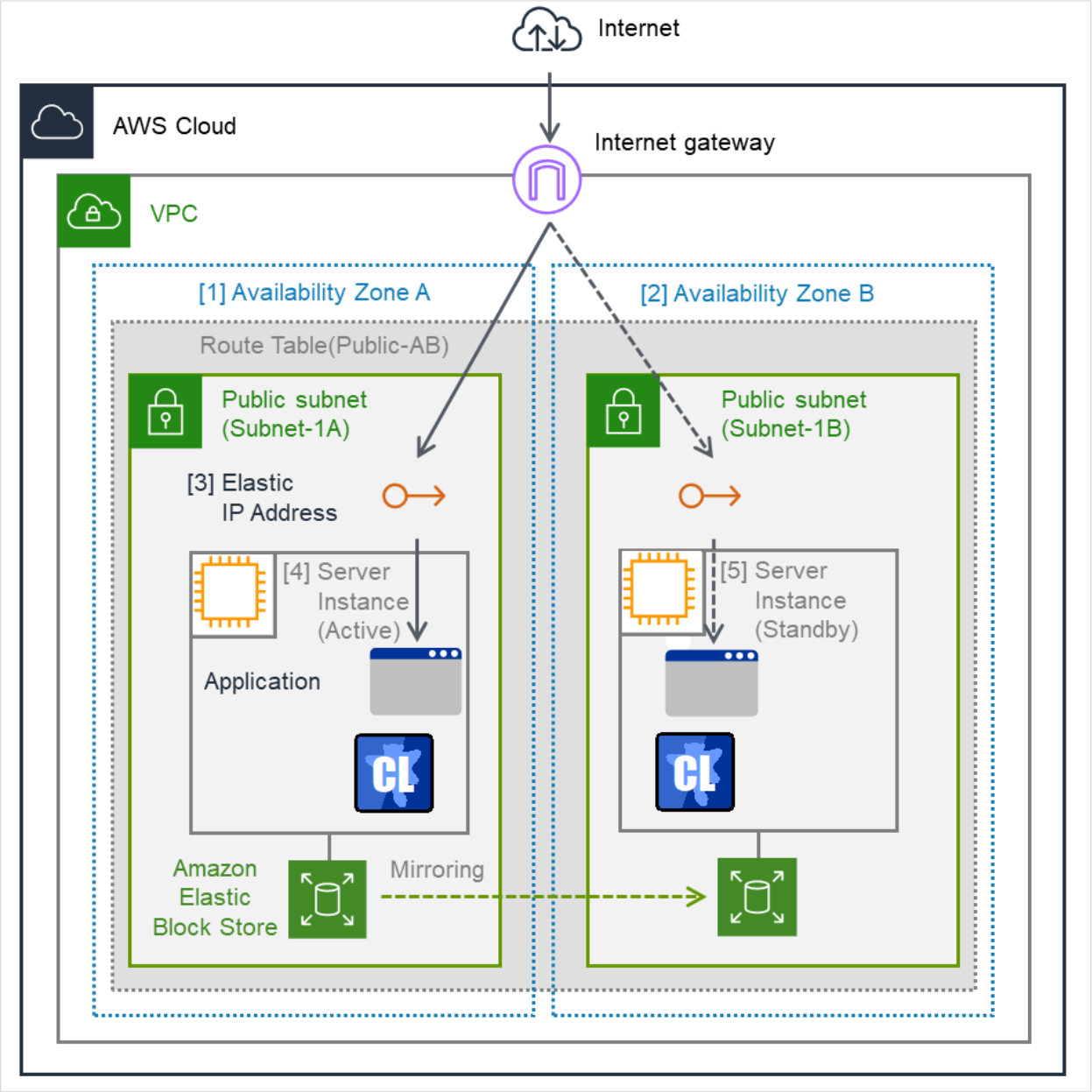


Fig. 6.1: System Configuration of the HA cluster based on EIP control

CIDR (VPC)	10.0.0.0/16
Public subnet (Subnet-1A)	10.0.10.0/24
Public subnet (Subnet-1B)	10.0.20.0/24

6.1 Configuring the VPC Environment

Configure the VPC on the VPC Management console and EC2 Management console.
The IP address used in the figures and description is an example. In the actual configuration, use the actual IP address assigned to the VPC. When installing EXPRESSCLUSTER in the existing VPC, specify the appropriate settings such as adding a subnet if the number of subnets is insufficient.

1) **Configure the VPC and subnet.**

   Create a VPC and subnet first.

   -> Add a VPC and subnet in **VPC** and **Subnets** on the VPC Management console.

2) **Configure the Internet gateway.**

   Add an Internet gateway to access the Internet from the VPC.

   -> To create an Internet gateway, select **Internet Gateways > Create internet gateway** on the VPC Management console. Attach the created Internet gateway to the VPC.

3) **Configure the network ACL and security group.**

   Specify the appropriate network ACL and security group settings to prevent unauthorized network access from in and out of the VPC.
   Change the network ACL and security group path settings so that the instances of the HA cluster node can communicate with the Internet gateway via HTTPS, communicate with Cluster WebUI, and communicate with each other. The instances are to be placed on the public networks (Subnet-1A and Subnet-1B).

   -> Change the settings in **Network ACLs** and **Security Groups** on the VPC Management console.

   For the port numbers that are used by the EXPRESSCLUSTER components, refer to the following:

   - Getting Started Guide
     -> Notes and Restrictions
     -> Before installing EXPRESSCLUSTER

4) **Add an HA cluster instance.**

   Create an HA cluster node instance on the public networks (Subnet-1A and Subnet-1B).
   When creating an HA cluster node instance, be sure to specify the setting to enable a public IP. If an instance is created without using a public IP, it is necessary to add an EIP or NAT needs to be prepared.
   (This guide does not describe this case.)

   -> To create an instance, select **Instances > Launch Instance** on the EC2 Management console.

   -> For details about the IAM settings, refer to the following:

   Getting Started Guide
   -> Notes and Restrictions
   -> Before installing EXPRESSCLUSTER
   -> IAM settings in the AWS environment

Check the ID of the elastic network interface (ENI) assigned to each created instance.

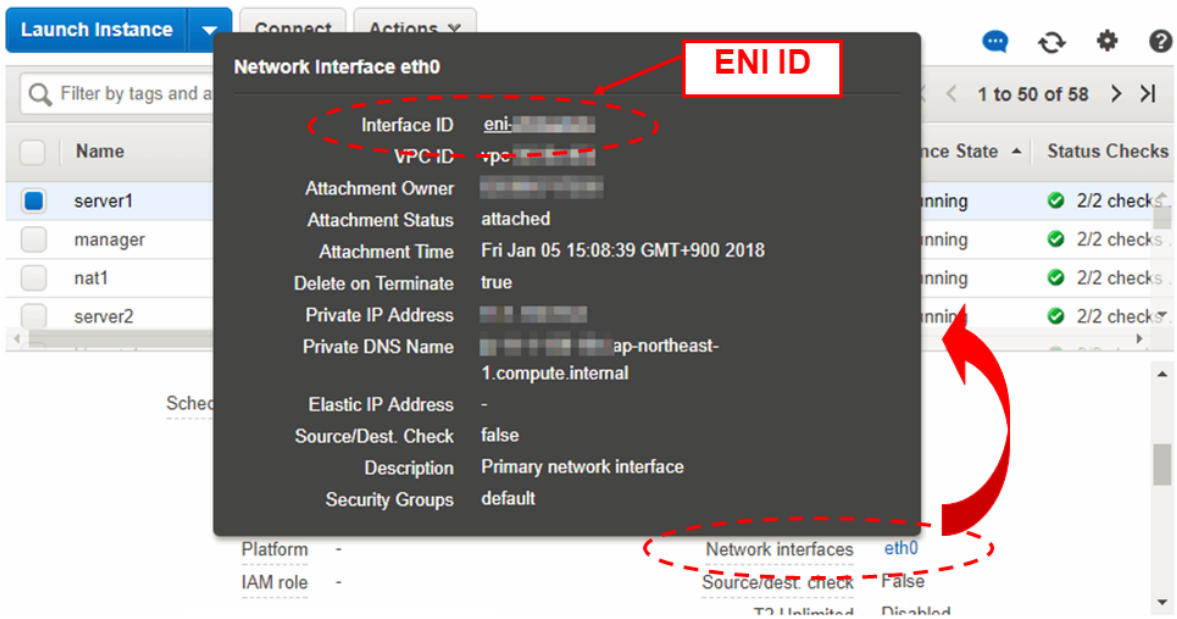
[4] Server Instance (Active), [5] Server Instance (Standby)

The ENIs assigned respectively to the instance of the active server and the instance of the standby server can be identified according to the ENI IDs.

Write down the ENI ID (eni-xxxxxxxx) of each instance, because the ID is needed later for setting up the AWS elastic IP resource.

Use the following procedure to check the ENI ID assigned to the instance.

1. Select the instance to display its detailed information.
2. Click the target device in **Network Interfaces**.
3. Check **Interface ID** displayed in the pop-up window.



5) **Add an EIP.**

Add an EIP to access an instance in the VPC from the Internet.

-> To add an EIP, select **Elastic IPs > Allocate new address** on the EC2 Management console.

[3] Elastic IP Address

The EIP can be identified according to the EIP Allocation ID.

Write down the Allocation ID (eipalloc-xxxxxxxx) of the added EIP, because the ID is needed later for setting up the AWS elastic IP resource.

6) **Configure the route table.**

Add the routing to the Internet gateway so that the AWS CLI can communicate with the regional endpoint via NAT.

The following routings must be set in the route table (Public-AB) of the public networks (Subnet-1A and Subnet-1B in the above figure).

- Route table (Public-AB)

Destination	Target	Remarks
VPC network (Example: 10.0.0.0/16)	local	Existing by default
0.0.0.0/0	Internet Gateway	Add (required)

When a failover occurred, the AWS Elastic IP resource deassigns the EIP assigned to the active server instance by using the AWS CLI, and assign it to the standby server instance.

Configure other routings according to the environment.

7) **Add a mirror disk (EBS).**

Add an EBS to be used as the mirror disk (cluster partition or data partition) as needed.

-> To add an EBS, select **Volumes > Create volume** on the EC2 Management console, and then attach the created volume to an instance.

6.2 Configuring the instance

Log in to each instance of the HA cluster and specify the following settings.

For the AWS CLI versions supported by EXPRESSCLUSTER, refer to the following:

- Getting Started Guide
-> Installation requirements for EXPRESSCLUSTER
-> Operation environment for AWS Elastic IP resource, AWS Elastic IP monitor resource, AWS AZ monitor resource

1) **Adjusting the OS startup time, verifying the network settings, verifying the root file system, verifying the firewall settings, synchronizing the server clock, and verifying the SELinux settings**

   For information on each of the procedures, refer to the following:
   - "Installation and Configuration Guide" -> "Determining a system configuration" -> "Settings after configuring hardware"

2) **Install the AWS CLI.**

   Install the AWS CLI.

   The installation path of the AWS CLI must be any of the following:

   ```
   /sbin, /bin, /usr/sbin, /usr/bin, /usr/local/bin
   ```

   For details about how to set up the AWS CLI, refer to the following:
   https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html

   (If EXPRESSCLUSTER has been installed before installing the AWS CLI, be sure to restart the OS before using EXPRESSCLUSTER.)

3) **Register the AWS access key ID.**

   Run the following command from the shell.

   ```
   $ sudo aws configure
   ```

   Enter information such as the AWS access key ID to the inquiries.
   The settings to be specified vary depending on whether an IAM role is assigned to the instance or not.

   - Instance to which an IAM role is assigned.

     ```
     AWS Access Key ID [None]: (Press Enter without entering anything.)
     AWS Secret Access Key [None]: (Press Enter without entering anything.)
     Default region name [None]: <default region name>
     Default output format [None]: text
     ```

- Instance to which an IAM role is not assigned.

```
AWS Access Key ID [None]: <AWS access key ID>
AWS Secret Access Key [None]: <AWS secret access key>
Default region name [None]: <default region name>
Default output format [None]: text
```

For "Default output format", other format than "text" may be specified.
If you specified incorrect settings, delete the directory `/root/.aws` entirely, and specify the above settings again.

4) **Prepare the mirror disk.**

If an EBS has been added to be used as the mirror disk, divide the EBS into partitions and use each partition as the cluster partition and data partition.
For details about the mirror disk partition, refer to the following:

Installation and Configuration Guide
-> Determining a system configuration
-> Partition settings for Mirror disk resource (when using Replicator)

5) **Install EXPRESSCLUSTER.**

For the installation procedure, refer to "Installation and Configuration Guide".
Store the EXPRESSCLUSTER installation media in the environment to which to install EXPRESSCLUSTER.
(To transfer data, use any method such as Remote Desktop and Amazon S3.)
After the installation, restart the OS.

6.3 Setting up EXPRESSCLUSTER

For details about how to set up and connect to Cluster WebUI, refer to the following:

Installation and Configuration Guide
-> Creating the cluster configuration data

This section describes how to add the following resources:

- Mirror disk resource
- AWS Elastic IP resource
- AWS AZ monitor resource
- AWS Elastic monitor resource
- NP resolution (HTTP method)

For the settings other than the above, refer to "Installation and Configuration Guide".

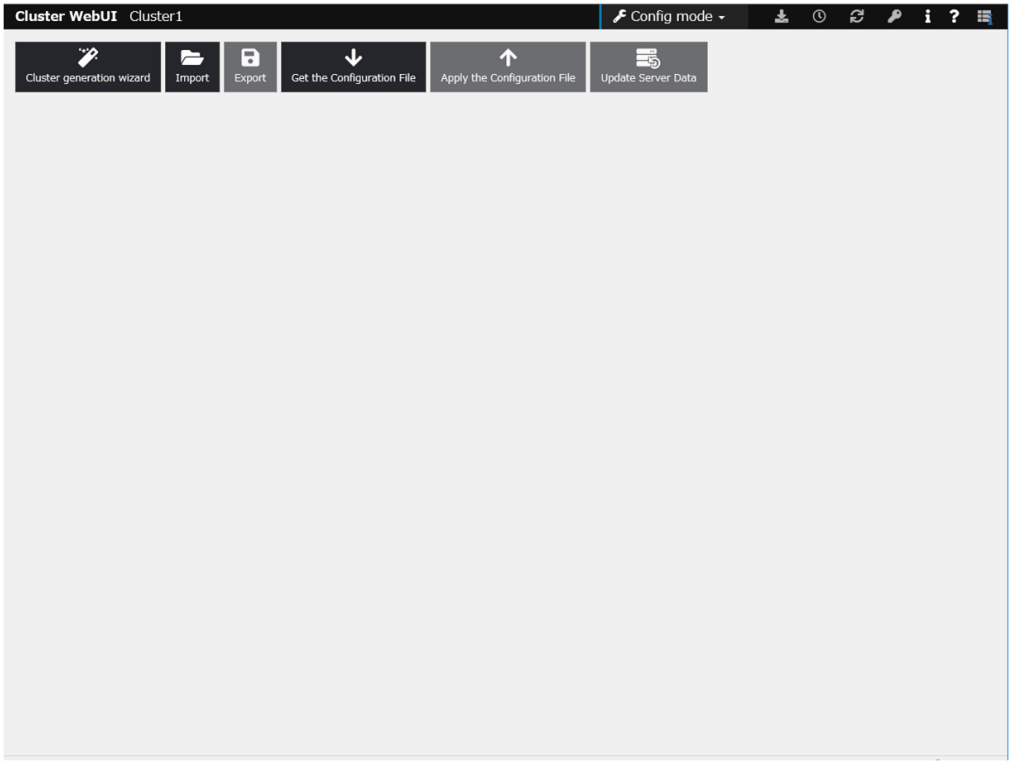
1) **Construct a cluster.**

   Start the Cluster generation wizard to construct a cluster.

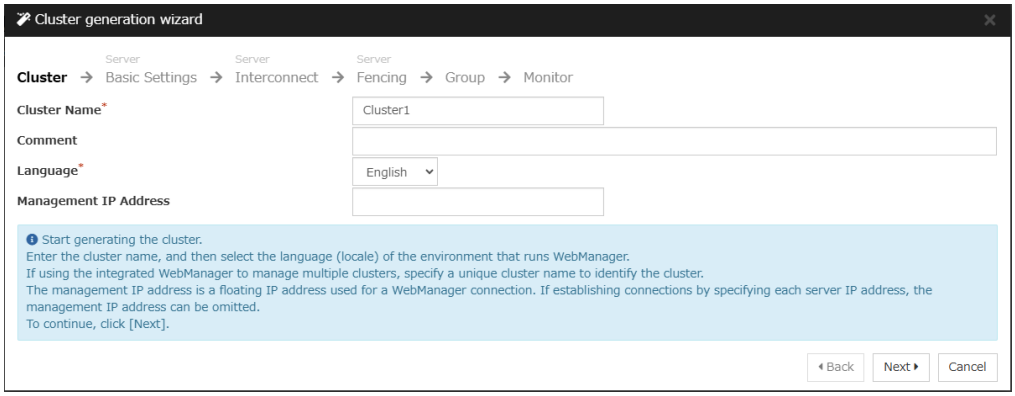
   - Construct a cluster.

     Steps

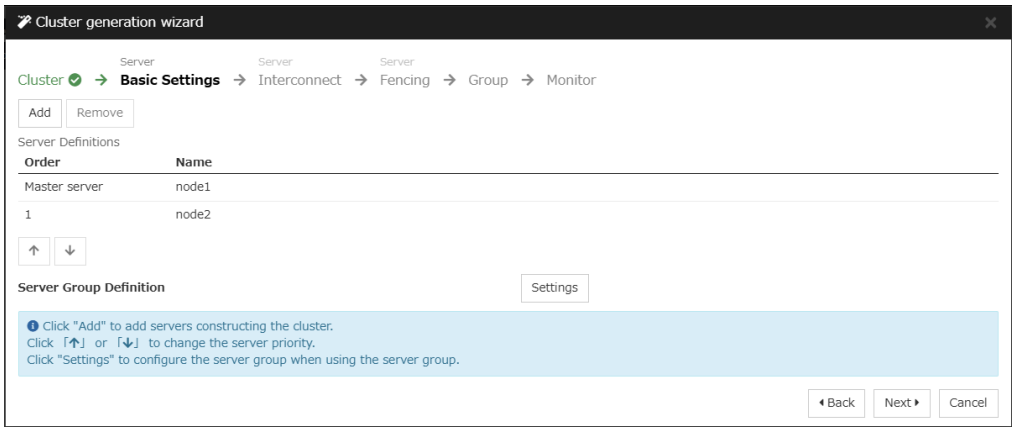
     1. Access Cluster WebUI, and click **Cluster generation wizard**.



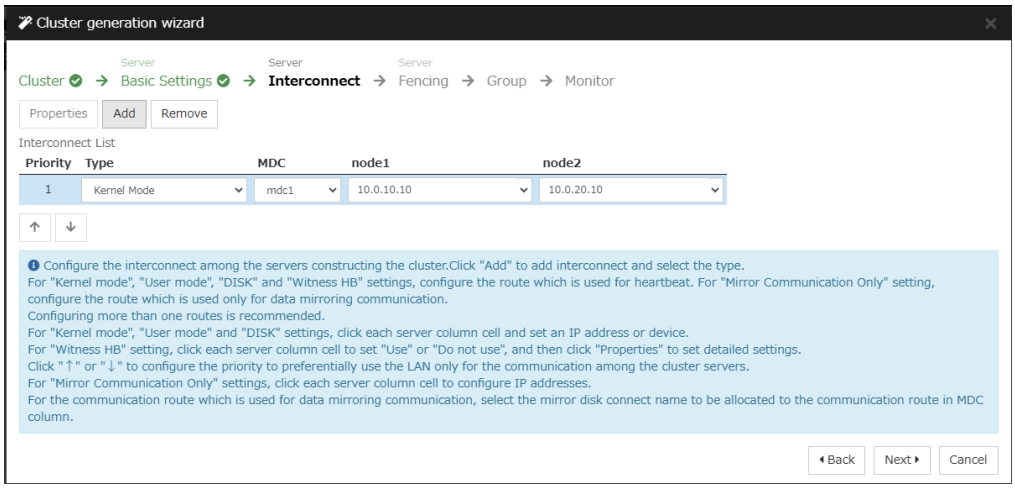
2. The **Cluster** window on the **Cluster Generation Wizard** is displayed.
   Enter a cluster name in **Cluster Name**.
   Select an appropriate language from **Language**. Click **Next**.



3. The **Basic Settings** window is displayed.
   The instance connecting to Cluster WebUI is displayed as the registered master server.
   Click **Add** to add other instances (by specifying their private IP addresses). Click **Next**.



4. The **Interconnect** window is displayed.
   Specify the IP address (private IP address of each instance) to be used for interconnect. Select mdc1 from **MDC** for the communication path of the mirror disk resource to be created later.
   Click **Next**.



5. The **Fencing** window is displayed.
   Set the HTTP NP resolution.
   Click **Next**.

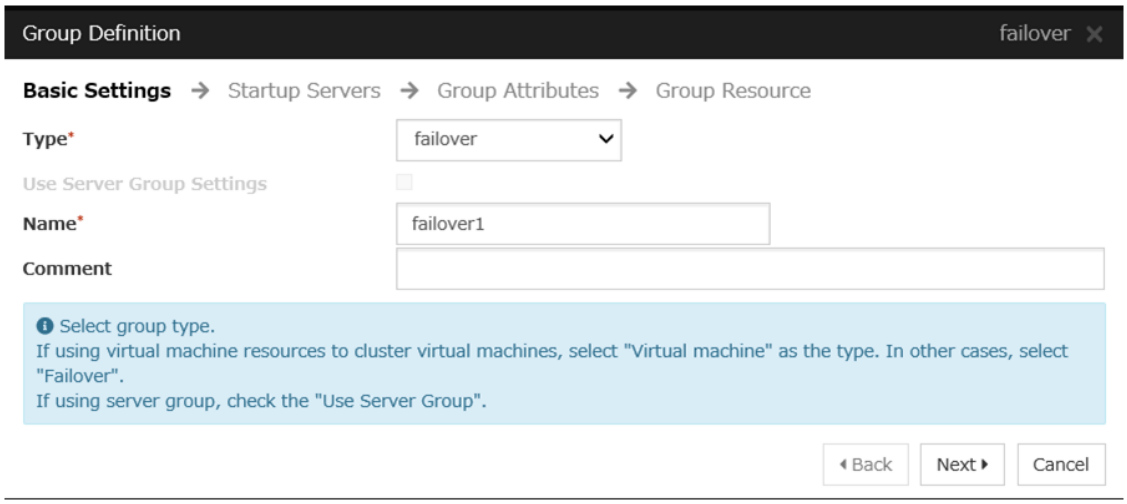
2) **Add a group resource.**

- Group definition

  Create a failover group.

  Steps

  1. The **Group List** window is displayed.
     Click **Add**.
  2. The **Group Definition** dialog box is displayed.
     Enter the failover group name (failover1) in the **Name** box. Click **Next**.



3. The **Startup Servers** window is displayed.
   Click **Next** without specifying anything.

4. The **Group Attributes** window is displayed.
   Click **Next** without specifying anything.
5. The **Group Resource** window is displayed.
   Add a group resource on this page following the procedure below.

- Mirror disk resource

  Create the mirror disk resource according to the mirror disk (EBS) as needed.

  For details, refer to the following:

  - Reference Guide
    -> Understanding Mirror disk resources

  Steps

  1. Click **Add** in **Group Resource List**.
  2. The **Resource Definition of Group | failover1** window is displayed.
     Select the group resource type (Mirror disk resource) from the **Type** box and enter the group resource name (md) in the **Name** box. Click **Next**.
  3. The **Dependency** window is displayed.
     Click **Next** without specifying anything.
  4. The **Recovery Operation** window is displayed.
     Click **Next**.
  5. Enter the device name for the partition set up in "*Configuring the instance*" -> "6. **Prepare the mirror disk.**" in **Data Partition Device Name** and **Cluster Partition Device Name**. Specify Mount Point and File System. Click Finish to finish setting.

- AWS Elastic IP resource

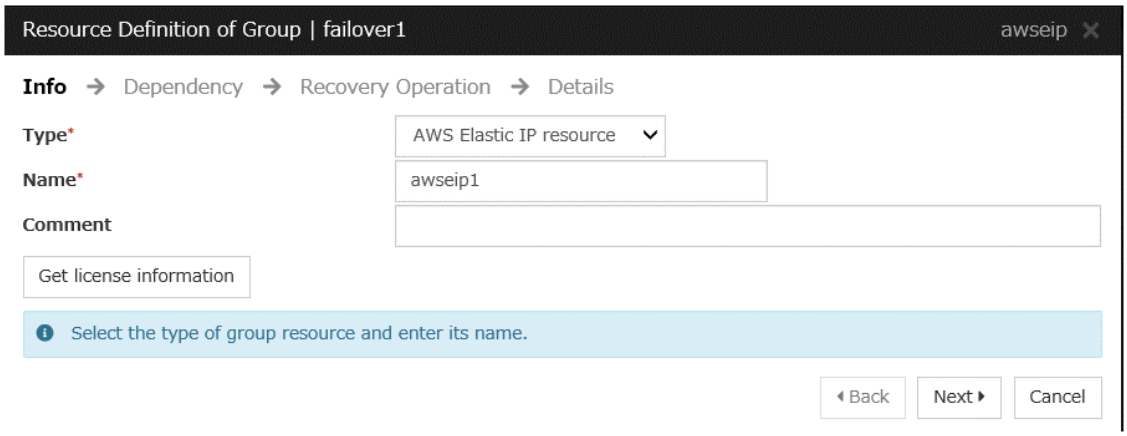
  Add an AWS Elastic IP resource that controls the EIP by using the AWS CLI.

  For details, refer to the following:

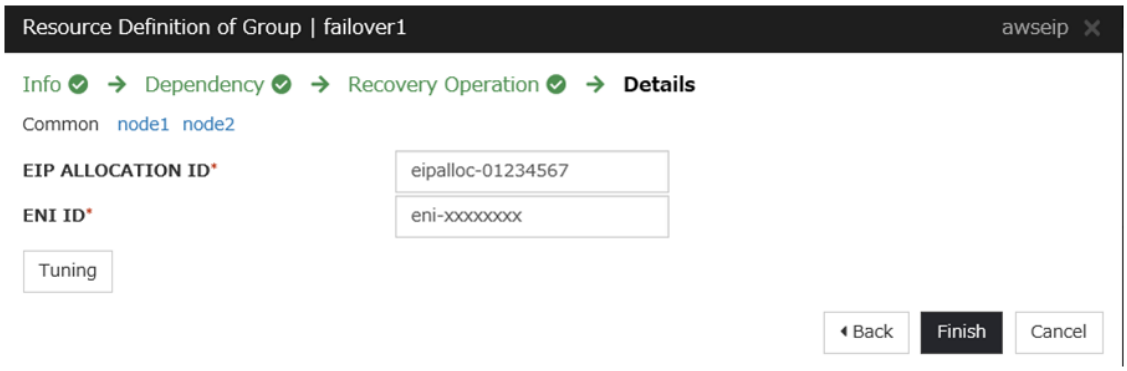
  - Reference Guide
    -> Understanding AWS Elastic IP resources

  Steps

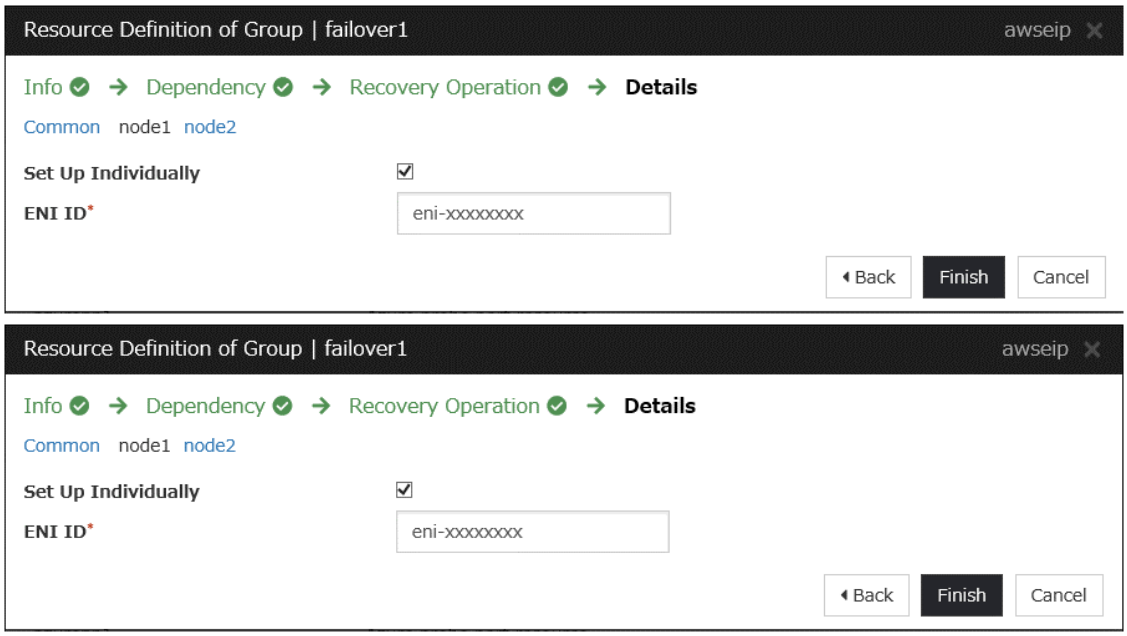
  1. Click **Add** in **Group Resource List**.
  2. The **Resource Definition of Group | failover1** window is displayed.
     Select the group resource type (AWS Elastic IP resource) from the **Type** box and enter the group resource name (awseip1) in the **Name** box. Click **Next**.



3. The **Dependency** window is displayed. Click **Next** without specifying anything.
4. The **Recovery Operation** window is displayed.
   Click **Next**.
5. The **Details** window is displayed.
   Enter the allocation ID of the EIP to be assigned in the **EIP ALLOCATION ID** box on the **Common** tab (corresponds to [3] and [4] in Figure 6.1 System Configuration of the HA cluster based on EIP control).
   Enter the ENI ID of the active server instance to which the EIP is assigned in the **ENI ID** box.



6. Specify the node settings on each node tab
   Select the **Set Up Individually** check box.
   Enter the ENI ID of the instance corresponding to the node in the **ENI ID** box (corresponds to [4] and [5] in Figure 6.1 System Configuration of the HA cluster based on EIP control).



7. Click **Finish** to complete setting.

3) **Add a monitor resource.**

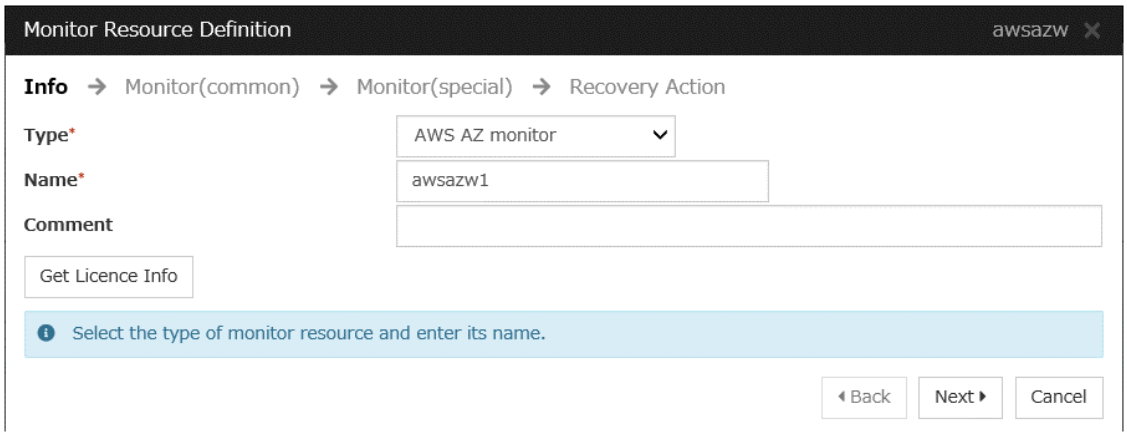
- AWS AZ monitor resource

Create the AWS AZ monitor resource to check whether the specified AZ is usable by using the monitor command.
For details, refer to the following:

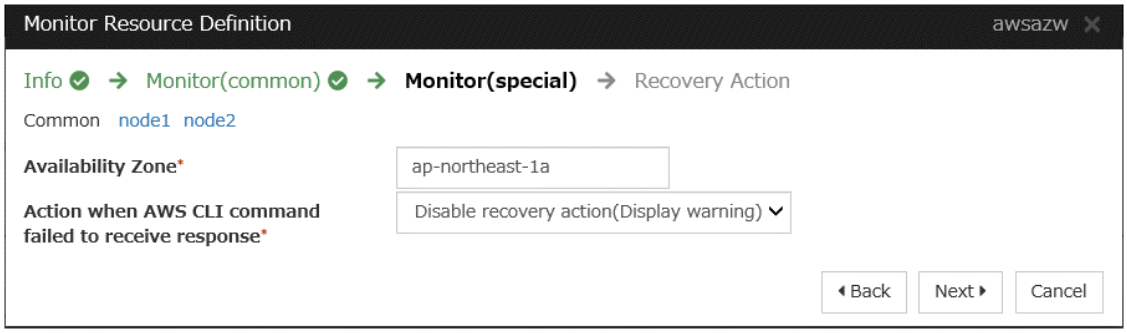
- Reference Guide
  -> Understanding AWS AZ monitor resources

Steps

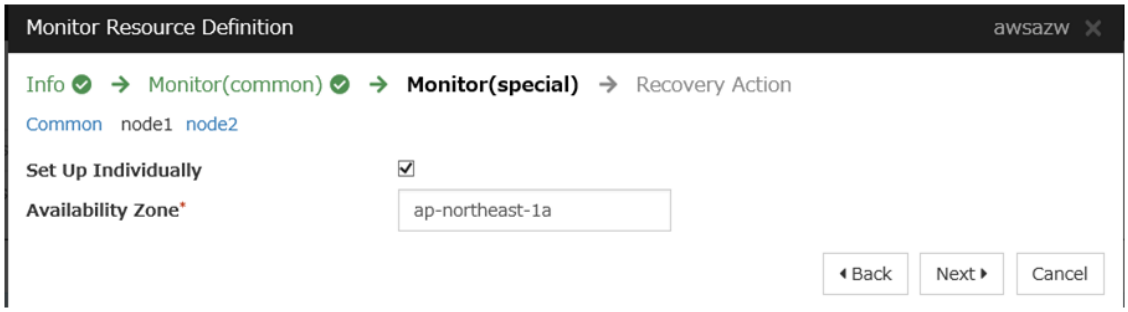
1. Click **Add** in **Monitor Resource List**.
2. Select the monitor resource type (AWS AZ monitor) from the **Type** box and enter the monitor resource name (awsazw1) in the **Name** box. Click **Next**.

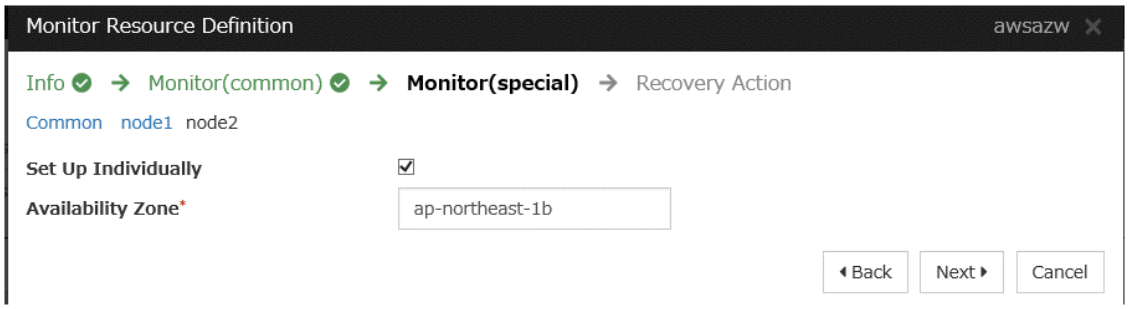


3. The **Monitor (common)** window is displayed.
   Click **Next** without specifying anything.
4. The **Monitor (special)** window is displayed.
   Enter the AZ to be monitored in the **Availability Zone** box on the **Common** tab. (Specify the AZ of the active server instance.) (corresponds to [1] in Figure 6.1 System Configuration of the HA cluster based on EIP control)

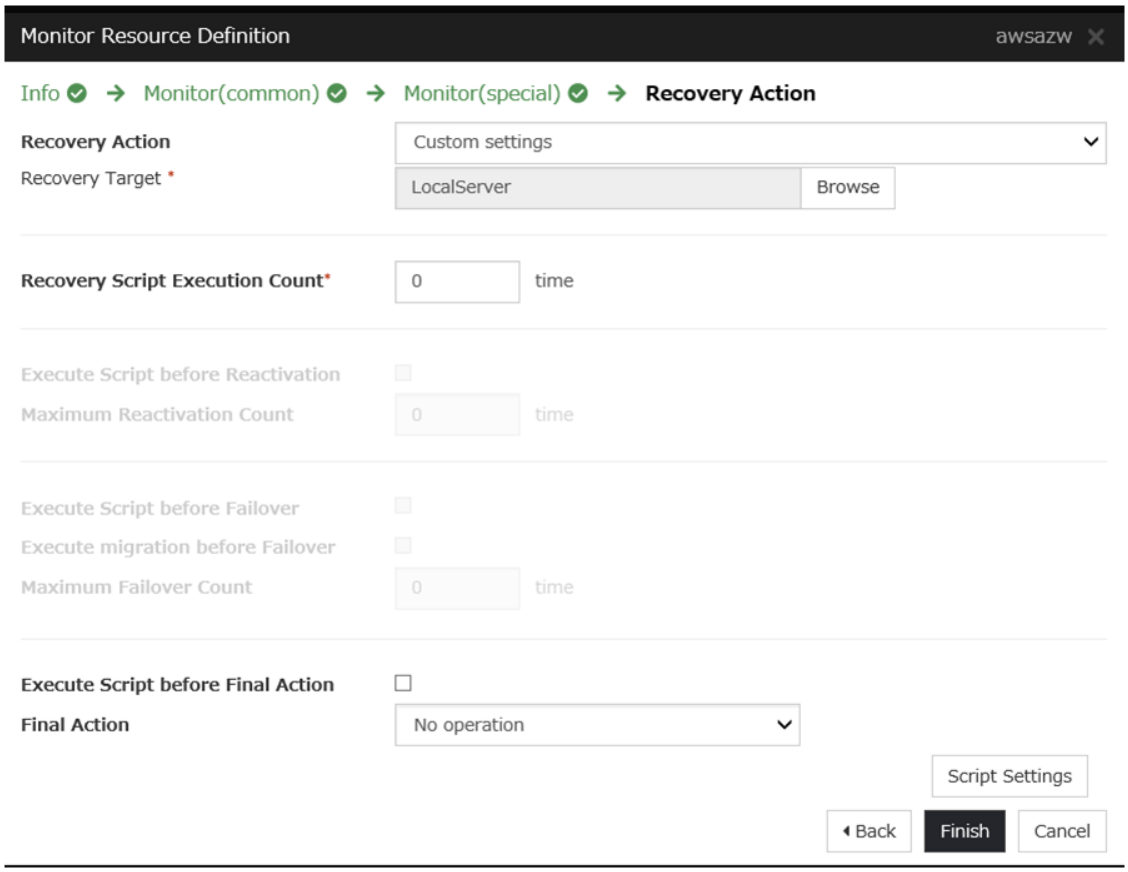


5. Specify the node settings on each node tab
   Select the **Set Up Individually** check box.
   Enter the AZ of the instance corresponding to the node in the **Availability Zone** box (corresponds to [1] and [2] in Figure 6.1 System Configuration of the HA cluster based on EIP control). Click **Next**.





6. The **Recovery Action** window is displayed.
   Set LocalServer in the **Recovery Target** box.



7. Click **Finish** to complete setting.

- AWS Elastic IP monitor resource

  This resource is automatically added when the AWS Elastic IP resource is added.
  The health of the EIP address can be checked by monitoring the communication with the EIP address that is assigned to the active server instance.
  For details, refer to the following:

Reference Guide
-> Understanding AWS Elastic IP monitor resources

4) **Apply the settings and start the cluster.**

1. Click **Apply the Configuration File** on the **File** in the config mode of Cluster WebUI.
   If the upload succeeds, the message saying "The application finished successfully."
2. Select the **Operation Mode** on the drop down menu of the toolbar in Cluster WebUI to switch to the operation mode.
3. The procedure depends on the resource used. For details, refer to the following: Installation and Configuration Guide -> How to create a cluster

CHAPTER

SEVEN

CONSTRUCTING AN HA CLUSTER BASED ON DNS NAME CONTROL

This chapter describes how to construct an HA cluster based on DNS name control.

In the figure below, "Server Instance (Active)" and "Server Instance (Standby)" respectively represent the instance of the active server and that of the standby server.

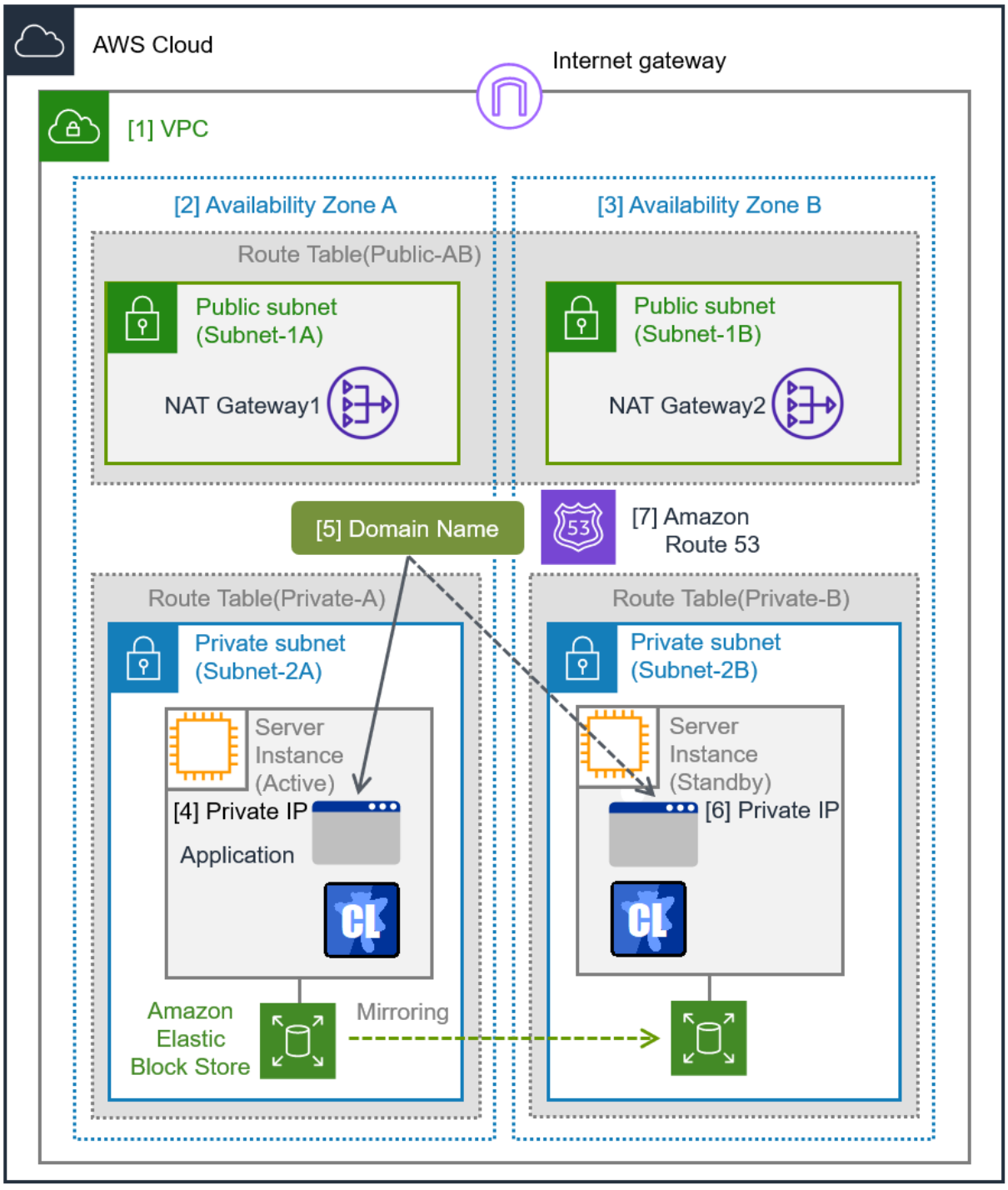


Fig. 7.1: System Configuration HA Cluster Based on DNS Name Control

CIDR (VPC)	10.0.0.0/16
Domain Name	srv.hz1.local
Public subnet (Subnet-1A)	10.0.10.0/24

Continued on next page

Table 7.1 – continued from previous page

Public subnet (Subnet-1B)	10.0.20.0/24
Private subnet (Subnet-2A)	10.0.110.0/24
Private subnet (Subnet-2B)	10.0.120.0/24

7.1 Configuring the VPC Environment

Configure the VPC on the VPC Management console and EC2 Management console.

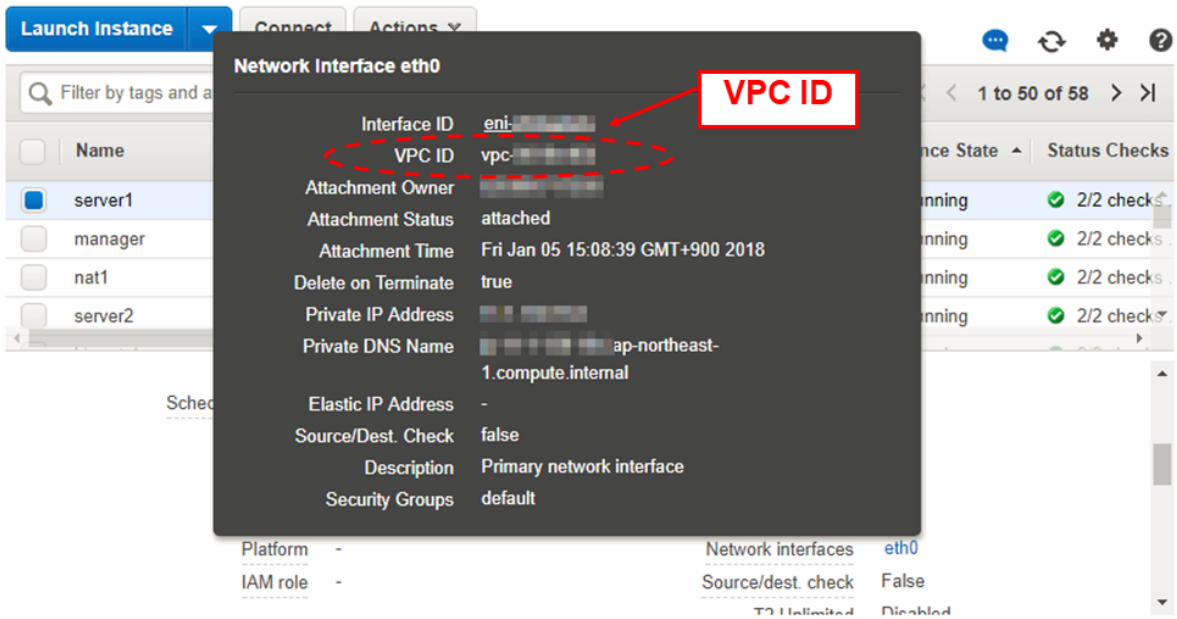
The IP addresses used in the figures and description are an example. In the actual configuration, use the actual IP addresses assigned to the VPC. When installing EXPRESSCLUSTER in the existing VPC, specify the appropriate settings such as adding a subnet if the number of subnets is insufficient.

1) **Configure the VPC and subnet.**

   Create a VPC and subnet first.

   -> Add a VPC and subnet in **VPC** and **Subnets** on the VPC Management console.

   [1] VPC Write down the VPC ID (vpc-xxxxxxxx), which is needed later for adding the Hosted Zone.



2) **Configure the Internet gateway.**

   Add an Internet gateway to access the Internet from the VPC.

   -> To create an Internet gateway, select **Internet Gateways > Create internet gateway** on the VPC Management console. Attach the created Internet gateway to the VPC.

3) **Configure the network ACL and security group.**

   Specify the appropriate network ACL and security group settings to prevent unauthorized network access from in and out of the VPC.

   Change the network ACL and security group path settings so that the instances of the HA cluster node can communicate with the Internet gateway via HTTPS, communicate with Cluster WebUI, and communicate with each other. The instances are to be placed on the private networks (Subnet-2A and Subnet-2B).

   -> Change the settings in **Network ACLs** and **Security Groups** on the VPC Management console.

   For the port numbers that are used by the EXPRESSCLUSTER components, refer to the following:

- Getting Started Guide
  -> Notes and Restrictions
  -> Before installing EXPRESSCLUSTER

4) **Add an HA cluster instance.**

Create an HA cluster node instance on the private networks (Subnet-2A and Subnet-2B).

-> To create an instance, select **Instances > Launch Instance** on the EC2 Management console.

-> For details about the IAM settings, refer to the following:

Getting Started Guide
-> Notes and Restrictions
-> Before installing EXPRESSCLUSTER
-> IAM settings in the AWS environment

5) **Add a NAT.**

To perform the VIP control by using the AWS CLI, communication from the instance of the HA cluster node to the regional endpoint via HTTPS must be enabled.

To do so, create a NAT gateway on the public networks (Subnet-1A and Subnet-1B).

For more information on the NAT gateway, see the corresponding AWS document.

6) **Configure the route table.**

Add the routing to the Internet gateway so that the AWS CLI can communicate with the regional endpoint via NAT.

The following routings must be set in the route table (Public-AB) of the public networks (Subnet-1A and Subnet-1B in the above figure).

- Route Table (Public-AB)

Destination	Target	Remarks
VPC network (Example: 10.0.0.0/16)	local	Existing by default
0.0.0.0/0	Internet gateway	Add (required)

The following routings must be set in the route tables (Private-A and Private-B) of the private networks (Subnet-2A and Subnet-2B in the above figure).

- Route Table (Private-A)

Destination	Target	Remarks
VPC network (Example: 10.0.0.0/16)	local	Existing by default
0.0.0.0/0	NAT Gateway1	Add (required)

- Route Table (Private-B)

Destination	Target	Remarks
VPC network (Example: 10.0.0.0/16)	local	Existing by default
0.0.0.0/0	NAT Gateway2	Add (required)

Configure other routings according to the environment.

7) **Add a Hosted Zone**

Private Hosted Zone is added to Amazon Route 53.

-> To add a hosted zone, select **DNS management > Created Hosted Zone** on the **Route 53 Management Console**. Select **Private Hosted Zone for Amazon VPC** from the **Type** box and set the ID of VPC where the instance belongs, in the **VPC ID** box.

[7] Amazon Route 53 (Hosted Zone)

The Hosted Zone can be identified according to the Hosted Zone ID.

Note the Hosted Zone ID separately because it will be needed for the setup of AWS DNS resource later.

The reason that this guide includes the procedure to add Private Hosted Zone is to make it possible to access from the client within the VPC with the cluster located on the Private subnet. When access from internet is required, cluster must be located on Public subnet, therefore Public Hosted Zone will be added.

8) **Add a mirror disk (EBS).**

Add an EBS to be used as the mirror disk (cluster partition or data partition) as needed.

-> To add an EBS, select **Volumes > Create Volume** on the EC2 Management console, and then attach the created volume to an instance.

7.2 Configuring the instance

Log in to each instance of the HA cluster and specify the following settings.
For the AWS CLI versions supported by EXPRESSCLUSTER, refer to the following:

- Getting Started Guide
  -> Installation requirements for EXPRESSCLUSTER
  -> Operation environment for AWS DNS resource, AWS DNS monitor resource

1) **Disable SELinux.**

   Set permissive or disabled to SELinux to perform communication required by EXPRESSCLUSTER. Run the following command to check the status of SELinux.

```
$ getenforce
Enforcing
```

   (* Enforcing indicates that SELinux is enabled.)

   Change the status of SELinux to "disabled" by using `/etc/sysconfig/selinux` and restart SELinux. Then run the getenforce command to confirm that Disabled is returned.

2) **Configure a firewall.**

   Change the firewall setting as needed.
   For the port numbers that are used by the EXPRESSCLUSTER components, refer to the following:

   - Getting Started Guide
     -> Notes and Restrictions
     -> Before installing EXPRESSCLUSTER

3) **Install the host command.**

   Install the host command.
   The host command is included in the bind-utils package.
   If the bind-utils package is not installed, install it by, for example, using the yum command.
   The path to the host command must be set in the PATH environment variable.

4) **Install the AWS CLI.**

   Install the AWS CLI.

   The installation path of the AWS CLI must be any of the following:
   `/sbin, /bin, /usr/sbin, /usr/bin, /usr/local/bin`

   For details about how to set up the AWS CLI, refer to the following:

https://docs.aws.amazon.com/cli/latest/userguide/cli-chap-install.html

(If EXPRESSCLUSTER has been installed before installing the AWS CLI, be sure to restart the OS before using EXPRESSCLUSTER.)

5) **Register the AWS access key ID.**

Run the following command from the shell.

```
$ sudo aws configure
```

Enter information such as the AWS access key ID to the inquiries.
The settings to be specified vary depending on whether an IAM role is assigned to the instance or not.

- Instance to which an IAM role is assigned.

```
AWS Access Key ID [None]: (Press Enter without entering anything.)
AWS Secret Access Key [None]: (Press Enter without entering anything.)
Default region name [None]: <default region name>
Default output format [None]: text
```

- Instance to which an IAM role is not assigned.

```
AWS Access Key ID [None]: <AWS access key ID>
AWS Secret Access Key [None]: <AWS secret access key>
Default region name [None]: <default region name>
Default output format [None]: text
```

For "Default output format", other format than "text" may be specified.
If you specified incorrect settings, delete the directory `/root/.aws` entirely, and specify the above settings again.

6) **Prepare the mirror disk.**

If an EBS has been added to be used as the mirror disk, divide the EBS into partitions and use each partition as the cluster partition and data partition.
For details about the mirror disk partition, refer to the following:

Installation and Configuration Guide
-> Determining a system configuration
-> Partition settings for Mirror disk resource (when using Replicator)

7) **Install EXPRESSCLUSTER.**

For the installation procedure, refer to "Installation and Configuration Guide".

Store the EXPRESSCLUSTER installation media in the environment to which to install EXPRESSCLUSTER. (To transfer data, use any method such as Remote Desktop and Amazon S3.)
After the installation, restart the OS.

7.3 Setting up EXPRESSCLUSTER

For details about how to set up and connect to Cluster WebUI, refer to the following:

Installation and Configuration Guide
-> Creating the cluster configuration data

This section describes how to add the following resources:

- Mirror disk resource
- AWS DNS resource
- AWS AZ monitor resource
- AWS DNS monitor resource
- NP resolution (HTTP method)

For the settings other than the above, refer to "Installation and Configuration Guide".

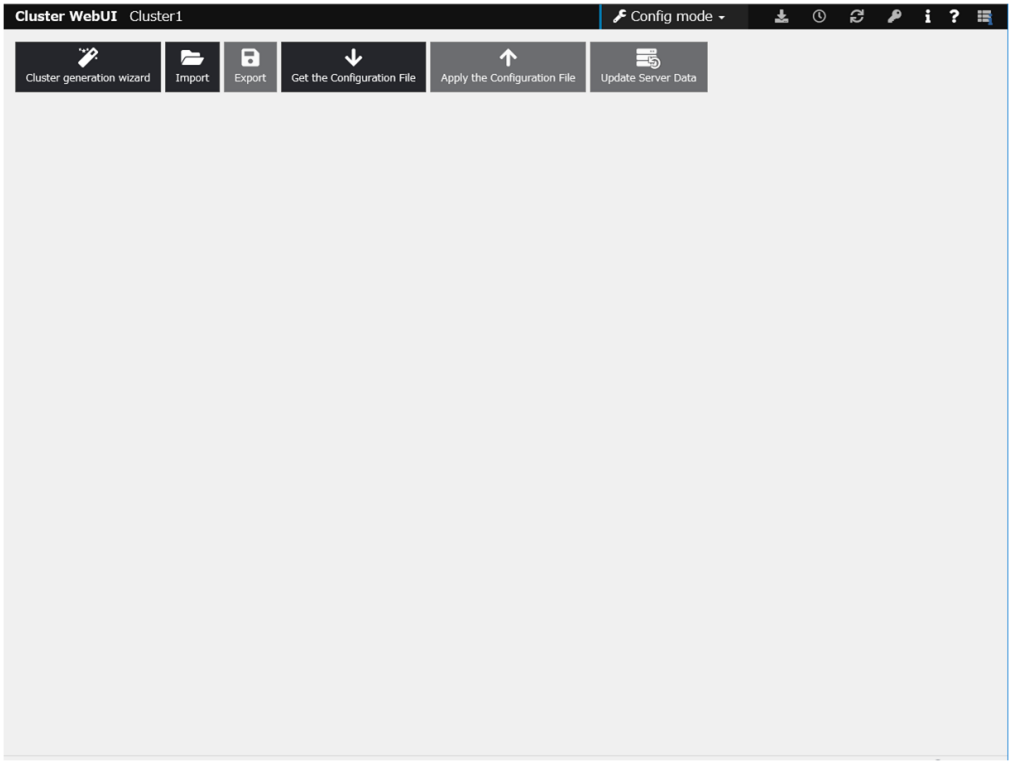
1) **Construct a cluster.**

   Start the Cluster generation wizard to construct a cluster.

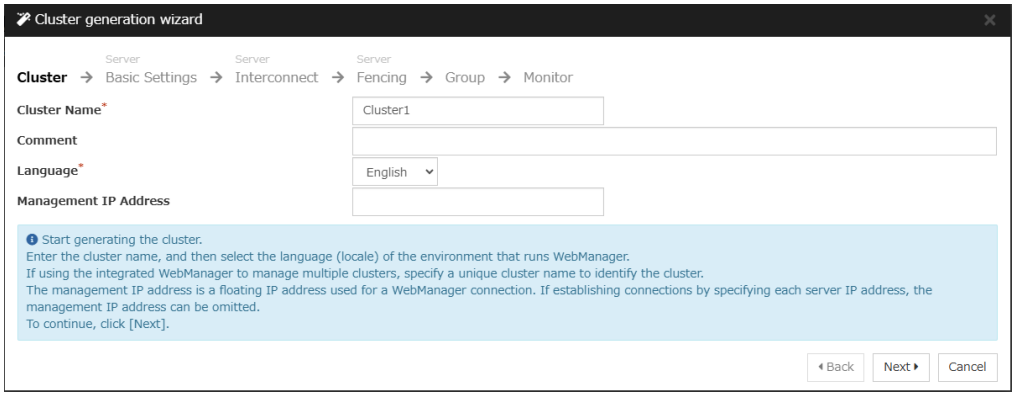
   - Construct a cluster.

     Steps

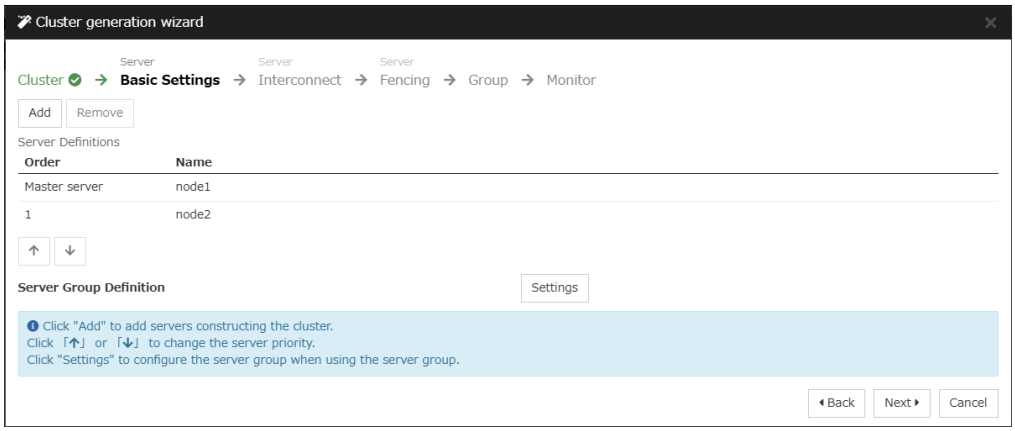
     1. Access Cluster WebUI, and click **Cluster generation wizard**.



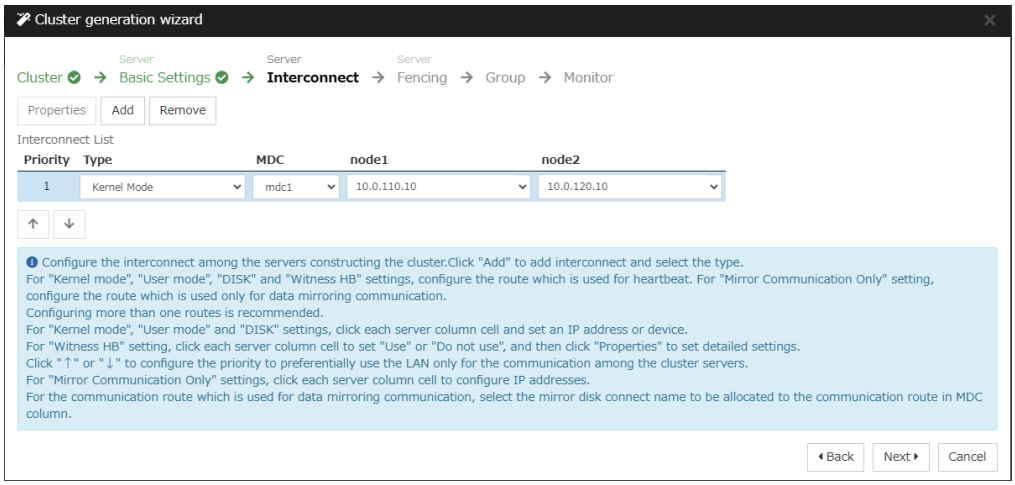
2. The **Cluster** window on the **Cluster Generation Wizard** is displayed.
   Enter a cluster name in **Cluster Name**.
   Select an appropriate language from **Language**. Click **Next**.



3. The **Basic Settings** window is displayed.
   The instance connecting to WebManager is displayed as the registered master server.
   Click **Add** to add other instances (by specifying their private IP addresses). Click **Next**.



4. The **Interconnect** window is displayed.
   Specify the IP address (private IP address of each instance) to be used for interconnect. Select mdc1 from **MDC** for the communication path of the mirror disk resource to be created later.
   Click **Next**.



5. The **Fencing** window is displayed.
   Set the HTTP NP resolution.
   Click **Next**.

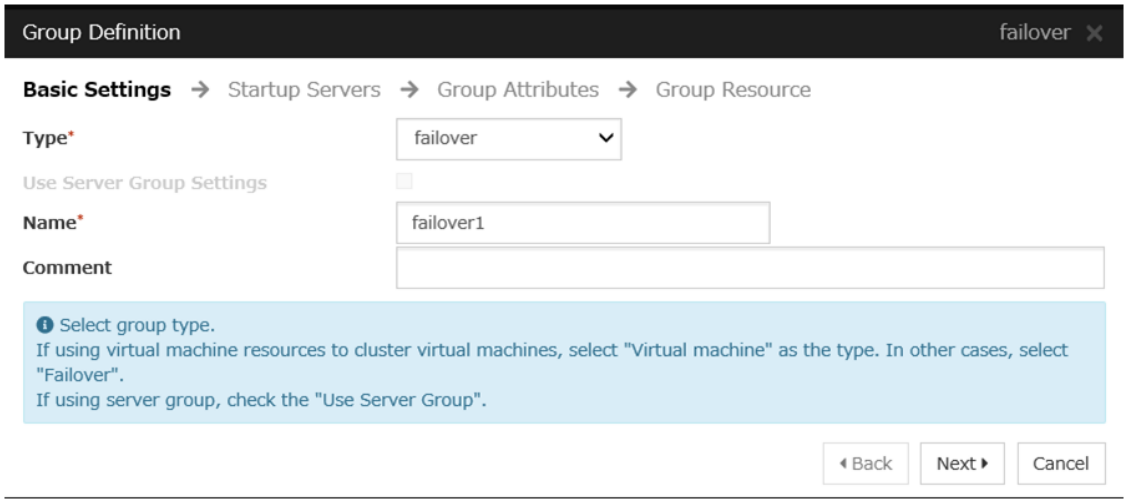
2) **Add a group resource.**

- Group definition

  Create a failover group.

  Steps

  1. The **Group List** window is displayed.
     Click **Add**.
  2. The **Group Definition** dialog box is displayed.
     Enter the failover group name (failover1) in the **Name** box. Click **Next**.



  3. The **Startup Servers** window is displayed.
     Click **Next** without specifying anything.

4. The **Group Attributes** window is displayed.
   Click **Next** without specifying anything.
5. The **Group Resource** window is displayed.
   Add a group resource on this page following the procedure below.

- Mirror disk resource

  Create a mirror disk resource according the mirror disk (EBS) as needed.

  For details, refer to the following:

  - Reference Guide
    -> Understanding Mirror disk resources

  Steps

  1. Click **Add** in **Group Resource List**.
  2. The **Resource Definition of Group | failover1**window is displayed.
     Select the group resource type (Mirror disk resource) from the **Type** box and enter the group resource name (md) in the **Name** box. Click **Next**.
  3. The **Dependency** window is displayed.
     Click **Next** without specifying anything.
  4. The **Recovery Operation** window is displayed.
     Click **Next**.
  5. Enter the drive letter for the partition set up in "*Configuring the instance*" -> "6. **Prepare the mirror disk.**" in **Data partition device name** and **Cluster partition device name**. Specify Mount Point and File System. Click Finish to finish setting.

- AWS DNS resource

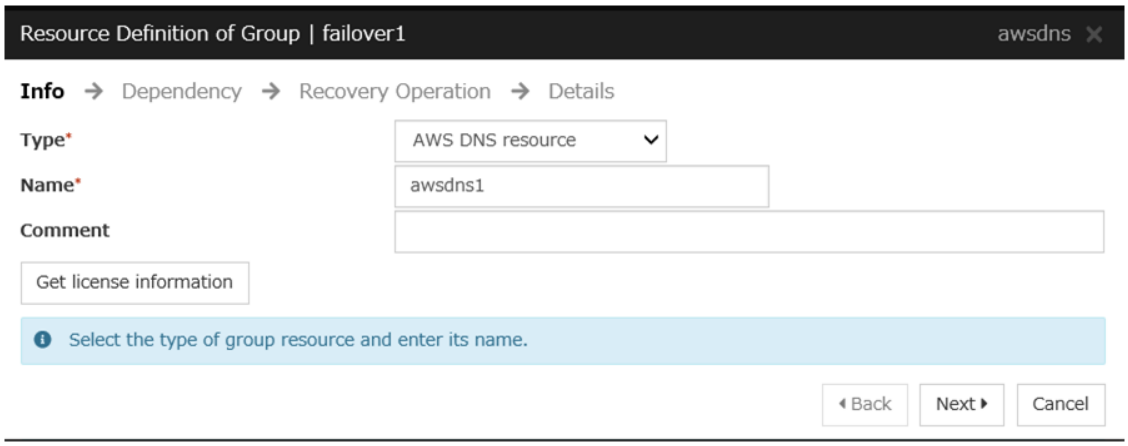
  Add the AWS DNS resource that controls the DNS name by using the AWS CLI.

  For details, refer to the following:

  - Reference Guide
    -> Understanding AWS DNS resources

  Steps

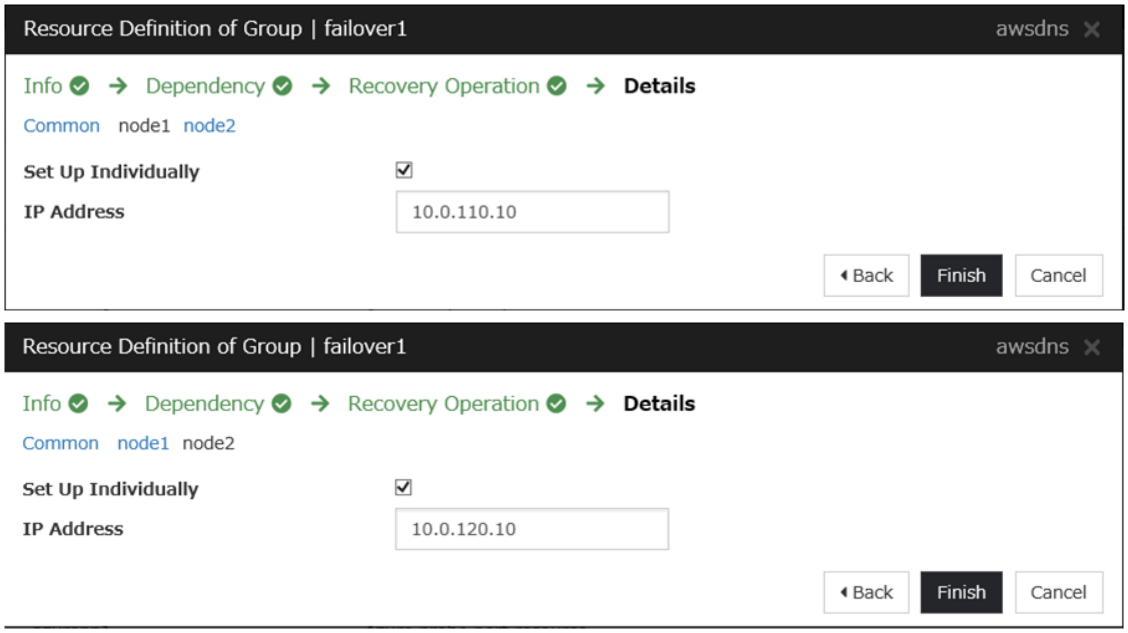
  1. Click **Add** in **Group Resource List**.
  2. The **Resource Definition of Group | failover1** window is displayed. Select the group resource type (AWS DNS resource) from the **Type** box and enter the group resource name (awsdns1) in the **Name** box.



3. The **Dependency** window is displayed. Click **Next** without specifying anything.
4. The **Recovery Operation** window is displayed. Click **Next**.
5. The **Details** window is displayed.
   Set the hosted zone ID in the **Hosted Zone ID** box on the **Common** tab (corresponds to [7] in Figure 7.1 System Configuration HA Cluster Based on DNS Name Control).
   Set a DNS name to be assigned in the **Resource Record Set Name** box (corresponds to [6] in Figure 7.1 System Configuration HA Cluster Based on DNS Name Control).
   Set the DNS name as FQDN, adding dot (.) at the end of the name.
   Set the IP address corresponding to the DNS name in the **IP Address** box (corresponds to [4] in Figure 7.1 System Configuration HA Cluster Based on DNS Name Control).
   Enter the IP address of one server on the **Common** tab and specify the IP address of the other server separately.
   Since this guide uses the configuration in which the IP address of each server is included in the resource record set, the procedure is as described above. However, if VIP and EIP are included in the resource record set, enter the IP address on the **Common** tab. No individual setting is required.
   Set the time to live (TTL) of the cache in the **TTL** box.

   The time is specified in seconds.
   Set the **Delete a resource record set at deactivation** checkbox to on.
   If the resource record set is not deleted from the hosted zone when AWS DNS resource is deactivated, uncheck the checkbox.
   If it is not deleted, a client may access the remaining DNS name.

6. Specify the node settings on each node tab.
   Select the **Set Up Individually** check box.
   Enter the IP address of the instance corresponding to the node in the **IP Address** box (corresponds to [4] and [6] in Figure 7.1 System Configuration HA Cluster Based on DNS Name Control).
   Since this guide uses the configuration in which the IP address of each server is included in the resource record set, the procedure is as described above. However, if VIP and EIP are included in the resource record set, this procedure is not needed.



7. Click **Finish** to complete setting.

3) **Add a monitor resource.**

- AWS AZ monitor resource

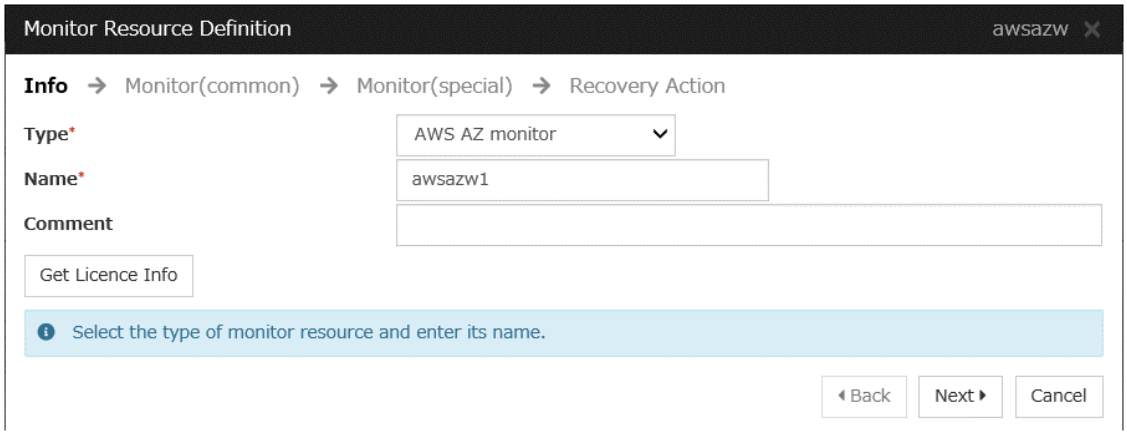
Create an AWS AZ monitor resource to check whether the specified AZ is usable by using the monitor command.

For details, refer to the following:

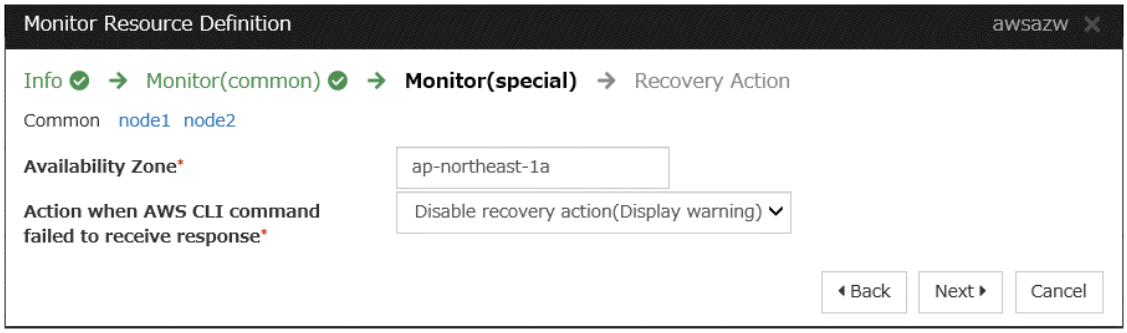
Reference Guide
-> Understanding AWS AZ monitor resources

Steps

1. Click **Add** in **Monitor Resource List**.
2. Select the monitor resource type (AWS AZ monitor) from the **Type** box and enter the monitor resource name (awsazw1) in the **Name** box. Click **Next**.

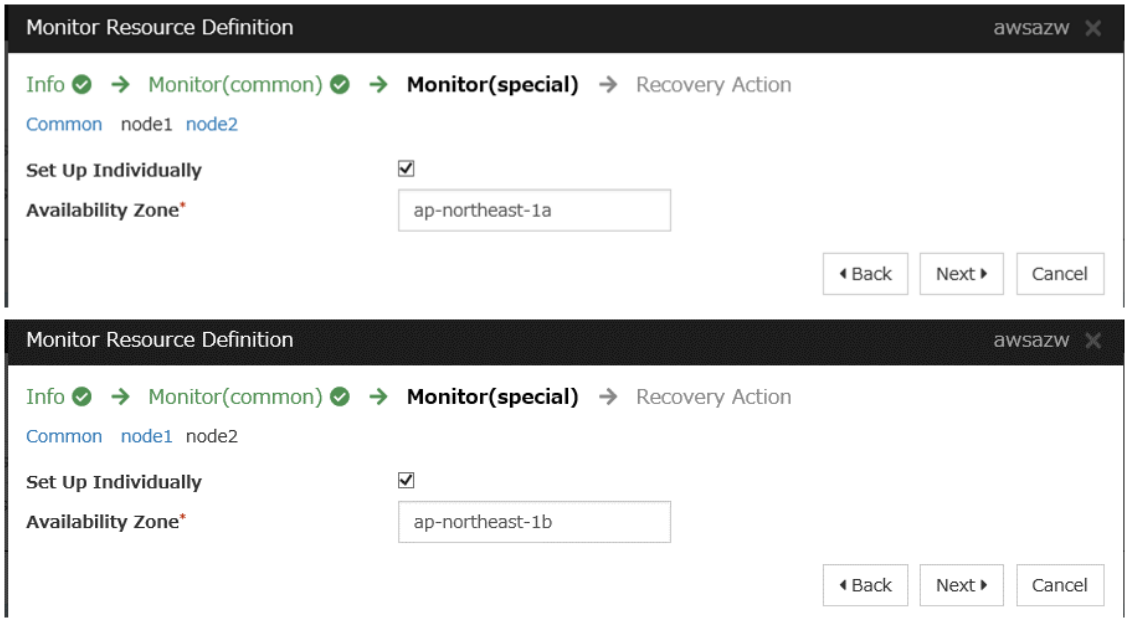


3. The **Monitor (common)** window is displayed.
   Click **Next** without specifying anything.
4. The **Monitor (special)** window is displayed.
   Enter the AZ to be monitored in the **Availability Zone** box on the **Common** tab. (Specify the AZ of the active server instance.) (corresponds to [2] in Figure 7.1 System Configuration HA Cluster Based on DNS Name Control)

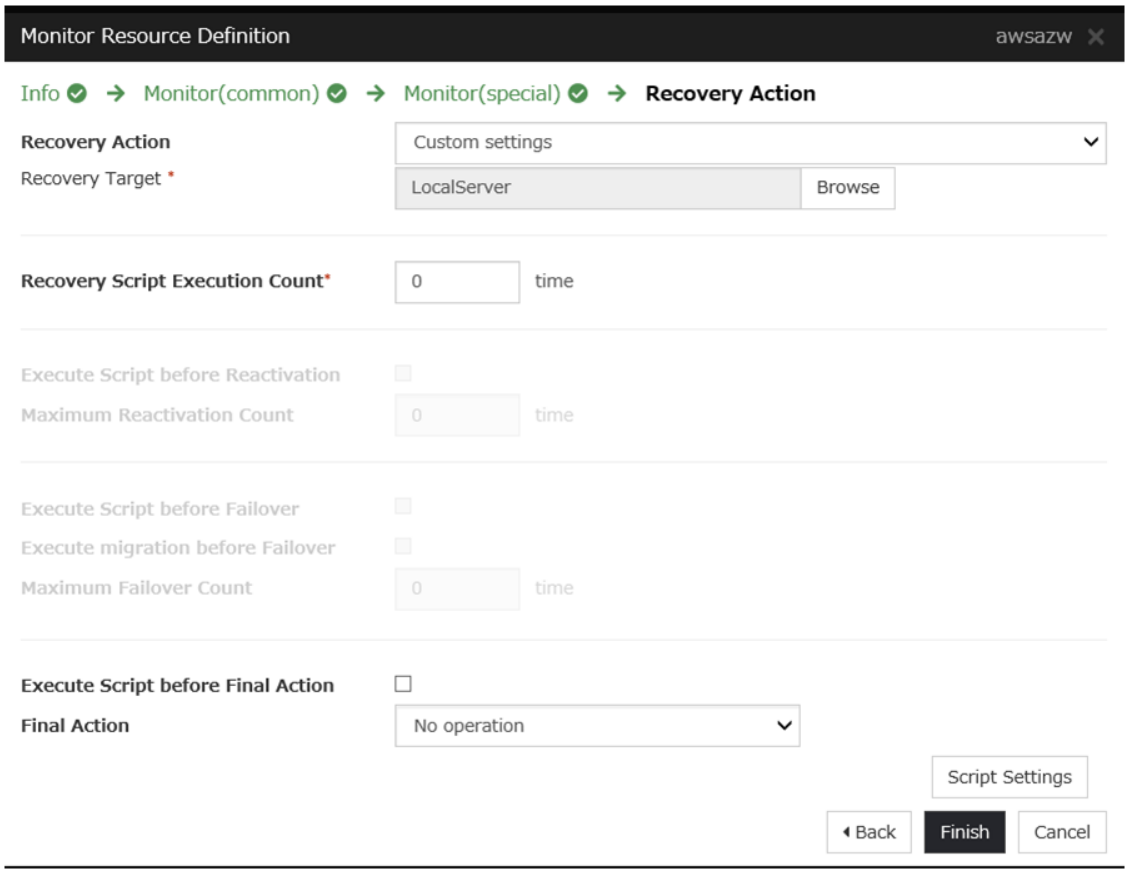


5. Specify the node settings on each node tab.

Select the **Set Up Individually** check box.
Enter the AZ of the instance corresponding to the node in the **Availability Zone** box (corresponds to [2] and [3] in Figure 7.1 System Configuration HA Cluster Based on DNS Name Control). Click **Next**.



6. The **Recovery Action** window is displayed.
   Set LocalServer in the **Recovery Target** box.



7. Click **Finish** to complete setting.

- AWS DNS monitor resource

  This resource is automatically added when the AWS DNS resource is added.

  Using AWS CLI commands, check whether the resource record set exists and the registered IP address can be obtained by resolving the DNS name.

  For details, refer to the following:

  Reference Guide
  -> Understanding AWS DNS monitor resources

4) **Apply the settings and start the cluster.**

1. Click **Apply the Configuration File** on the **File** in the config mode of Cluster WebUI.
   If the upload succeeds, the message saying "The application finished successfully."
2. Select the **Operation Mode** on the drop down menu of the toolbar in Cluster WebUI to switch to the operation mode.
3. The procedure depends on the resource used. For details, refer to the following: Installation and Configuration Guide -> How to create a cluster

CHAPTER

EIGHT

TROUBLESHOOTING

This chapter describes the points to be checked and solutions if EXPRESSCLUSTER cannot be set up in the AWS environment.

- Failed to start a resource or monitor resource related to AWS.

  Confirm that the OS has restarted, the AWS CLI are installed, and the AWS CLI has been set up correctly.

  If the OS has been restarted when installing EXPRESSCLUSTER, the environment variable settings might be changed by installing the AWS CLI. In this case, restart the OS again.

- Failed to start the AWS Virtual IP resource.

  Cluster WebUI message

  ```
  Activating awsvip1 resource has failed.(51 : The AWS CLI command is not found.
  ↪)
  ```

  Possible cause Any of the following might be the cause.

  – The AWS CLI has not been installed, or the path does not reach AWS CLI.

  Solution

  – Confirm that the AWS CLI is installed.

  – The installation path of the AWS CLI must be any of the following:
  `/sbin, /bin, /usr/sbin, /usr/bin, /usr/local/bin`

Cluster WebUI message

```
Activating awsvip1 resource has failed.(50 : Failed in the AWS CLI␣
↪command.)
```

Possible cause Any of the following might be the cause.

- The AWS CLI has not been set up. (aws configure has not been run.)
- The AWS CLI configuration file could not be found. (A user other than root ran aws configure, or A user without sudo ran aws configure.)
  Search for a credentials file and a config file by the following order (in case of policy for which the IAM user is used).

  1) $HOME/.aws follower
  2) /root/.aws follower

- The specified AWS CLI settings (such as a region, access key ID, and secret key) are not correct.

- (For an operation using an IAM role) An IAM role has not been set to the instance.
  Access the URL below from the corresponding instance and then check whether the given IAM role name is displayed. If the message "404 Not Found" appears, no IAM role has been set.
  http://169.254.169.254/latest/meta-data/iam/security-credentials/
- The specified VPC ID or ENI ID is invalid.
- The regional endpoint has been stopped due to maintenance or failure.
- An issue of the communication path to the regional endpoint.
- Delay caused by the heavily loaded node.

Solution Check the following:

- Correct the AWS CLI settings. Then confirm that the AWS CLI works successfully.
- When the node is heavily loaded, remove the causes.
- For an operation using an IAM role, check the settings on the AWS Management Console.

Cluster WebUI message

```
Activating awsvip1 resource has failed.(50 : The vpc ID 'vpc-xxxxxxxx'␣
↪does not exist)
```

Possible cause The specified VPC ID might not be correct or might not exist.

Solution Specify a correct VPC ID.

Cluster WebUI message

```
Activating awsvip1 resource has failed.(50 : The networkInterface ID
↪'eni-xxxxxxxx' does not exist)
```

Possible cause The specified ENI ID might not be correct or might not exist.

Solution Specify a correct ENI ID.

Cluster WebUI message

```
Activating awsvip1 resource has failed.(50 : You are not authorized to␣
↪perform this operation.)
```

Possible cause If the ReplaceRoute right of an IAM role can be exercised only on a route table specified in a resource in the IAM policy, the route table might have an error or lack of its settings.

Solution

Of all route tables under a specified VPC, an AWS virtual IP resource updates only ones that include specified virtual IP address entries.
For all such route tables to be updated, give permission to the resource in the IAM policy.

Cluster WebUI message

```
Activating awsvip1 resource has failed.(1 : Command was not completed␣
↪within %1 seconds.)
```

Possible cause Any of the following might be the cause:

- The AWS CLI command might not be able to communicate with the regional endpoint, due to a misconfiguration of the route table, NAT, or proxy server.
- Delay caused by the heavily loaded node.

Solution Check the following:

- The routing for the NAT gateway has been set up.
- The packet is not excluded by filtering.
- Check the settings of the route table, NAT, or proxy server.
- When the node is heavily loaded, remove the causes.

Cluster WebUI message

```
Activating awsvip1 resource has failed.(53 : The VIP address vvv.www.xxx.
↪yyy belongs to a VPC subnet.)
```

Possible cause The specified VIP address is not appropriate because it is within of the VPC CIDR range.

Solution Specify an IP address out of the VPC CIDR range as the VIP address.

- The AWS Virtual IP resource is running normally, but ping cannot reach the VIP address.

  Cluster WebUI message

  ```
  -
  ```

  Possible cause Source/Dest. Check of the ENI set to the AWS Virtual IP resource is enabled.

  Solution Disable Source/Dest. Check of the ENI set to the AWS Virtual IP resource.

- The AWS Virtual IP monitor resource enters the error state.

  Cluster WebUI message

  ```
  Detected an error in monitoring awsvipw1. (56 : The routing for VIP vvv.www.
  ↪xxx.yyy was changed.)
  ```

  Possible cause In the route table, the target of the VIP address corresponding to the AWS Virtual IP resource has been changed to another ENI ID for some reason.

  Solution

  When an error is detected, the AWS Virtual IP resource is restarted automatically and the target is updated to a correct ENI ID.

  Check whether another HA cluster uses the same VIP address mistakenly and so on.

- Failed to start the AWS Elastic IP resource.

  Cluster WebUI message

```
Activating awseip1 resource has failed.(51 : The AWS CLI commandis not found.)
```

  Possible cause The AWS CLI has not been installed, or the path does not reach AWS CLI.

  Solution Check the following:

  - Confirm that the AWS CLI is installed.
  - The installation path of the AWS CLI must be any of the following:
    `/sbin, /bin, /usr/sbin, /usr/bin, /usr/local/bin`

Cluster WebUI message

```
Activating awseip1 resource has failed.(50 : Failed in the AWS CLI␣
↪command.)
```

Possible cause Any of the following might be the cause:

- The AWS CLI has not been set up. (aws configure has not been run.)
- The AWS CLI configuration file could not be found. (A user other than root ran aws configure, or A user without sudo ran aws configure.)
  Search for a credentials file and a config file by the following order (in case of policy for which the IAM user is used):

  1) $HOME/.aws follower
  2) /root/.aws follower

- The specified AWS CLI settings (such as a region, access key ID, and secret key) are not correct.
- (For an operation using an IAM role) An IAM role has not been set to the instance.
  Access the URL below from the corresponding instance and then check whether the given IAM role name is displayed. If the message "404 Not Found" appears, no IAM role has been set.
  http://169.254.169.254/latest/meta-data/iam/security-credentials/
- The specified EIP Allocation ID or ENI ID is invalid.
- The regional endpoint has been stopped due to maintenance or failure.
- An issue of the communication path to the regional endpoint.
- Delay caused by the heavily loaded node.

Solution Check the following:

- Correct the AWS CLI settings. Then confirm that the AWS CLI works successfully.
- When the node is heavily loaded, remove the causes.
- For an operation using an IAM role, check the settings on the AWS Management Console.

Cluster WebUI message

```
Activating awseip1 resource has failed.(50 : The allocation ID 'eipalloc-
↪xxxxxxxx' does not exist)
```

Possible cause The specified EIP Allocation ID might not be correct or might not exist.

Solution Specify a correct EIP Allocation ID.

Cluster WebUI message

```
Activating awseip1 resource has failed.(50 : The networkInterface ID
↪'eni-xxxxxxxx' does not exist)
```

Possible cause The specified ENI ID might not be correct or might not exist.

Solution Specify a correct ENI ID.

Cluster WebUI message

```
Activating awseip1 resource has failed.(53 : Timeout occurred.)
```

Possible cause Any of the following might be the cause:

- The AWS CLI command might not be able to communicate with the regional endpoint, due to a misconfiguration of the route table, NAT, or proxy server.
- Delay caused by the heavily loaded node.

Solution Check the following:

- Confirm that a public IP is assigned to each instance.
- Confirm that the AWS CLI works normally in each instance.
- Check the settings of the route table, NAT, or proxy server.
- When the node is heavily loaded, remove the causes.

- The AWS Elastic IP monitor resource enters the error state.

Cluster WebUI message

```
Detected an error in monitoring awseipw1. (52 : The EIP address does not␣
↪exist. (EIP ALLOCATION ID=eipalloc-xxxxxxxx))
```

Possible cause The specified ENI ID and elastic IP have been deassociated for some reason.

Solution

When an error is detected, the AWS Elastic IP resource is restarted automatically and the specified ENI ID and elastic IP are associated.
Check whether another HA cluster uses the same EIP allocation ID mistakenly and so on.

- Fails to start the AWS DNS resource.

Cluster WebUI message

```
Activating awsdns1 resource has failed.(52 : The AWS CLI command is not found.
↪)
```

Possible cause The AWS CLI has not been installed, or the path does not reach AWS CLI.

Solution Check the following:

- Confirm that the AWS CLI is installed.
- The installation path of the AWS CLI must be any of the following:
  `/sbin, /bin, /usr/sbin, /usr/bin, /usr/local/bin`

Cluster WebUI message

```
Activating awsdns1 resource has failed. (50 : The AWS CLI command failed.
↪)
```

Possible cause Any of the following might be the cause:

- The AWS CLI has not been set up (aws configure has not been started).
- The AWS CLI configuration could not be found (e.g. aws configuration was done by a user other than root, executed without sudo etc.)
  When an IAM user is to be used, search for a credentials or config file by the following step:
  1) Under <$HOME/.aws>
  2) Under </root/.aws>
- Incorrect values are set in AWS CLI configuration (e.g. region, accesskey, secret key etc.).
- An IAM role has not been set to the instance (for an operation using an IAM role)
  Access the URL below from the corresponding instance and then check whether the given IAM role name is displayed. If the message "404 Not Found" appears, no IAM role has been set.
  http://169.254.169.254/latest/meta-data/iam/security-credentials/
- The specified resource record set is invalid.
- The regional endpoint has been stopped due to maintenance or failure.
- An issue of the communication path to the regional endpoint.
- Delay caused by the heavily loaded node.
- Route 53 cannot be accessed or does not respond.
- No VPC to which the HA instance belongs is added to a VPC targeted in the hosted zone of Route 53.
- DNS name resolution is not enabled in the VPC to which the HA instance belongs.
- The value of **Resource Record Set Name** is specified in capital letters.
- On the terminal of the node (instance), manually execute the following command:

  ```
  # aws route53 list-resource-record-sets --hosted-zone-id
  ↪<hosted-zone ID>
  ```

  If the error message "Could not connect to the endpoint URL" appears, the possible cause is either of the following:

- If you are using a VPC endpoint, which does not support the Route 53 service, AWS DNS resources/monitor resources are unavailable.
- If you are not using a VPC endpoint, there may be some issue of the AWS configuration.

Solution Check the following:

- Correct the AWS CLI settings. Then confirm that the AWS CLI works successfully.
- When the node is heavily loaded, remove the causes.
- In applicable Hosted Zone of the Route 53 Management Console, check that the necessary VPC is added to **Associated VPC**.
- On the VPC Management Console, check that **enableDnsSupport** is enabled in the properties of the current VPC. If **enableDnsSupport** is intentionally disabled, set an appropriate DNS resolver for the record set added in the AWS DNS resource by the instance.
- Specify the value of **Resource Record Set Name** in lowercase letters.
- If you are using a VPC endpoint, consider changing to any of the following methods: a NAT gateway, or proxy server. If you are not using a VPC endpoint, consult AWS.
- For an operation using an IAM role, check the settings on the AWS Management Console.

Cluster WebUI message

```
Activating awsdns1 resource has failed. (50 : No hosted zone found with␣
↪ID: %1)
```

Possible cause Specified Host Zone ID may not be correct or exist.

Solution Specify the correct Host Zone ID.

Cluster WebUI message

```
Activating awsdns1 resource has failed. (51: Timeout occurred.)
```

Possible cause Any of the following might be the cause:

- The AWS CLI command might not be able to communicate with the regional endpoint, due to a misconfiguration of the route table, NAT, or proxy server.
- Delay caused by the heavily loaded node.
- Delayed processing on the Route 53 endpoint side.
- Delayed access to the instance metadata by the AWS CLI.

Solution Check the following:

- If the routing for the NAT gateway has been configured properly.
- If the packets are not blocked by filtering.
- Check the settings of the route table, NAT, or proxy server.
- When the node is heavily loaded, remove the causes.

- The value of **Timeout** for **Monitor (common)** in the AWS environment is set at or larger than that of the time required for running the AWS CLI. Measure the required time by manually executing the AWS CLI. The AWS DNS monitor resource runs the following AWS CLI:

  ```
  # aws route53 list-resource-record-sets
  ```

- For an operation using an IAM role: When running the AWS CLI, the AWS DNS resource and monitor resource of EXPRESSCLUSTER acquires credentials (such as an access key ID) from the instance metadata.

  Check if access to the instance metadata is not delayed, by manually determining the time required for executing the commands below.

  If running either of the commands is delayed, the access to the instance metadata is delayed.

  If the delay is confirmed, allow an IAM user to access the instance metadata--by running the aws configure command to add the settings of the access key ID and secret access key to each of the cluster nodes. This may reduce the occurrence of timeouts.

  - On each of the cluster nodes, run the curl command or use a browser to access the URL: http://169.254.169.254/latest/meta-data/

  - On any of the cluster nodes, run the command: aws configure list

---

- Despite the normal operation of the AWS DNS resource, it takes time to resolve names on clients.

  Cluster WebUI message

  –

  Possible cause Any of the following might be the cause:

  – Due to the specification of Route 53, it takes up to 60 seconds to propagate its settings to all the authoritative servers. Refer to the following:

    https://aws.amazon.com/route53/faqs/?nc1=h_ls

    Amazon Route 53 FAQs

    Q. How quickly will changes I make to my DNS settings on Amazon Route 53 propagate globally?

  – The OS-side resolver takes time.

  – During a failover, the AWS DNS resource takes time to delete and create resource record sets.

    If the **Delete a resource record set at deactivation** checkbox is checked: A resource record set deleted on a failover source with the AWS DNS resource deactivated is created on a failover destination with the AWS DNS resource activated. This may delay name resolution.

    If the checkbox is not checked: No resource record set is deleted even with the AWS DNS resource deactivated or with the cluster stopped, and only the IP address of the corresponding resource record set is updated. This may shorten the time before names can be resolved. Even after the AWS DNS resource is deactivated or the cluster is stopped, names are resolved.

  – A large value of **TTL** for the AWS DNS resource.

  – A small value of **Start Monitor Wait Time** for the AWS DNS monitor resource.

    If a name resolution is tried prior to the completion of Route 53 change propagation, the DNS returns NXDOMAIN (non-existing domain). In this case, the name resolution fails until the valid period of the negative cache expires.

    Therefore, with **Start Monitor Wait Time** set at a small value, a name resolution may take a long time.

  Solution Check the following:

- Review the settings of the OS-side resolver.
- Uncheck the **Delete a resource record set at deactivation** checkbox of the AWS DNS resource.
- Set **TTL** at a smaller value for the AWS DNS resource.
- Set **Start Monitor Wait Time** at an allowable large value for the AWS DNS monitor resource.

- The AWS DNS monitor resource enters the error state.

  Cluster WebUI message

```
Detected an error in monitoring awsdnsw1. (52 : The resource record set in␣
↪Amazon Route 53 does not exist.)
```

  Possible cause Any of the following might be the cause:

  - In the Host Zone, the resource record set corresponding to the AWS DNS resource has been deleted for some reason.
  - Immediately after the AWS DNS resource is activated, if the AWS DNS monitor resource starts monitoring prior to the propagation of changed DNS settings in Route 53, the monitoring fails due to inability in resolving names. Refer to the following:

    - Getting Started Guide
      -> Notes and Restrictions
      -> Setting up AWS DNS monitor resources

  - Of the IAM policy, the following is not set: route53:ChangeResourceRecordSets and route53:ListResourceRecordSets.
  - No VPC to which the HA instance belongs is added to a VPC targeted in the hosted zone of Route 53.
  - The DNS name specified in the **Resource Record Set Name** does not have a dot (.) at the end.

  Solution Check the following:

  - No other HA clusters use the same resource record set by mistake. (If used, that is a cause of the deleted resource record set.)
  - The value of **Start Monitor Wait Time** of the AWS DNS monitor resource is set larger than that of the time to propagate changed DNS settings in Route 53.
  - The following is set in the IAM policy: route53:ChangeResourceRecordSets and route53:ListResourceRecordSets.
  - In applicable Hosted Zone of the Route 53 Management Console, the necessary VPC is added to **Associated VPC**.
  - The DNS name specified in the **Resource Record Set Name** is an FQDN, and has a dot (.) at the end.

Cluster WebUI message

```
Detected an error in monitoring awsdnsw1. (53: IP address different from␣
↪the setting is registered in the resource record set of Amazon Route␣
↪53.)
```

Possible cause In the Host Zone, the IP address of resource record set corresponding to the AWS DNS resource has been changed for some reason.

Solution Resource record set may have been deleted when another HA cluster uses the same resource record set by mistake.

Cluster WebUI message

```
Detected an error in monitoring awsdnsw1. (54 : Failed to resolve domain␣
↪name.)
```

Possible cause The name resolution using the DNS name registered in the hosted zone as resource record set failed.

Solution Check the following:

- If the resolver settings are correct.
- If the network settings are correct.
- If the domain query is set to refer to Amazon Route 53 name server (NS) based on the NS record setting of registrar when Public Host Zone is used.

Cluster WebUI message

```
Detected an error in monitoring awsdnsw1. (55 : IP address which is␣
↪resolved domain name from the DNS resolver is defferent from the␣
↪setting.)
```

Possible cause The IP address obtained by name resolution check with the DNS name registered in the Hosted Zone as the resource record set is not correct.

Solution Check the following:

- If the resolver setting is correct.
- If there are no entries related to the DNS name in the hosts file.

- The AWS DNS monitor resource enters the warning or error state.

Cluster WebUI message

[Warning]

```
Warn monitoring awsdnsw1. (151 : Timeout occurred.)
```

[Error]

```
Detected an error in monitoring awsdnsw1. (51 : Timeout occurred.)
```

Possible cause Any of the following might be the cause:

– The AWS CLI command might not be able to communicate with the regional endpoint, due to a misconfiguration of the route table, NAT, or proxy server.

- Delay caused by the heavily loaded node.
- Delayed processing on the Route 53 endpoint side.
- Delayed access to the instance metadata by the AWS CLI.

Solution Check the following:

- If the routing for the NAT gateway has been configured properly.
- If the packets are not blocked by filtering.
- Check the settings of the route table, NAT, or proxy server.
- The value of **Timeout** for **Monitor (common)** in the AWS environment is set at or larger than that of the time required for running the AWS CLI. Measure the required time by manually executing the AWS CLI. The AWS DNS monitor resource runs the following AWS CLI:

  ```
  # aws route53 list-resource-record-sets
  ```

- For an operation using an IAM role: When running the AWS CLI, the AWS DNS resource and monitor resource of EXPRESSCLUSTER acquires credentials (such as an access key ID) from the instance metadata.
  Check if access to the instance metadata is not delayed, by manually determining the time required for executing the commands below.
  If running either of the commands is delayed, the access to the instance metadata is delayed.
  If the delay is confirmed, allow an IAM user to access the instance metadata--by running the aws configure command to add the settings of the access key ID and secret access key to each of the cluster nodes. This may reduce the occurrence of timeouts.
  - On each of the cluster nodes, run the curl command or use a browser to access the URL: http://169.254.169.254/latest/meta-data/
  - On any of the cluster nodes, run the command: aws configure list

---

- The AWS AZ monitor resource enters the warning or error state.

  Cluster WebUI message

  [Warning]

  ```
  Warn monitoring awsazw1. (105 : Failed in the AWS CLI command.)
  ```

  [Error]

  ```
  Detected an error in monitoring awsazw1. (5 : Failed in the AWS CLI␣
  ↪command.)
  ```

  Possible cause Any of the following might be the cause:

  - The AWS CLI has not been set up. (aws configure has not been run.)
  - The AWS CLI configuration file could not be found. (A user other than root ran aws configure, or A user without sudo ran aws configure.)
    Search for a credentials file and a config file by the following order (in case of policy for which the IAM user is used).
    1) $HOME/.aws follower
    2) /root/.aws follower
  - The specified AWS CLI settings (such as a region, access key ID, and secret key) are not correct.
  - (For an operation using an IAM role) An IAM role has not been set to the instance.

Access the URL below from the corresponding instance and then check whether the given IAM role name is displayed. If the message "404 Not Found" appears, no IAM role has been set.
http://169.254.169.254/latest/meta-data/iam/security-credentials/

- The specified AZ is invalid.
- The regional endpoint has been stopped due to maintenance or failure.
- An issue of the communication path to the regional endpoint.
- Delay caused by the heavily loaded node.

Solution Check the following:

- Correct the AWS CLI settings. Then confirm that the AWS CLI works successfully.
- When the node is heavily loaded, remove the causes.
- If the warning frequently appears, it is recommended to change to **Disable recovery action (Display warning)**. Even if you do it, it is possible to detect errors except those caused by delayed response and by failure in running the AWS CLI on the monitor resource.
- For an operation using an IAM role, check the settings on the AWS Management Console.

Cluster WebUI message

[Warning]

```
Warn monitoring awsazw1. (105 : Invalid availability zone: [ap-
↪northeast-1x])
```

[Error]

```
Detected an error in monitoring awsazw1. (5 : Invalid availability␣
↪zone: [ap-northeast-1x])
```

Possible cause The specified AZ might not be correct or might not exist.

Solution Specify a correct AZ.

Cluster WebUI message

[Warning]

```
Warn monitoring awsazw1. (106 : Timeout occurred.)
```

[Error]

```
Detected an error in monitoring awsazw1. (6 : Timeout occurred.)
```

Possible cause Any of the following might be the cause:

- The AWS CLI command might not be able to communicate with the regional endpoint, due to a misconfiguration of the route table, NAT, or proxy server.
- Delay caused by the heavily loaded node.

Solution Check the following:

- The routing for the NAT gateway has been set up.

- The packet is not excluded by filtering.
- Check the settings of the route table, NAT, or proxy server.
- The value of **Timeout** for **Monitor (common)** in the AWS environment is set at or larger than that of the time required for running the AWS CLI. Measure the required time by manually executing the AWS CLI. The AWS AZ monitor resource runs the following AWS CLI:

  ```
  # aws ec2 describe-availability-zones
  ```

- If When the node is heavily loaded, remove the causes.

CHAPTER

NINE

LEGAL NOTICE

9.1 Disclaimer

- Information in this document is subject to change without notice.
- NEC Corporation is not liable for technical or editorial mistakes in or omissions from this document.
  In addition, whether the customer achieves the desired effectiveness by following the introduction and usage instructions in this document is the responsibility of the customer.
- No part of this document may be reproduced or transmitted in any form by any means, electronic or mechanical, for any purpose, without the express written permission of NEC Corporation.

9.2 Trademark Information

- EXPRESSCLUSTER X is a registered trademark of NEC Corporation.
- Linux is a registered trademark of Linus Torvalds in the United States and other countries.
- Python is a registered trademark of the Python Software Foundation.
- Amazon Web Services and all AWS-related trademarks, as well as other AWS graphics, logos, page headers, button icons, scripts, and service names are trademarks, registered trademarks or trade dress of AWS in the United States and/or other countries.
- Other product names and slogans written in this manual are trademarks or registered trademarks of their respective companies.

CHAPTER

TEN

REVISION HISTORY

Edition	Revised Date	Description
1st	Apr 15, 2024	New Guide
2nd	Nov 29, 2024	Corrected typographical errors and other mistakes.