

EXPRESSCLUSTER® X 4.1

HA Cluster Configuration Guide for Amazon Web Services (Linux)

April 10, 2019
1st Edition



Revision History

Edition	Revised Date	Description
1st	Apr 10, 2019	New Guide

© Copyright NEC Corporation 2019. All rights reserved.

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.

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.

Table of Contents

Preface	v
Chapter 1 Overview	9
1-1. Functional overview	9
1-2. HA cluster configuration	10
1-3. Multi-AZ	17
1-4. Network partition resolution	18
1-5. On-premises and AWS	19
Chapter 2 Operating Environment	22
Chapter 3 Notes	23
Chapter 4 Constructing an HA cluster based on VIP control	25
4-1. Configuring the VPC Environment	26
4-2. Configuring the instance	29
4-3. Setting up EXPRESSCLUSTER	31
Chapter 5 Constructing an HA cluster based on EIP control	41
5-1. Configuring the VPC Environment	42
5-2. Configuring the instance	44
5-3. Setting up EXPRESSCLUSTER	46
Chapter 6 Constructing an HA cluster based on DNS name control	54
6-1. Configuring the VPC Environment	55
6-2. Configuring the instance	58
6-3. Setting up EXPRESSCLUSTER	60
Chapter 7 Configuring the IAM	71
7-1. Creating an IAM policy	72
7-2. Configuring the instance	73
Chapter 8 Troubleshooting	76

Preface

Who Should Use This Guide

The "*EXPRESSCLUSTER® X 4.1 HA Cluster Configuration Guide for Amazon Web Services (Linux)*" is intended for administrators who set up cluster systems, system engineers who provide user support for such systems, and cluster-system maintenance personnel. They must also have knowledge of Amazon EC2, Amazon VPC, and IAM provided by Amazon Web Services.

Scope of Application

This guide covers the following product versions.

- EXPRESSCLUSTER X 4.1 for Linux (Internal version: 4.1.0-1)
- VPC Management console, EC2 Management Console: Environment as of January 07, 2019

How This Guide is Organized

Chapter 1	Overview: Describes the functional overview.
Chapter 2	Operating Environment: Describes the tested operating environment of this function.
Chapter 3	Notes: Describes the notes on constructing a cluster.
Chapter 4	Constructing an HA cluster based on VIP control: Describes how to create an HA cluster based on VIP control.
Chapter 5	Constructing an HA cluster based on EIP control: Describes how to create an HA cluster based on EIP control.
Chapter 6	Constructing an HA cluster based on DNS name control: Describes how to create an HA cluster based on DNS name control.
Chapter 7	Configuring the IAM: Describes how to configure the IAM.
Chapter 8	Troubleshooting: Describes the problems and their solutions.

EXPRESSCLUSTER X Documentation Set

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

Getting Started Guide

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

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.

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*.

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.

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*.

Legacy Feature Guide

This guide is intended for administrators and for system engineers who want to build EXPRESSCLUSTER-based cluster systems. The guide describes EXPRESSCLUSTER X 4.0 WebManager and Builder.

Conventions

In this guide, **Note**, **Important**, **Related Information** 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.

Related Information:

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.	<code>clpstat -s[-h <i>host_name</i>]</code>
#	Prompt to indicate that a Linux user has logged on as root user.	<code># clpstat</code>
Monospace (Courier)	Indicates path names, commands, system output (message, prompt, etc.), directory, file names, functions and parameters.	<code>/Linux</code>
Monospace bold (Courier)	Indicates the value that a user actually enters from a command line.	Enter the following: <code># clpcl -s -a</code>
<i>Monospace italic</i> (Courier)	Indicates that users should replace italicized part with values that they are actually working with.	<code># ping <IP address></code>

Contacting NEC

For the latest product information, visit our website below:

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

Chapter 1 Overview

1-1. 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).

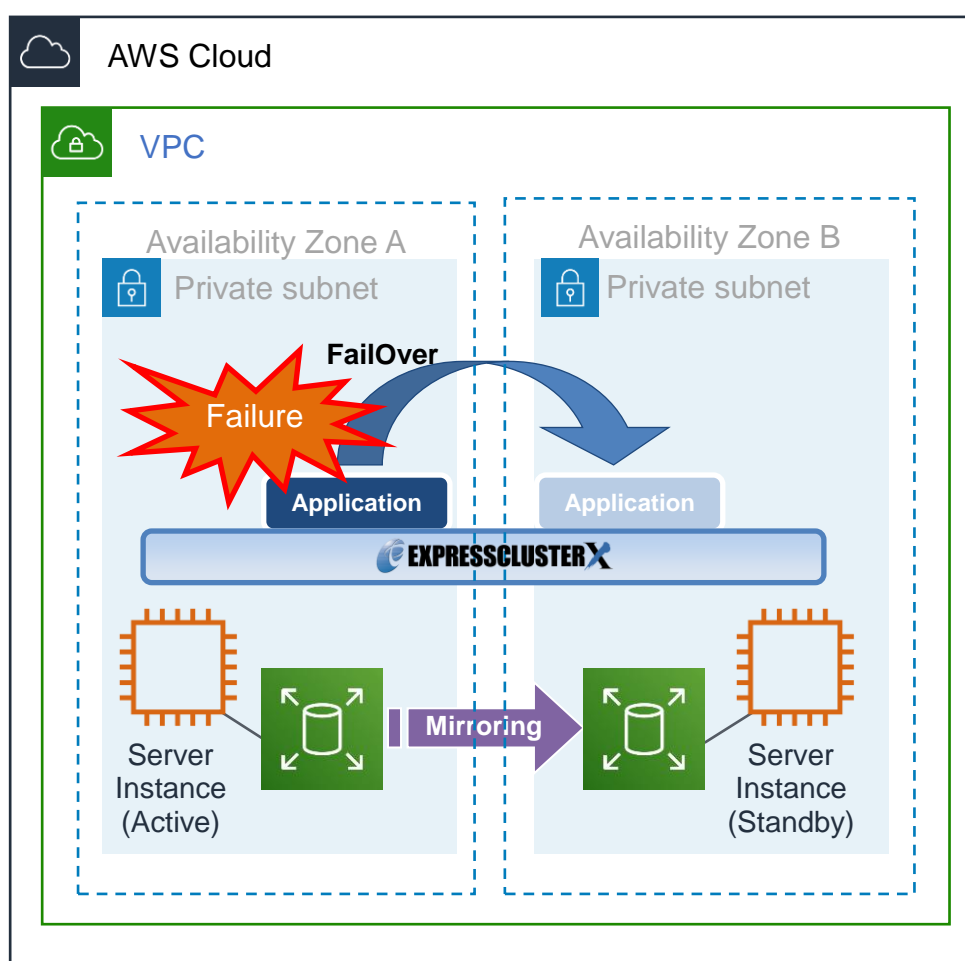


Figure 1-1 Mirror Type HA Cluster in Multi-AZ Configuration

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.

1-2. HA cluster configuration

This guide describes two 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 "1-3 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

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.

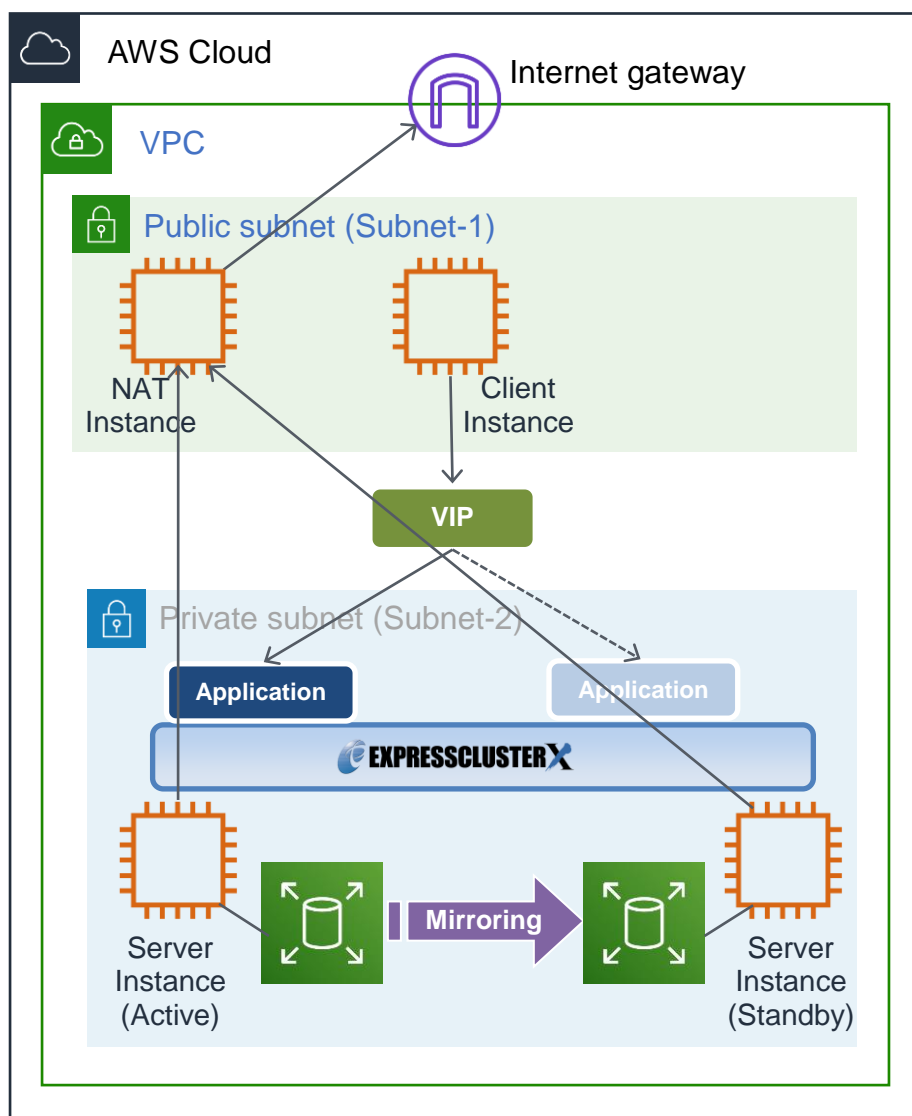


Figure 1-2 HA Cluster Based on VIP Control

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.

NEC has verified that the AWS specifications do not allow clients outside the VPC to access the server instance via the VIP address assigned by the AWS Virtual IP resource. Therefore, to enable clients outside the VPC to access, specify the EIP address assigned by the AWS Elastic IP resource.

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

* When executing the AWS CLI, each instance must be able to communicate with the regional endpoint by -. In this guide, instance for NAT is used for the HA cluster based on VIP control.

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 sever 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
IP monitor resource	Monitors the health of communication between subnets by checking whether communication with a NAT is available.	Required to check the health of communication between subnets.
Other resources and monitor resources	Depends on the configuration of the application, such as a mirror disk, used in an HA cluster.	Optional

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.

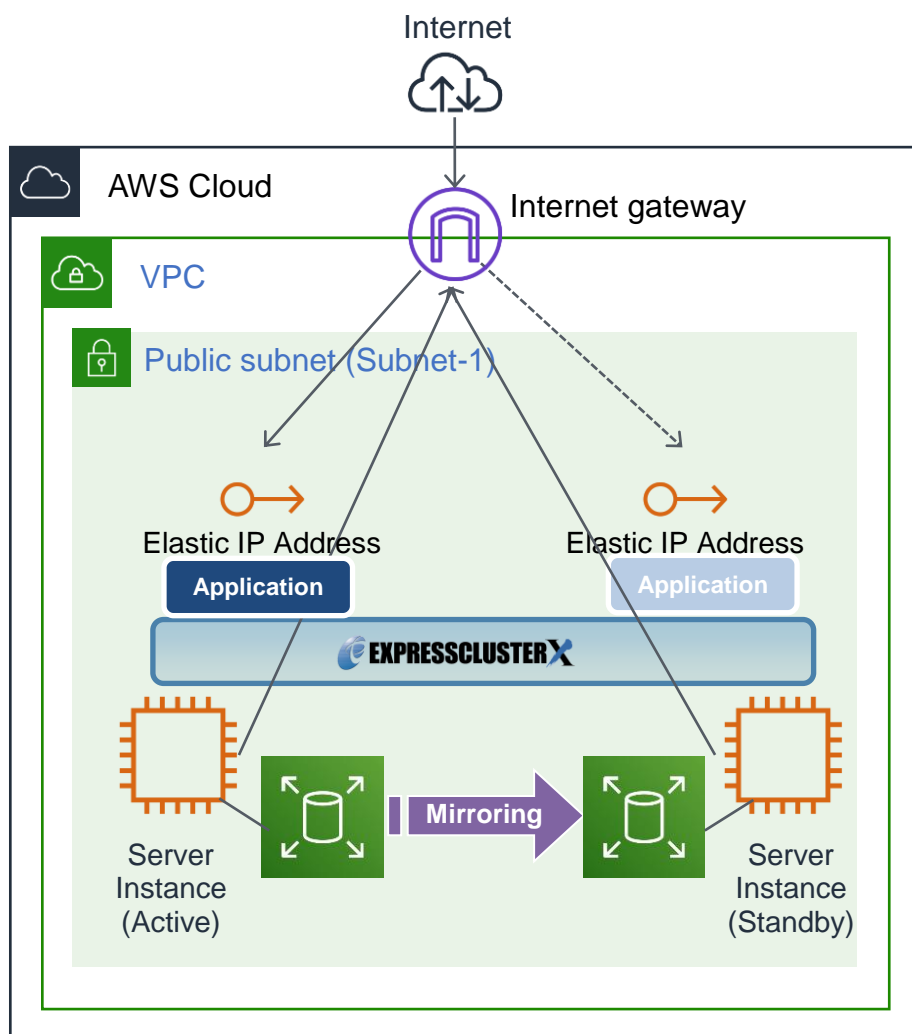


Figure 1-3 HA Cluster Based on EIP Control

In the above figure, the server instances are clustered and placed on the public subnet. The AWS Virtual 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.

* When executing the AWS CLI, each instance must be able to communicate with the regional endpoint by using a method such as a proxy server, NAT, public IP, and EIP. In this guide, a public IP assigned to the instance is used for the HA cluster based on EIP control.

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 sever 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
Custom monitor resource	Monitors a network partition (NP) so that the same resource does not start in multiple instances at the same time.	Required to perform NP resolution
Other resources and monitor resources	Depends on the configuration of the application, such as a mirror disk, used in an HA cluster.	Optional

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.

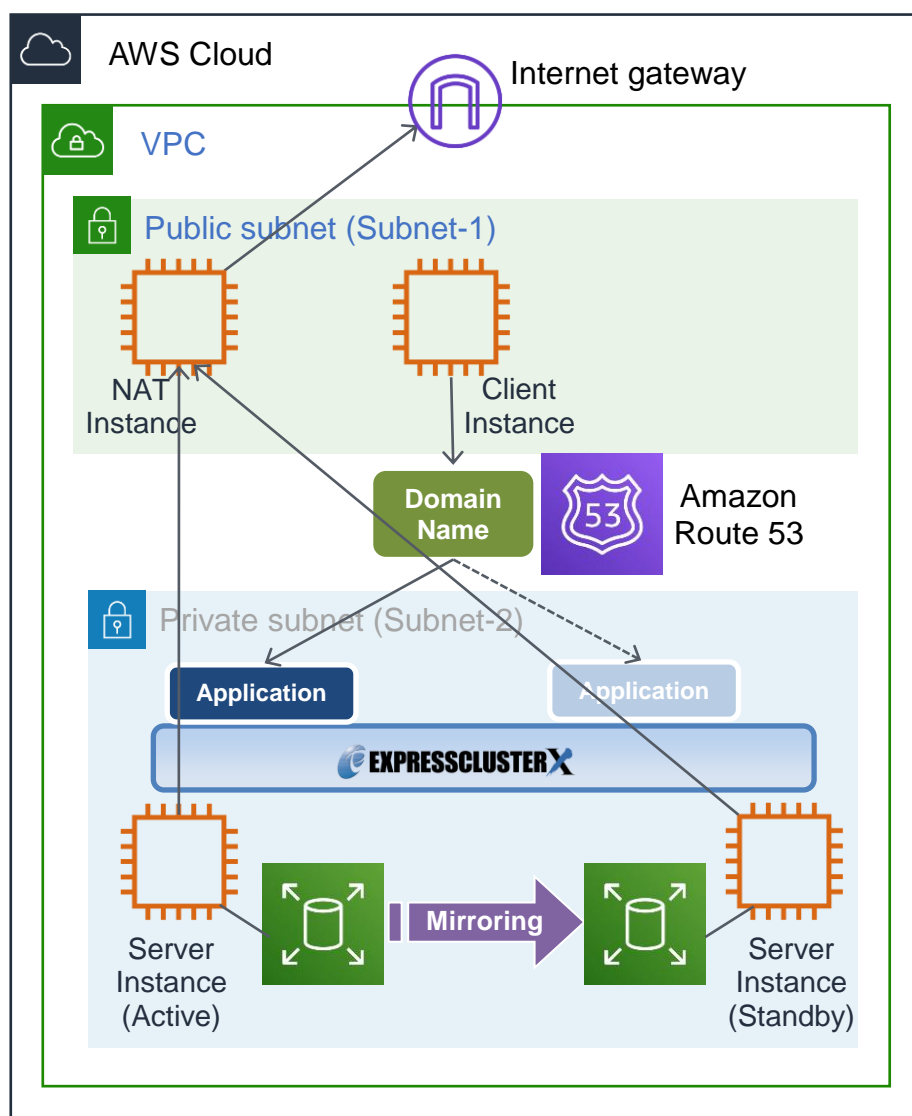


Figure 1-4 HA cluster based on DNS name control

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.

* When executing the AWS CLI, each instance must be able to communicate with the regional endpoint by using a method such as a proxy server, NAT, public IP and EIP. In this guide, NAT is used for the HA cluster based on DNS name control.

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
IP monitor resource	Monitors the health of communication between subnets by checking whether communication with a NAT is available.	Required to check the health of communication between subnets.
Other resources and monitor resources	Depends on the configuration of the application, such as a mirror disk, used in an HA cluster.	Optional

1-3. 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

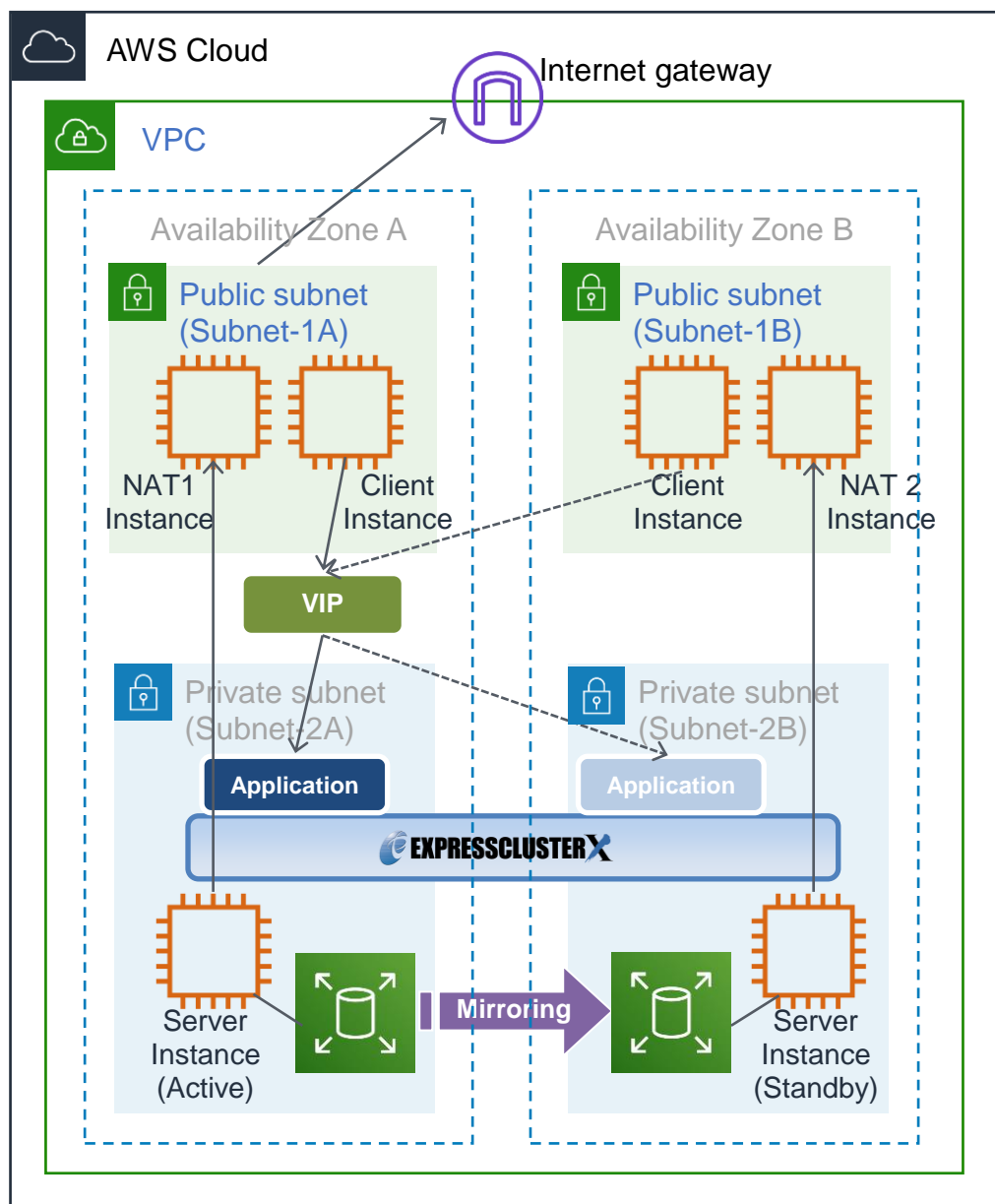


Figure 1-5 HA Cluster Using Multi-AZ

1-4. Network partition resolution

The instances configuring an HA cluster perform alive monitoring on each other by using heartbeat. In the configuration in which instances are distributed to multiple subnets, an undesirable condition such as redundant startup of a service occurs if the heartbeat is lost. To prevent redundant startup of a service, it is required to determine whether the instance itself was isolated in a network (network partition: NP) or the other instance was down.

The NP resolution conducts a ping or LISTEN port test for an always running device that can return a response (hereafter referred to as an *acknowledgement device*). If the acknowledgement device does not return a response, it is determined that an NP has occurred and the predefined process is performed (for example, issuing a warning, performing a recovery operation, or shutting down the server).

The Amazon VPC uses the following as the ping device usually.

HA cluster type	ping device	Method	Remarks
HA cluster based on VIP control	Instance always running on another subnet	Ping	In this guide, Instance for NAT is used.
HA cluster based on EIP control	Regional endpoint	LISTEN port acknowledgement	For the regional endpoints, refer to the following URL: https://docs.aws.amazon.com/general/latest/gr/rande.html Example: When the region name is Asia Pacific (Tokyo), the regional endpoint is <code>ec2.ap-northeast-1.amazonaws.com</code> .

1-5. On-premises and AWS

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

A: Available, N: Not available

Function	On-premises	AWS
Creation of a shared disk type cluster	A	NA
Creation of a mirror disk type cluster	A	A
Floating IP resource	A	NA
Virtual IP resource	A	NA
AWS Elastic IP resource	NA	A
AWS Virtual IP resource	NA	A
AWS DNS resource	NA	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.

	Step	On-premises	AWS
Before installing EXPRESSCLUSTER			
1	Configure the VPC environment.	Not required	<ul style="list-style-type: none"> ◇ When using the AWS Virtual IP resource, refer to “4-1 Configuring the VPC Environment” in this guide. ◇ When using the AWS Elastic IP resource, refer to “5-1 Configuring the VPC Environment” in this guide. ◇ When AWS DNS resource is used, refer to “6-1 Setting up the VPC Environment” in this guide.
2	Configure the instance.	Not required	<ul style="list-style-type: none"> ◇ When using the AWS Virtual IP resource, refer to “4-2 Configuring the instance” in this guide. ◇ When using the AWS Elastic IP resource, refer to “5-2 Configuring the instance” in this guide. ◇ When AWS DNS resource is used, refer to “6-2 Setting up the instance” in this guide.
3	Configure a partition for a mirror disk resource.	Refer to the following: <ul style="list-style-type: none"> • <i>Installation and Configuration Guide</i> → Chapter 1 Determining a system configuration → Settings after configuring hardware • <i>Reference Guide</i> → Understanding mirror disk resources 	Same as the on-premises environment

4	Adjust the OS startup time.	Refer to the following: <i>Installation and Configuration Guide</i> → Chapter 1 Determining a system configuration → Settings after configuring hardware	Same as the on-premises environment
5	Check the network.		
6	Check the root file system		
7	Check the firewall.		
8	Synchronize the server time.		
9	Install EXPRESSCLUSTER.	Refer to the following: • <i>Installation and Configuration Guide</i> → Chapter 3 Installing EXPRESSCLUSTER	Same as the on-premises environment
After installing EXPRESSCLUSTER			
10	Register the EXPRESSCLUSTER license.	Refer to the following: • <i>Installation and Configuration Guide</i> → Chapter 4 Registering the license	Same as the on-premises environment
11	Construct a cluster - Set up the heartbeat method.	Refer to the following: • <i>Installation and Configuration Guide</i> → Chapter 5 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: • <i>Installation and Configuration Guide</i> → Chapter 5 Creating the cluster configuration data → Creating the cluster configuration data • <i>Reference Guide</i> → Chapter 5 Network partition resolution resources details	<ul style="list-style-type: none"> ◇ When using the AWS Virtual IP resource, refer to “4-3 Setting up EXPRESSCLUSTER” → “3) Add a monitor resource.” → “IP monitor resource” in this guide. ◇ When using the AWS Elastic IP resource, refer to “5-3 Setting up EXPRESSCLUSTER” → “1) Construct a cluster” in this guide. ◇ When AWS DNS resource is used, refer to “6-3 Setting up of EXPRESSCLUSTER” - “1) Cluster configuration” in this guide.

13	Construct a cluster: Create a failover group Create a monitor resource.	Refer to the following: <ul style="list-style-type: none">• <i>Installation and Configuration Guide</i><ul style="list-style-type: none">→ Chapter 5 Creating the cluster configuration data→ Creating the cluster configuration data	<p>In addition to the reference for the on-premises environment, refer to the following:</p> <ul style="list-style-type: none">◇ When using the AWS Virtual IP resource<ul style="list-style-type: none">• “4-3 Setting up EXPRESSCLUSTER” in this guide• <i>Reference Guide</i><ul style="list-style-type: none">→ Understanding AWS Virtual IP resources◇ When using the AWS Elastic IP resource, refer to the following:<ul style="list-style-type: none">• “5-3 Setting up EXPRESSCLUSTER” in this guide• <i>Reference Guide</i><ul style="list-style-type: none">→ Understanding AWS Elastic IP resources◇ When AWS DNS resource is used, refer to below documents:<ul style="list-style-type: none">• “6-3 Setting up EXPRESSCLUSTER” in this guide.• <i>Reference Guide</i><ul style="list-style-type: none">→ Understanding AWS DNS resources.
----	---	--	---

Chapter 2 Operating Environment

For details, refer to the following:

- *Getting Started Guide*
 - Chapter 3 Installation requirements for EXPRESSCLUSTER
 - Operation environment for AWS Elastic IP resource, AWS Virtual IP resource, AWS Elastic IP monitor resource, AWS virtual IP monitor resource, AWS AZ monitor resource
- *Getting Started Guide*
 - Chapter 3 Installation requirements for EXPRESSCLUSTER
 - Operation environment for AWS DNS resource, AWS DNS monitor resource

Chapter 3 Notes

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 “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.

However, if NAT does not exist, IP address monitoring cannot be executed by IP monitor resource for NP resolution. Therefore, ping device should be prepared separately.

Moreover, even when VCP 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.

Restrictions on the group resource and monitor resource functions

Refer to the following:

- *Getting Started Guide*
 - Chapter 5 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

For a mirror type HA cluster, a write request to a mirror disk takes the following routes:

Write request I/O:

Guest OS on the active server → Host OS on the active server → Host OS on the standby server → Guest OS on the standby server

Writing completion notice:

Guest OS on the standby server → Host OS on the standby server → Host OS on the active server → Guest OS on the active server

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.

Chapter 4 Constructing an HA cluster based on VIP control

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

The numbers in the figure correspond to the descriptions and setting values in the following sections.

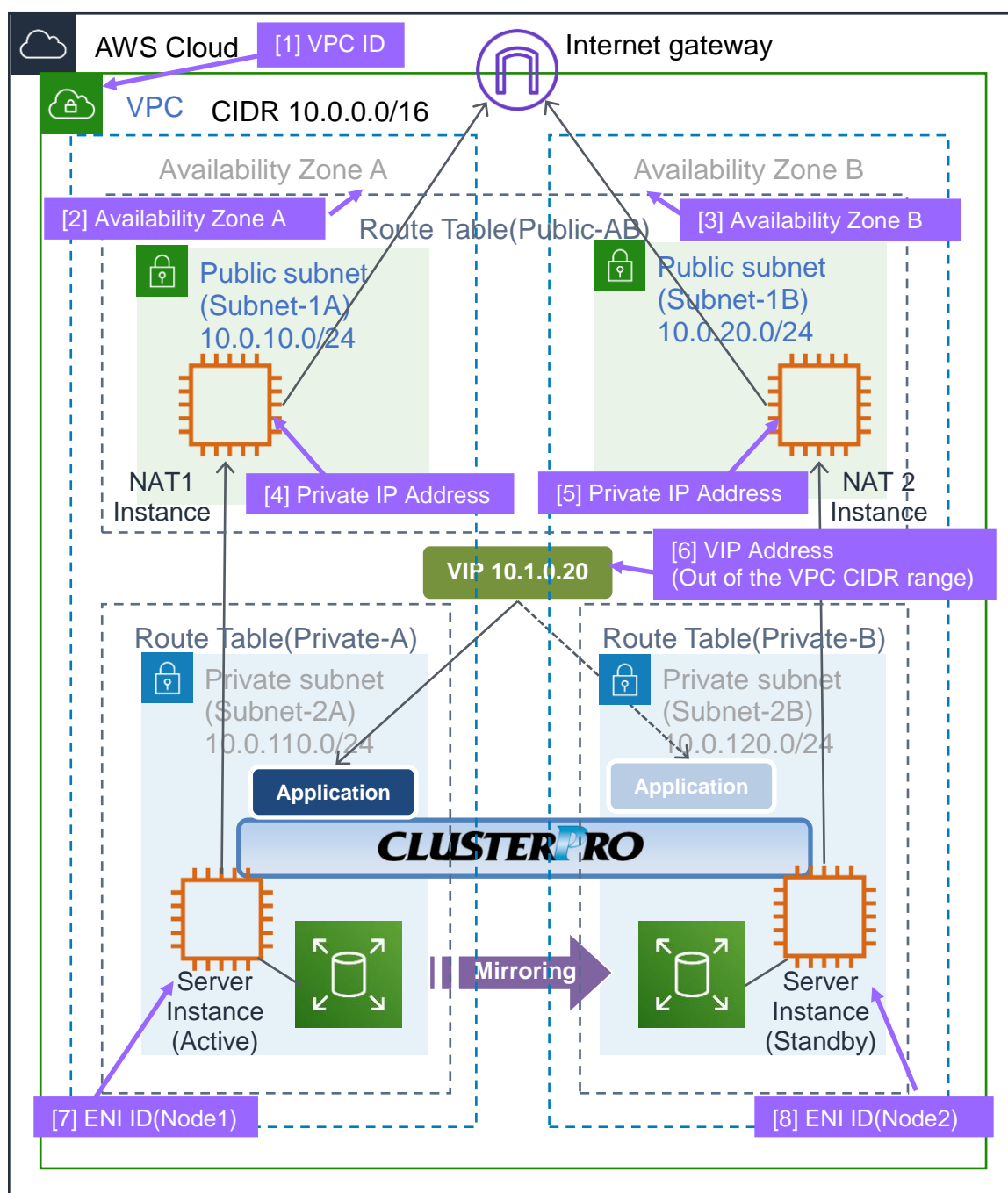


Figure 4-1 System Configuration of the HA Cluster Based on VIP Control

4-1. 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. This guide does not describe the case to perform operations by adding an ENI to an instance of an HA cluster node.

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 ID

Write down the VPC ID (vpc-xxxxxxx) because it is necessary to set up the AWS Virtual IP resource later.

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*
 - Chapter 5 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 "Chapter 7 Configuring the IAM"

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**.

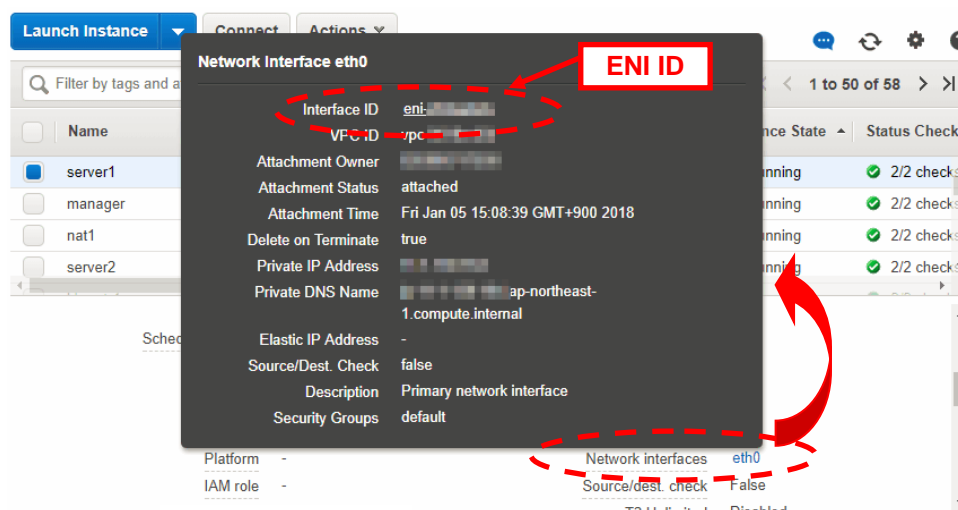
[7] ENI ID (Node1)

[8] ENI ID (Node2)

Write down the ENI ID (eni-xxxxxxx) of each instance because it is necessary to set up the AWS Virtual IP resource later.

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 instance.

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 instance on the public networks (Subnet-1A and Subnet-1B). In the AWS environment, `amzn-ami-vpc-nat-pv-2014.09.1.x86_64-ebs` is prepared as the AMI with the string, `amzn-ami-vpc-nat` included.

When creating a NAT instance, enable the public IP. In addition, disable **Source/Dest. Check** of the added NAT instance to enable the NAT function.

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

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-xxxxxxx (ENI ID of the active server instance) [7] ENI ID (Node1)	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	NAT1	Add (required)
VIP address (Example: 10.1.0.20/32)	eni-xxxxxxx (ENI ID of the active server instance) [7] ENI ID (Node1)	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	NAT2	Add (required)
VIP address (Example: 10.1.0.20/32)	eni-xxxxxxx (ENI ID of the active server instance) [7] ENI ID (Node1)	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 Address

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 it is necessary to set up the AWS Virtual IP resource later.

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.

4-2. Configuring the instance

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

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

- *Getting Started Guide*
 - Chapter 3 Installation requirements for EXPRESSCLUSTER
 - Operation environment for AWS Elastic IP resource, AWS Virtual IP 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*
 - Chapter 5 Notes and Restrictions
 - Before installing EXPRESSCLUSTER

3) Install Python.

Install Python required by EXPRESSCLUSTER.

First, confirm that Python is installed.

If Python has not been installed, install it by using a command such as `yum`.

The installation path of the python commands must be any of the following:

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

4) Install the AWS CLI.

Install the AWS CLI by running the `pip` command from a shell.

```
$ pip install awscli
```

For details about the `pip` command, refer to the following:

<https://pip.pypa.io/en/latest/>

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 Python or 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*
 - Chapter 1 Determining a system configuration
 - 4. 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.

4-3. Setting up EXPRESSCLUSTER

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

- *Installation and Configuration Guide*
→ Chapter 5 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 (IP monitor resource)

For the settings other than the above, refer to “*Installation and Configuration Guide*”.

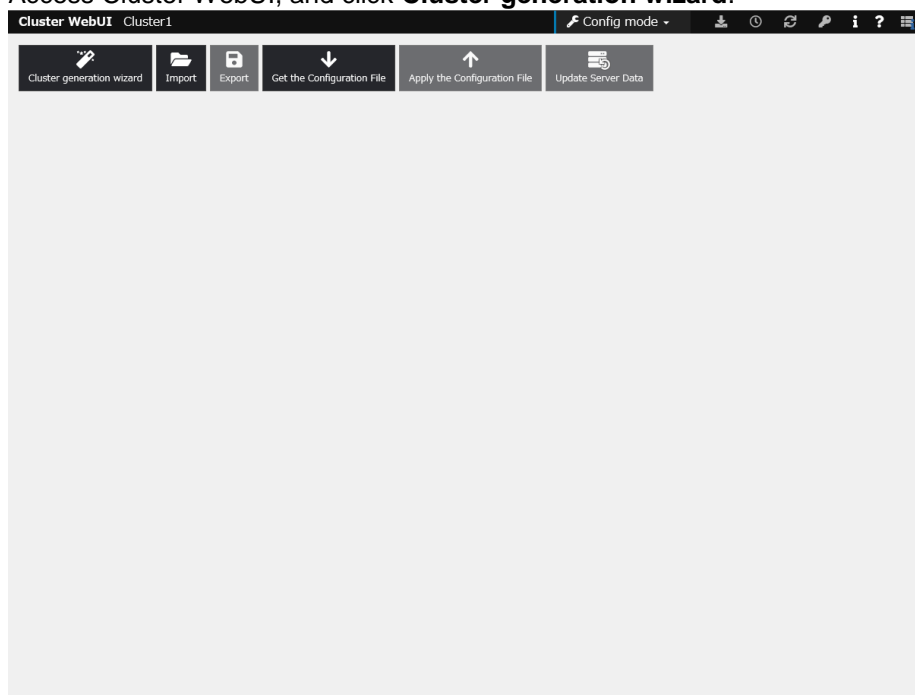
1) Construct a cluster.

Start the Cluster generation wizard to construct a cluster.

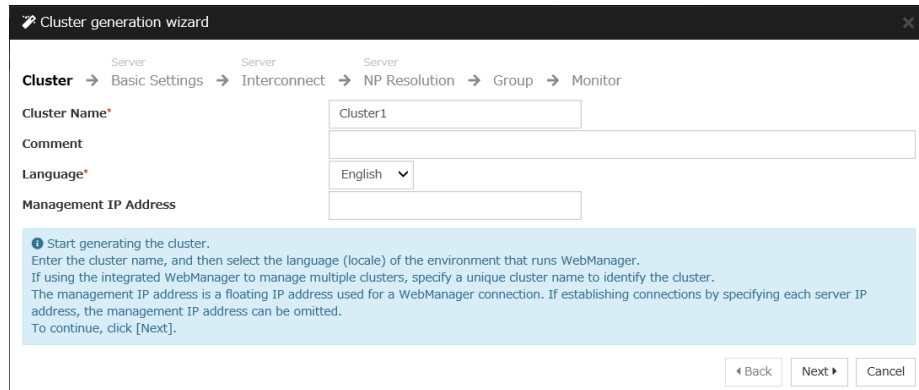
- ◇ Construct a cluster.

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**.



Cluster generation wizard

Cluster → Basic Settings → Interconnect → NP Resolution → Group → Monitor

Cluster Name*

Comment

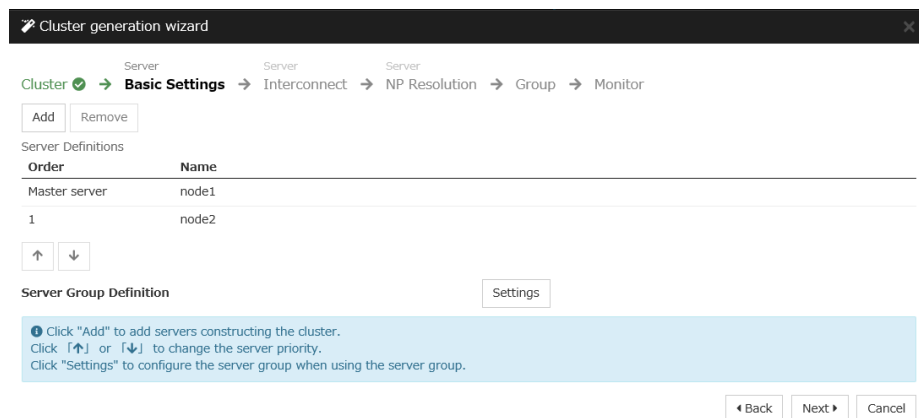
Language* English ▾

Management IP Address

Start generating the cluster.
Enter the cluster name, and then select the language (locale) of the environment that runs WebManager.
If using the integrated WebManager to manage multiple clusters, specify a unique cluster name to identify the cluster.
The management IP address is a floating IP address used for a WebManager connection. If establishing connections by specifying each server IP address, the management IP address can be omitted.
To continue, click [Next].

◀ Back Next ▶ Cancel

- 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**.



Cluster generation wizard

Cluster → Basic Settings → Interconnect → NP Resolution → Group → Monitor

Add Remove

Server Definitions

Order	Name
Master server	node1
1	node2

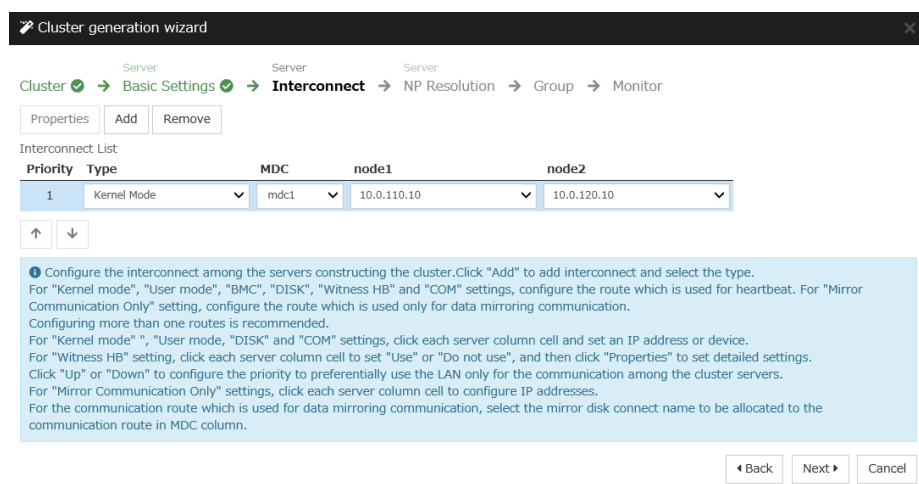
⬆ ⬇ ⬆

Server Group Definition Settings

Click "Add" to add servers constructing the cluster.
Click "⬆" or "⬇" to change the server priority.
Click "Settings" to configure the server group when using the server group.

◀ Back Next ▶ Cancel

- 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**.



Cluster generation wizard

Cluster → Basic Settings → Interconnect → NP Resolution → Group → Monitor

Properties Add Remove

Interconnect List

Priority	Type	MDC	node1	node2
1	Kernel Mode ▾	mdc1 ▾	10.0.110.10 ▾	10.0.120.10 ▾

⬆ ⬇ ⬆

Configure the interconnect among the servers constructing the cluster. Click "Add" to add interconnect and select the type.
For "Kernel mode", "User mode", "BMC", "DISK", "Witness HB" and "COM" settings, configure the route which is used for heartbeat. For "Mirror Communication Only" setting, configure the route which is used only for data mirroring communication.
Configuring more than one routes is recommended.
For "Kernel mode", "User mode", "DISK" and "COM" settings, click each server column cell and set an IP address or device.
For "Witness HB" setting, click each server column cell to set "Use" or "Do not use", and then click "Properties" to set detailed settings.
Click "Up" or "Down" to configure the priority to preferentially use the LAN only for the communication among the cluster servers.
For "Mirror Communication Only" settings, click each server column cell to configure IP addresses.
For the communication route which is used for data mirroring communication, select the mirror disk connect name to be allocated to the communication route in MDC column.

◀ Back Next ▶ Cancel

- The **NP Resolution** window is displayed.
However, the NP resolution is not set on this window. The same operation as the NP resolution can be achieved by adding the IP monitor resource and monitoring a NAT instance set in each AZ. (The NP resolution will be set in "3) Add a monitor resource." described later.)

You need to examine the NP resolution destination and method depending on the location of clients accessing a cluster system and the condition for connecting to an on-premise environment (for example, using a dedicated line). Additionally, you can use network partition resolution resources for 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 “4-2 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**.

Resource Definition of Group | failover1 awsvip ✕

Info → Dependency → Recovery Operation → Details

Type* AWS Virtual IP resource ▼

Name* awsvip1

Comment

Get license information

❗ Select the type of group resource and enter its name.

◀ Back Next ▶ Cancel

3. The **Dependency** window is displayed. Click **Next** without specifying anything.
4. The **Recovery Operation** window is displayed.
Click **Next**.

- 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 4-1).

Set the ID of the VPC including instances in the **VPC ID** box (corresponds to [1] in Figure 4-1).

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 4-1).

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.

Resource Definition of Group | failover1 awsvip ✕

Info → Dependency → Recovery Operation → **Details**

Common node1 node2

IP Address*

VPC ID*

ENI ID*

- 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 4-1).
Enter the ENI ID of the instance corresponding to the node in the **ENI ID** box (corresponds to [7] and [8] in Figure 4-1).

Resource Definition of Group | failover1 awsvip ✕

Info → Dependency → Recovery Operation → **Details**

Common node1 node2

Set Up Individually ☒

VPC ID*

ENI ID*

Resource Definition of Group | failover1 awsvip ✕

Info → Dependency → Recovery Operation → **Details**

Common node1 node2

Set Up Individually ☒

VPC ID*

ENI ID*

- 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**.

The screenshot shows the 'Monitor Resource Definition' window with the title bar 'awsazw1'. The breadcrumb navigation is 'Info → Monitor(common) → Monitor(special) → Recovery Action'. The 'Type' dropdown is set to 'AWS AZ monitor'. The 'Name' text box contains 'awsazw1'. There is a 'Comment' text box and a 'Get Licence Info' button. A blue information bar at the bottom states: 'Select the type of monitor resource and enter its name.' Navigation buttons at the bottom right are 'Back', 'Next', and 'Cancel'.

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 4-1)

The screenshot shows the 'Monitor Resource Definition' window with the title bar 'awsazw1'. The breadcrumb navigation is 'Info → Monitor(common) → Monitor(special) → Recovery Action'. The 'Common' tab is active, showing 'node1' and 'node2' as sub-tabs. The 'Availability Zone' text box contains 'ap-northeast-1a'. The 'Action when AWS CLI command failed to receive response' dropdown is set to 'Disable recovery action(Display warning)'. Navigation buttons at the bottom right are 'Back', 'Next', and 'Cancel'.

- 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 4-1) Click **Next**.

Monitor Resource Definition awsazw

Info ✓ → Monitor(common) ✓ → **Monitor(special)** → Recovery Action

Common node1 node2

Set Up Individually ☒

Availability Zone*

◀ Back Next ▶ Cancel

Monitor Resource Definition awsazw

Info ✓ → Monitor(common) ✓ → **Monitor(special)** → Recovery Action

Common node1 node2

Set Up Individually ☒

Availability Zone*

◀ Back Next ▶ Cancel

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

Monitor Resource Definition awsazw

Info ✓ → Monitor(common) ✓ → **Monitor(special)** ✓ → **Recovery Action**

Recovery Action

Recovery Target*

Recovery Script Execution Count* time

Execute Script before Reactivation ☐

Maximum Reactivation Count time

Execute Script before Failover ☐

Execute migration before Failover ☐

Maximum Failover Count time

Execute Script before Final Action ☐

Final Action

Script Settings

◀ Back **Finish** Cancel

- Click **Finish** to complete setting.

◇ AWS Virtual IP monitor resource

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

The existence of the VIP address and the health of the route table can be checked by using the OS API and the AWS CLI commands.

For details, refer to the following:

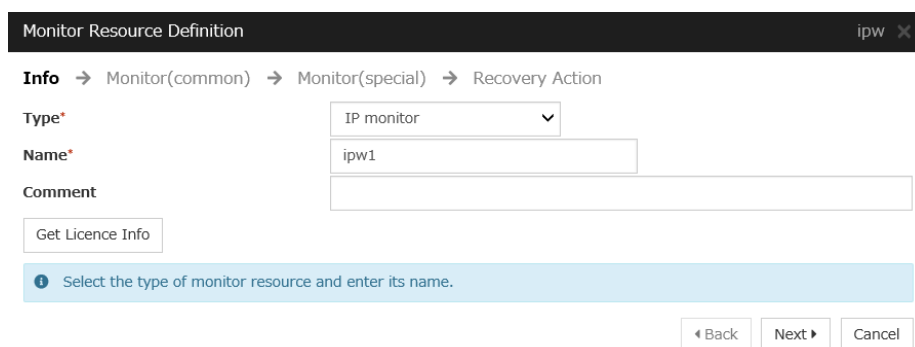
- *Reference Guide*
→ Understanding AWS Virtual IP monitor resources

◇ IP monitor resource

Create the IP monitor resource to monitor the health of the subnet by sending a ping to a NAT instance placed in each AZ. Specify the following:

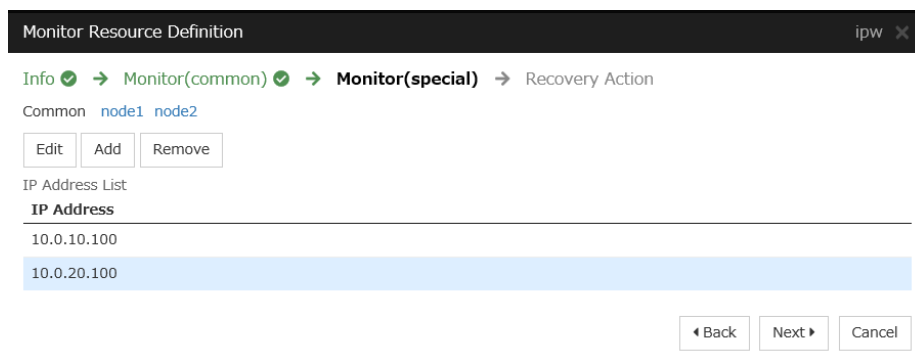
Steps

1. Click **Add** in **Monitor Resource List**.
2. Select the monitor resource type (IP monitor) from the **Type** box and enter the monitor resource name (ipw1) in the **Name** box. Click **Next**.



The screenshot shows the 'Monitor Resource Definition' window with the title bar 'ipw X'. The breadcrumb navigation is 'Info → Monitor(common) → Monitor(special) → Recovery Action'. The 'Type' dropdown is set to 'IP monitor'. The 'Name' field contains 'ipw1'. There is a 'Comment' field and a 'Get Licence Info' button. A blue information bar at the bottom states: 'Select the type of monitor resource and enter its name.' Navigation buttons at the bottom right are 'Back', 'Next', and 'Cancel'.

3. The **Monitor (common)** window is displayed. Confirm that **Monitoring Timing** is **Always** and click **Next**.
4. The **Monitor (special)** window is displayed. Enter the private IP address of the NAT instance used by each node in the **IP Address** box of the **Common** tab (corresponds to [4] and [5] in Figure 4-1). Click **Next**.



The screenshot shows the 'Monitor Resource Definition' window with the title bar 'ipw X'. The breadcrumb navigation is 'Info → Monitor(common) → Monitor(special) → Recovery Action'. The 'Common' tab is selected, showing 'node1' and 'node2'. There are 'Edit', 'Add', and 'Remove' buttons. Below is the 'IP Address List' section with a table containing two entries: '10.0.10.100' and '10.0.20.100'. The second entry is highlighted. Navigation buttons at the bottom right are 'Back', 'Next', and 'Cancel'.

5. The **Recovery Action** window is displayed.
Set LocalServer in the **Recovery Target** box.
Select **Stop the cluster service and shutdown OS** in **Final Action**.

The screenshot shows the 'Monitor Resource Definition' window with the 'Recovery Action' tab selected. The breadcrumb trail is 'Info' → 'Monitor(common)' → 'Monitor(special)' → 'Recovery Action'. The 'Recovery Action' dropdown is set to 'Custom settings'. The 'Recovery Target' is 'LocalServer' with a 'Browse' button. The 'Recovery Script Execution Count' is '0' with a 'time' unit. The 'Execute Script before Reactivation' checkbox is unchecked, and the 'Maximum Reactivation Count' is '0' with a 'time' unit. The 'Execute Script before Failover' checkbox is unchecked, and the 'Execute migration before Failover' checkbox is also unchecked. The 'Maximum Failover Count' is '0' with a 'time' unit. The 'Execute Script before Final Action' checkbox is unchecked. The 'Final Action' dropdown is set to 'Stop the cluster service and shutdown OS'. There is a 'Script Settings' button and 'Back', 'Finish', and 'Cancel' buttons at the bottom right.

Monitor Resource Definition ipw

Info → Monitor(common) → Monitor(special) → Recovery Action

Recovery Action Custom settings

Recovery Target * LocalServer Browse

Recovery Script Execution Count* 0 time

Execute Script before Reactivation ☐

Maximum Reactivation Count 0 time

Execute Script before Failover ☐

Execute migration before Failover ☐

Maximum Failover Count 0 time

Execute Script before Final Action ☐

Final Action Stop the cluster service and shutdown OS

Script Settings

Back Finish Cancel

6. Click **Finish** to complete setting.

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 5 Constructing an HA cluster based on EIP control

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

The numbers in the figure correspond to the descriptions and setting values in the following sections.

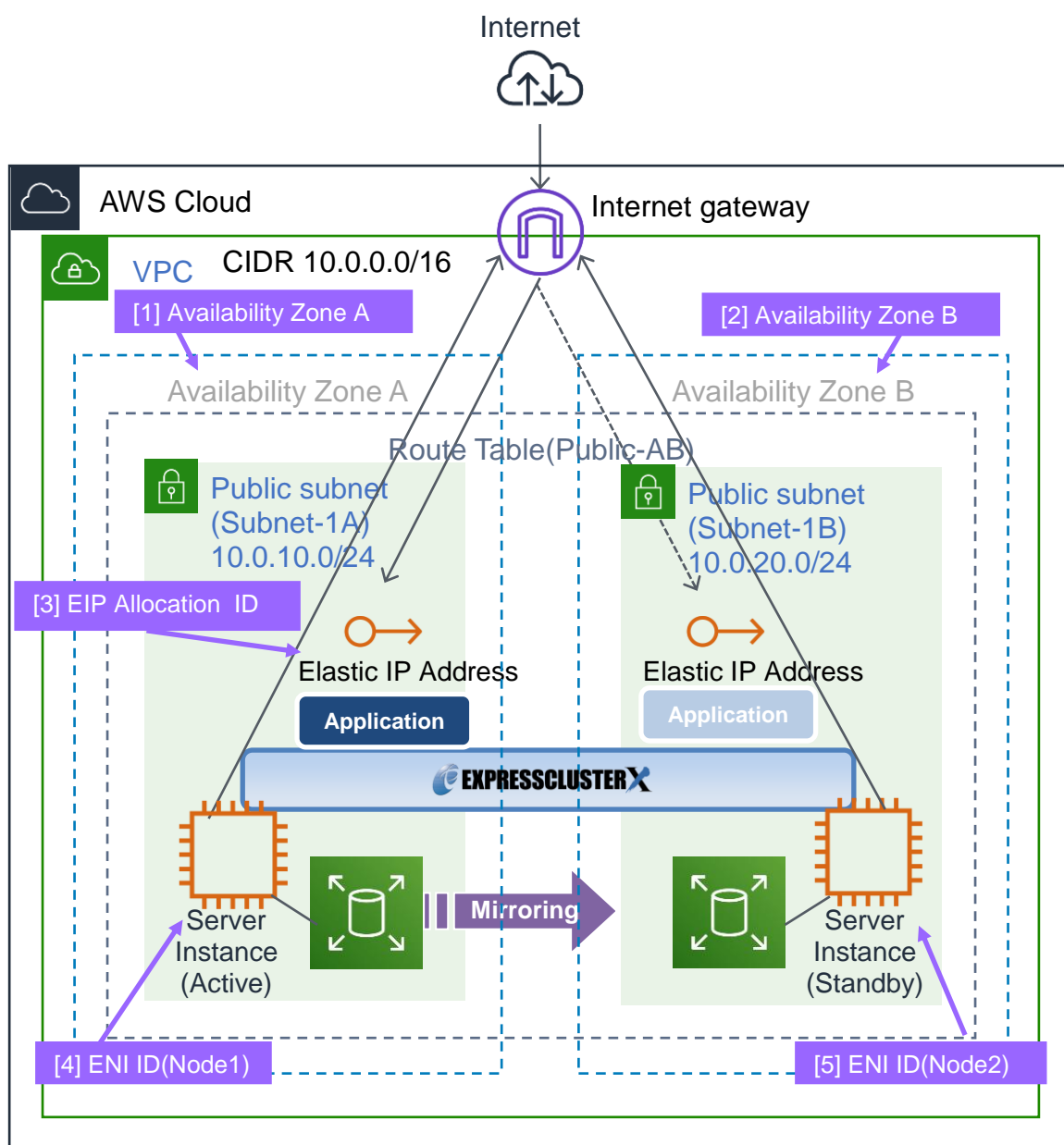


Figure 5-1 System Configuration of the HA cluster based on EIP control

5-1. 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. This guide does not describe the case to perform operations by adding an ENI to an instance of an HA cluster node.

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*
 - Chapter 5 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 "Chapter 7 Configuring the IAM".

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

[4] ENI ID (Node1)

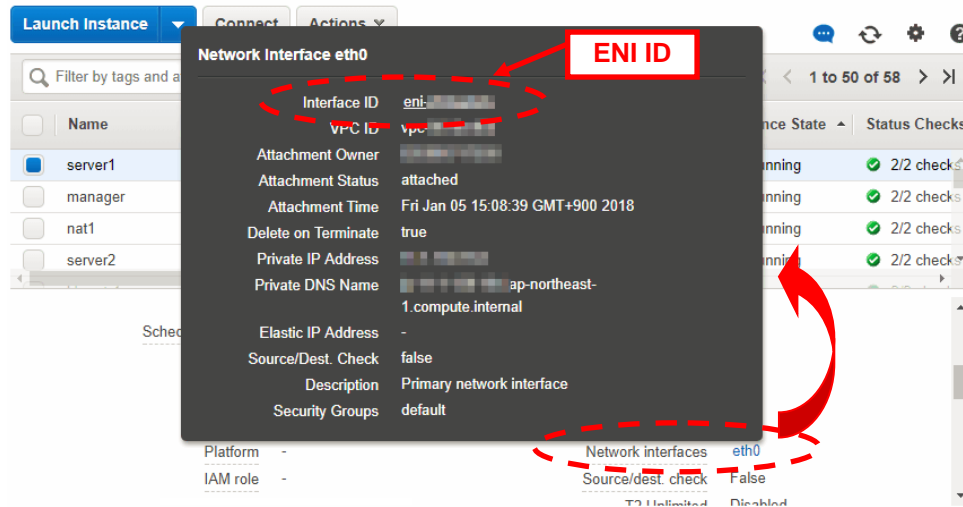
[5] ENI ID (Node2)

Write down the ENI ID (eni-xxxxxxx) of each instance because it is necessary to set up the AWS Elastic IP resource later.

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] EIP Allocation ID

Write down the Allocation ID (eipalloc-xxxxxxx) of the added EIP because it is necessary to set up the AWS Elastic IP resource later.

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.

5-2. Configuring the instance

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

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

- *Getting Started Guide*
 - Chapter 3 Installation requirements for EXPRESSCLUSTER
 - Operation environment for AWS Elastic IP resource, AWS Virtual IP resource, AWS Elastic IP monitor resource, AWS virtual IP monitor resource, AWS AZ 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*
 - Chapter 5 Notes and Restrictions
 - Before installing EXPRESSCLUSTER

3) Install Python.

Install Python required by EXPRESSCLUSTER.

First, confirm that Python is installed.

If Python has not been installed, install it by using a command such as `yum`.

The installation path of the python commands must be any of the following:

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

4) Install the AWS CLI.

Install the AWS CLI by running the `pip` command from a shell.

```
$ pip install awscli
```

For details about the `pip` command, refer to the following:

<https://pip.pypa.io/en/latest/>

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 Python or 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*
 - Chapter 1 Determining a system configuration
 - 4. 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.

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*
→ Chapter 5 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 (Custom monitor resource)

For the settings other than the above, refer to “*Installation and Configuration Guide*”.

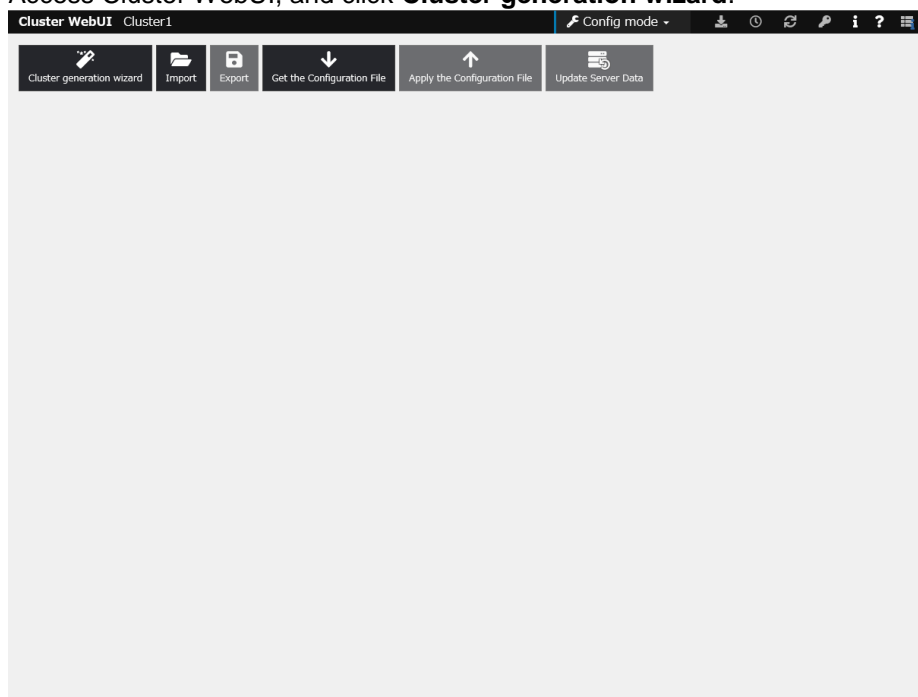
1) Construct a cluster.

Start the Cluster generation wizard to construct a cluster.

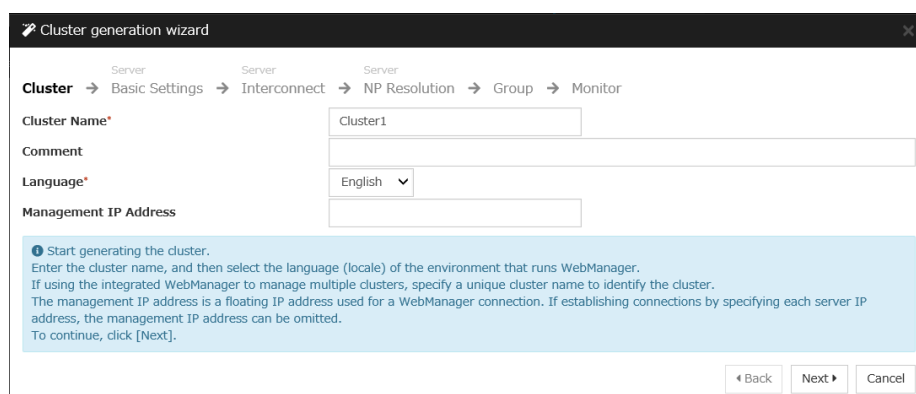
- ◇ Construct a cluster.

Steps

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



- 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**.



Cluster generation wizard

Cluster → Basic Settings → Interconnect → NP Resolution → Group → Monitor

Cluster Name*

Comment

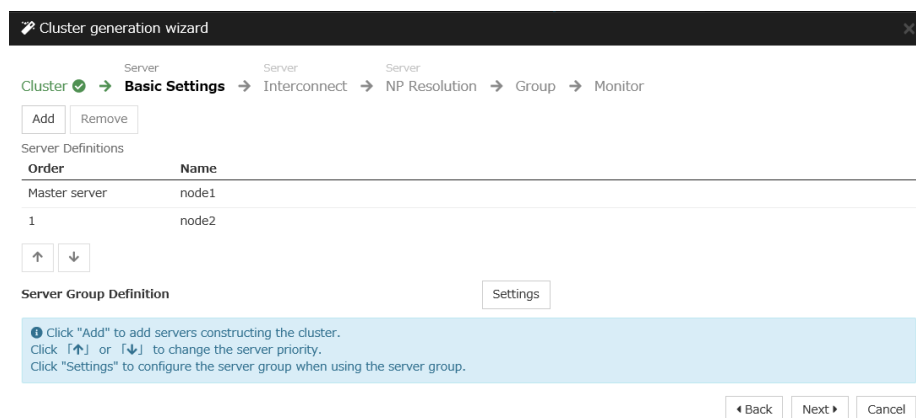
Language* English ▼

Management IP Address

Start generating the cluster.
Enter the cluster name, and then select the language (locale) of the environment that runs WebManager.
If using the integrated WebManager to manage multiple clusters, specify a unique cluster name to identify the cluster.
The management IP address is a floating IP address used for a WebManager connection. If establishing connections by specifying each server IP address, the management IP address can be omitted.
To continue, click [Next].

◀ Back Next ▶ Cancel

- 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**.



Cluster generation wizard

Cluster → Basic Settings → Interconnect → NP Resolution → Group → Monitor

Add Remove

Server Definitions

Order	Name
Master server	node1
1	node2

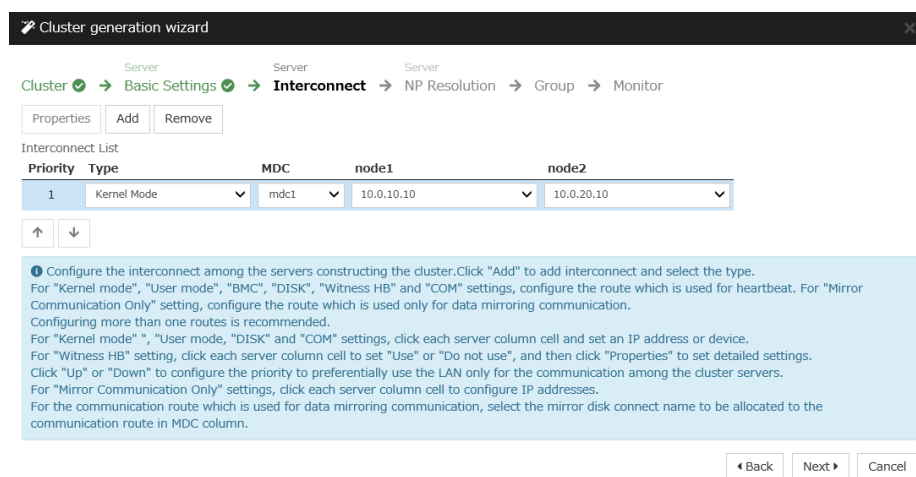
⬆ ⬇ ⬆

Server Group Definition Settings

Click "Add" to add servers constructing the cluster.
Click "⬆" or "⬇" to change the server priority.
Click "Settings" to configure the server group when using the server group.

◀ Back Next ▶ Cancel

- 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**.



Cluster generation wizard

Cluster → Basic Settings → Interconnect → NP Resolution → Group → Monitor

Properties Add Remove

Interconnect List

Priority	Type	MDC	node1	node2
1	Kernel Mode ▼	mdc1 ▼	10.0.10.10 ▼	10.0.20.10 ▼

⬆ ⬇ ⬆

Configure the interconnect among the servers constructing the cluster. Click "Add" to add interconnect and select the type.
For "Kernel mode", "User mode", "BMC", "DISK", "Witness HB" and "COM" settings, configure the route which is used for heartbeat. For "Mirror Communication Only" setting, configure the route which is used only for data mirroring communication.
Configuring more than one routes is recommended.
For "Kernel mode", "User mode", "DISK" and "COM" settings, click each server column cell and set an IP address or device.
For "Witness HB" setting, click each server column cell to set "Use" or "Do not use", and then click "Properties" to set detailed settings.
Click "Up" or "Down" to configure the priority to preferentially use the LAN only for the communication among the cluster servers.
For "Mirror Communication Only" settings, click each server column cell to configure IP addresses.
For the communication route which is used for data mirroring communication, select the mirror disk connect name to be allocated to the communication route in MDC column.

◀ Back Next ▶ Cancel

5. The **NP Resolution** window is displayed.

However, the NP resolution is not set on this. The same operation as the NP resolution can be achieved by adding the custom monitor resource to confirm whether listening on port 443 of the regional endpoint is normally performed. (The NP resolution will be set in "3) Add a monitor resource." described later.)

You need to examine the NP resolution destination and method depending on the location of clients accessing a cluster system and the condition for connecting to an on-premise environment (for example, using a dedicated line). Additionally, you can use network partition resolution resources for 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**.

Group Definition failover ✕

Basic Settings → Startup Servers → Group Attributes → Group Resource

Type* failover ▼

Use Server Group Settings ☐

Name* failover1

Comment

① Select group type.
If using virtual machine resources to cluster virtual machines, select "Virtual machine" as the type. In other cases, select "Failover".
If using server group, check the "Use Server Group".

◀ Back Next ▶ Cancel

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 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 “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 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 5-1).
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 5-1).

Resource Definition of Group | failover1 awseip

Info → Dependency → Recovery Operation → **Details**

[Common](#) [node1](#) [node2](#)

Set Up Individually ☒

ENI ID*

◀ Back Finish Cancel

Resource Definition of Group | failover1 awseip

Info → Dependency → Recovery Operation → **Details**

[Common](#) [node1](#) [node2](#)

Set Up Individually ☒

ENI ID*

◀ Back Finish Cancel

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

3) Add a monitor resource.

- ◇ AWS AZ monitor resource

Create the AWZ 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**.

Monitor Resource Definition awsazw

Info → Monitor(common) → Monitor(special) → Recovery Action

Type*

Name*

Comment

Get Licence Info

ⓘ Select the type of monitor resource and enter its name.

◀ Back Next ▶ Cancel

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 5-1)

Monitor Resource Definition awsazw

Info → Monitor(common) → **Monitor(special)** → Recovery Action

Common node1 node2

Availability Zone*

Action when AWS CLI command failed to receive response* Disable recovery action(Display warning) ▼

◀ Back Next ▶ Cancel

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 5-1). Click **Next**.

Monitor Resource Definition awsazw

Info → Monitor(common) → **Monitor(special)** → Recovery Action

Common node1 node2

Set Up Individually ☒

Availability Zone*

◀ Back Next ▶ Cancel

Monitor Resource Definition awsazw

Info → Monitor(common) → **Monitor(special)** → Recovery Action

Common node1 node2

Set Up Individually ☒

Availability Zone*

◀ Back Next ▶ Cancel

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

Monitor Resource Definition awsazw

Info → Monitor(common) → Monitor(special) → **Recovery Action**

Recovery Action: Custom settings

Recovery Target: LocalServer Browse

Recovery Script Execution Count*: 0 time

Execute Script before Reactivation: ☐ time

Maximum Reactivation Count: 0 time

Execute Script before Failover: ☐ time

Execute migration before Failover: ☐ time

Maximum Failover Count: 0 time

Execute Script before Final Action: ☐ time

Final Action: No operation

Script Settings

Back Finish Cancel

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

◇ Custom monitor resource

This resource checks the status of the communication with the EIP address by monitoring the communication with port 443 of the endpoint of the region in which the environment has been constructed.

For the regional endpoints, refer to the following URL:

<https://docs.aws.amazon.com/general/latest/gr/rande.html>

For details, refer to the following:

- *Reference Guide*
→ Understanding custom 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 6 Constructing an HA cluster based on DNS name control

This chapter describes how to construct an HA cluster based on DNS name control. The numbers in the figure correspond to the descriptions and setting values in the following sections.

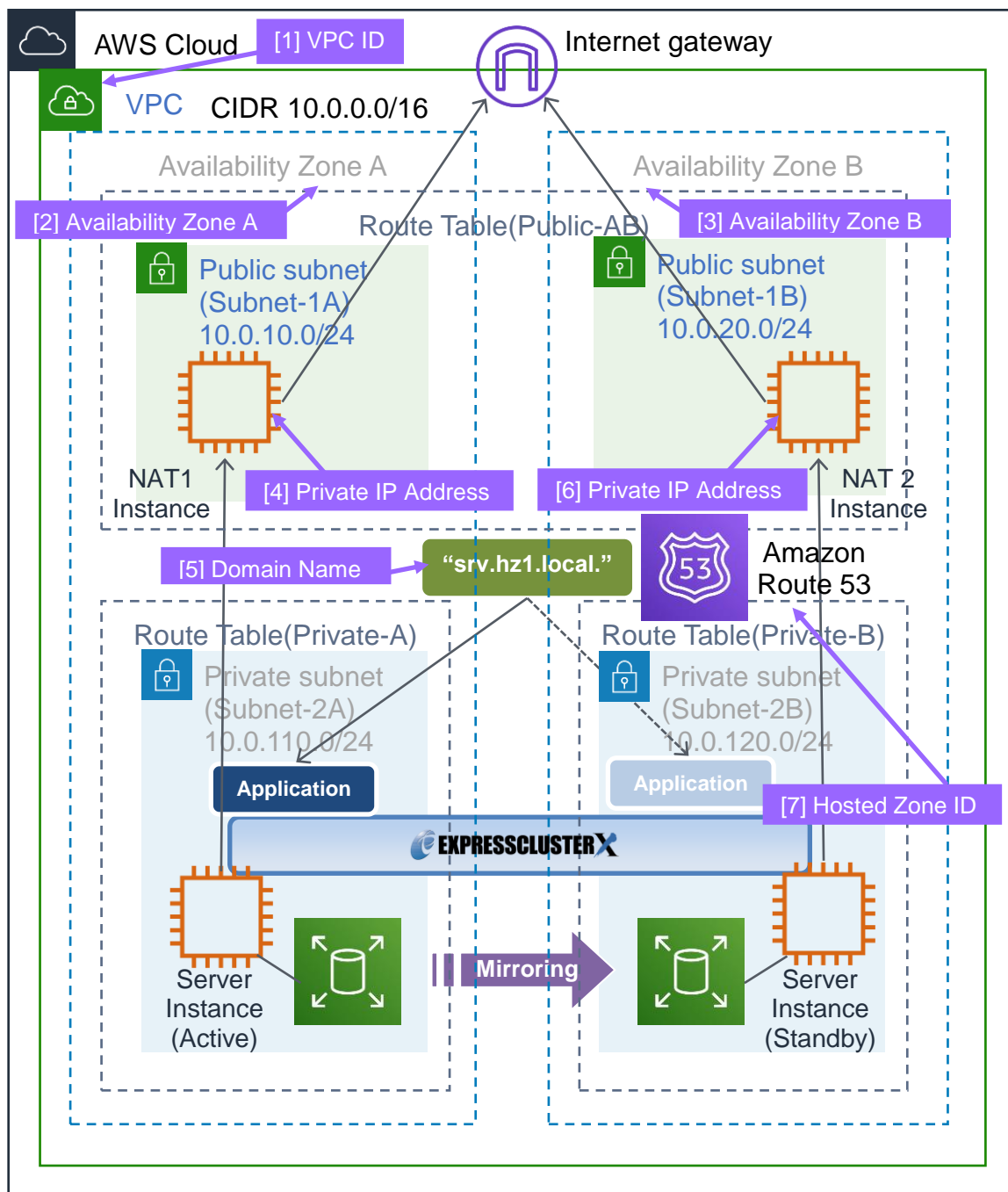


Figure 6-1 System Configuration HA Cluster Based on DNS Name Control

6-1. 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. This guide does not describe the case to perform operations by adding an ENI to an instance of an HA cluster node.

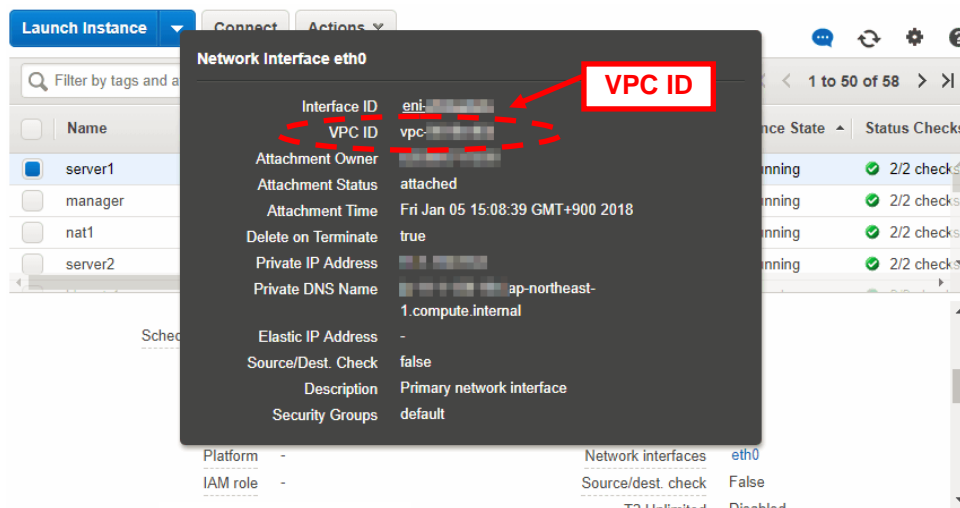
1) Configure the VPC and subnet.

Create a VPC and subnet first.

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

[1] VPC ID

Write down the VPC ID (vpc-xxxxxxx) because it is necessary to add the Hosted Zone later.



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*
 - Chapter 5 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 "Chapter 7 Configuring the IAM"

5) Add a NAT instance.

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 instance on the public networks (Subnet-1A and Subnet-1B). In the AWS environment, `amzn-ami-vpc-nat-pv-2014.09.1.x86_64-ebs` is prepared as the AMI with the string, `amzn-ami-vpc-nat` included.

When creating a NAT instance, enable the public IP. In addition, disable **Source/Dest. Check** of the added NAT instance to enable the NAT function.

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

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 <i>(Example: 10.0.0.0/16)</i>	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 <i>(Example: 10.0.0.0/16)</i>	local	Existing by default
0.0.0.0/0	NAT1	Add (required)

◇ Route Table (Private-B)

Destination	Target	Remarks
VPC network <i>(Example: 10.0.0.0/16)</i>	local	Existing by default
0.0.0.0/0	NAT2	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 **[1] VPC ID** where the instance belongs, in the **VPC ID** box.

[7] 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.

6-2. Configuring the instance

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

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

- *Getting Started Guide*
 - Chapter 3 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*
 - Chapter 5 Notes and Restrictions
 - Before installing EXPRESSCLUSTER

3) Install Python.

Install Python required by EXPRESSCLUSTER.

First, confirm that Python is installed.

If Python has not been installed, install it by using a command such as `yum`.

The installation path of the python commands must be any of the following:

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

4) Install the AWS CLI.

Install the AWS CLI by running the `pip` command from a shell.

```
$ pip install awscli
```

For details about the `pip` command, refer to the following:

<https://pip.pypa.io/en/latest/>

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 Python or 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*
 - Chapter 1 Determining a system configuration
 - 4. 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.

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*
→ Chapter 5 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 (IP monitor resource)

For the settings other than the above, refer to “*Installation and Configuration Guide*”.

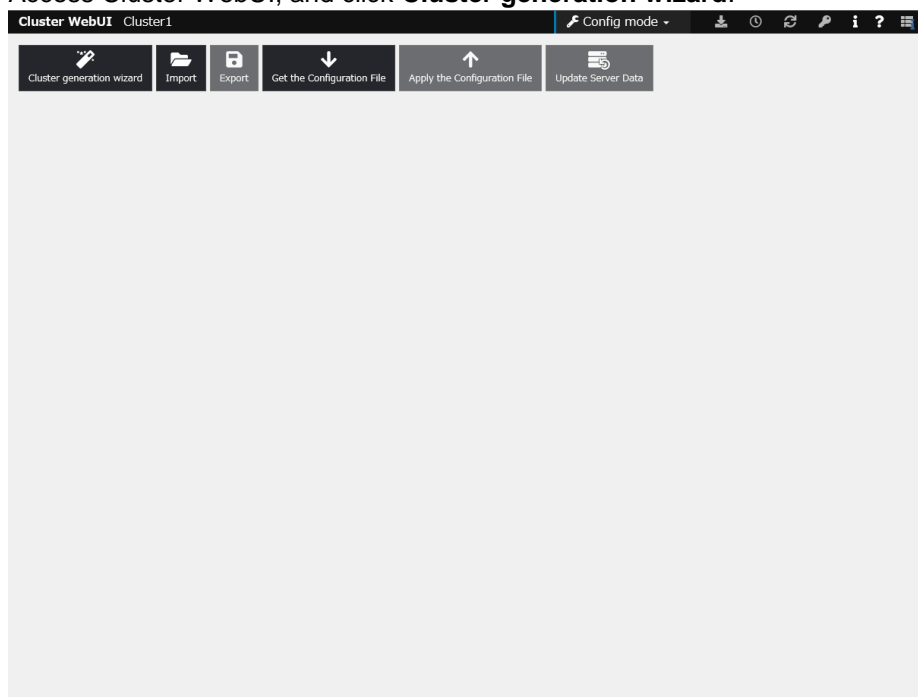
1) Construct a cluster.

Start the Cluster generation wizard to construct a cluster.

- ◇ Construct a cluster.

Steps

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



- 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**.

Cluster generation wizard

Cluster → Basic Settings → Interconnect → NP Resolution → Group → Monitor

Cluster Name*

Comment

Language* English ▼

Management IP Address

Start generating the cluster.
Enter the cluster name, and then select the language (locale) of the environment that runs WebManager.
If using the integrated WebManager to manage multiple clusters, specify a unique cluster name to identify the cluster.
The management IP address is a floating IP address used for a WebManager connection. If establishing connections by specifying each server IP address, the management IP address can be omitted.
To continue, click [Next].

◀ Back Next ▶ Cancel

- 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**.

Cluster generation wizard

Cluster → Basic Settings → Interconnect → NP Resolution → Group → Monitor

Add Remove

Server Definitions

Order	Name
Master server	node1
1	node2

↑ ↓

Server Group Definition Settings

Click "Add" to add servers constructing the cluster.
Click "↑" or "↓" to change the server priority.
Click "Settings" to configure the server group when using the server group.

◀ Back Next ▶ Cancel

- 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**.

Cluster generation wizard

Cluster → Basic Settings → Interconnect → NP Resolution → Group → Monitor

Properties Add Remove

Interconnect List

Priority	Type	MDC	node1	node2
1	Kernel Mode ▼	mdc1 ▼	10.0.110.10 ▼	10.0.120.10 ▼

↑ ↓

Configure the interconnect among the servers constructing the cluster. Click "Add" to add interconnect and select the type.
For "Kernel mode", "User mode", "BMC", "DISK", "Witness HB" and "COM" settings, configure the route which is used for heartbeat. For "Mirror Communication Only" setting, configure the route which is used only for data mirroring communication.
Configuring more than one routes is recommended.
For "Kernel mode", "User mode", "DISK" and "COM" settings, click each server column cell and set an IP address or device.
For "Witness HB" setting, click each server column cell to set "Use" or "Do not use", and then click "Properties" to set detailed settings.
Click "Up" or "Down" to configure the priority to preferentially use the LAN only for the communication among the cluster servers.
For "Mirror Communication Only" settings, click each server column cell to configure IP addresses.
For the communication route which is used for data mirroring communication, select the mirror disk connect name to be allocated to the communication route in MDC column.

◀ Back Next ▶ Cancel

5. The **NP Resolution** window is displayed.
However, the NP resolution is not set on this page. The same operation as the NP resolution can be achieved by adding the IP monitor resource and monitoring a NAT instance set in each AZ. (The NP resolution will be set in “3) **Add a monitor resource.**” described later.)
You need to examine the NP resolution destination and method depending on the location of clients accessing a cluster system and the condition for connecting to an on-premise environment (for example, using a dedicated line). Additionally, you can use network partition resolution resources for 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**.

Group Definition failover ✕

Basic Settings → Startup Servers → Group Attributes → Group Resource

Type* failover ▼

Use Server Group Settings ☐

Name* failover1

Comment

① Select group type.
If using virtual machine resources to cluster virtual machines, select "Virtual machine" as the type. In other cases, select "Failover".
If using server group, check the "Use Server Group".

◀ Back Next ▶ Cancel

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 “6-2 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 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 6-1).

Set a DNS name to be assigned in the **Resource Record Set Name** box (corresponds to [6] in Figure 6-1).

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 6-1).

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.

Resource Definition of Group | failover1 awsdns X

Info ✓ → Dependency ✓ → Recovery Operation ✓ → **Details**

Common node1 node2

Hosted Zone ID*

Resource Record Set Name*

IP Address*

TTL* sec

Delete a record set at deactivation ☒

Tuning

◀ Back Finish Cancel

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 6-1).
 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.

Resource Definition of Group | failover1

Info → Dependency → Recovery Operation → Details

Common node1 node2

Set Up Individually ☒

IP Address 10.0.110.10

Back Finish Cancel

Resource Definition of Group | failover1

Info → Dependency → Recovery Operation → Details

Common node1 node2

Set Up Individually ☒

IP Address 10.0.120.10

Back Finish Cancel

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**.

Monitor Resource Definition

Info → Monitor(common) → Monitor(special) → Recovery Action

Type* AWS AZ monitor

Name* awsazw1

Comment

Get Licence Info

Select the type of monitor resource and enter its name.

Back Next Cancel

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 6-1)

Monitor Resource Definition awsazw

Info → Monitor(common) → **Monitor(special)** → Recovery Action

Common node1 node2

Availability Zone*

Action when AWS CLI command failed to receive response*

◀ Back Next ▶ Cancel

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 6-1). Click **Next**.

Monitor Resource Definition awsazw

Info → Monitor(common) → **Monitor(special)** → Recovery Action

Common node1 node2

Set Up Individually ☒

Availability Zone*

◀ Back Next ▶ Cancel

Monitor Resource Definition awsazw

Info → Monitor(common) → **Monitor(special)** → Recovery Action

Common node1 node2

Set Up Individually ☒

Availability Zone*

◀ Back Next ▶ Cancel

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

Monitor Resource Definition awsazw

Info → Monitor(common) → Monitor(special) → **Recovery Action**

Recovery Action: Custom settings

Recovery Target: LocalServer Browse

Recovery Script Execution Count: 0 time

Execute Script before Reactivation: ☐

Maximum Reactivation Count: 0 time

Execute Script before Failover: ☐

Execute migration before Failover: ☐

Maximum Failover Count: 0 time

Execute Script before Final Action: ☐

Final Action: No operation

Script Settings

Back Finish Cancel

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

◇ AWS DNS monitor resource

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

Using the OS API and the AWS CLI commands, check the existence of the resource record set and whether 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

◇ IP monitor resource

Create the IP monitor resource to monitor the health of the subnet by sending a ping to a NAT instance placed in each AZ. Specify the following:

Steps

1. Click **Add** in **Monitor Resource List**.

2. Select the monitor resource type (IP monitor) from the **Type** box and enter the monitor resource name (ipw1) in the **Name** box. Click **Next**.

Monitor Resource Definition ipw ✕

Info → Monitor(common) → Monitor(special) → Recovery Action

Type*

Name*

Comment

❗ Select the type of monitor resource and enter its name.

3. The **Monitor (common)** window is displayed. Confirm that **Monitoring Timing** is **Always** and click **Next**.
4. The **Monitor (special)** window is displayed. Enter the private IP address of the NAT instance used by each node in the **IP Address** box of the **Common** tab (corresponds to [4] and [5] in Figure 6-1). Click **Next**.

Monitor Resource Definition ipw ✕

Info ✓ → Monitor(common) ✓ → **Monitor(special)** → Recovery Action

Common node1 node2

IP Address List

IP Address
10.0.10.100
10.0.20.100

5. The **Recovery Action** window is displayed.
Set LocalServer in the **Recovery Target** box.
Select **Stop the cluster service and shutdown OS** in **Final Action**.

The screenshot shows the 'Monitor Resource Definition' window with the 'Recovery Action' tab selected. The breadcrumb trail at the top is 'Info' → 'Monitor(common)' → 'Monitor(special)' → 'Recovery Action'. The 'Recovery Action' dropdown is set to 'Custom settings'. The 'Recovery Target' is 'LocalServer' with a 'Browse' button. The 'Recovery Script Execution Count' is '0' with a 'time' unit. The 'Execute Script before Reactivation' checkbox is unchecked, and the 'Maximum Reactivation Count' is '0' with a 'time' unit. The 'Execute Script before Failover' checkbox is unchecked, and the 'Execute migration before Failover' checkbox is also unchecked. The 'Maximum Failover Count' is '0' with a 'time' unit. The 'Execute Script before Final Action' checkbox is unchecked. The 'Final Action' dropdown is set to 'Stop the cluster service and shutdown OS'. There is a 'Script Settings' button and 'Back', 'Finish', and 'Cancel' buttons at the bottom right.

Monitor Resource Definition ipw

Info → Monitor(common) → Monitor(special) → **Recovery Action**

Recovery Action Custom settings

Recovery Target * LocalServer Browse

Recovery Script Execution Count* 0 time

Execute Script before Reactivation ☐

Maximum Reactivation Count 0 time

Execute Script before Failover ☐

Execute migration before Failover ☐

Maximum Failover Count 0 time

Execute Script before Final Action ☐

Final Action Stop the cluster service and shutdown OS

Script Settings

Back Finish Cancel

6. Click **Finish** to complete setting.

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 7 Configuring the IAM

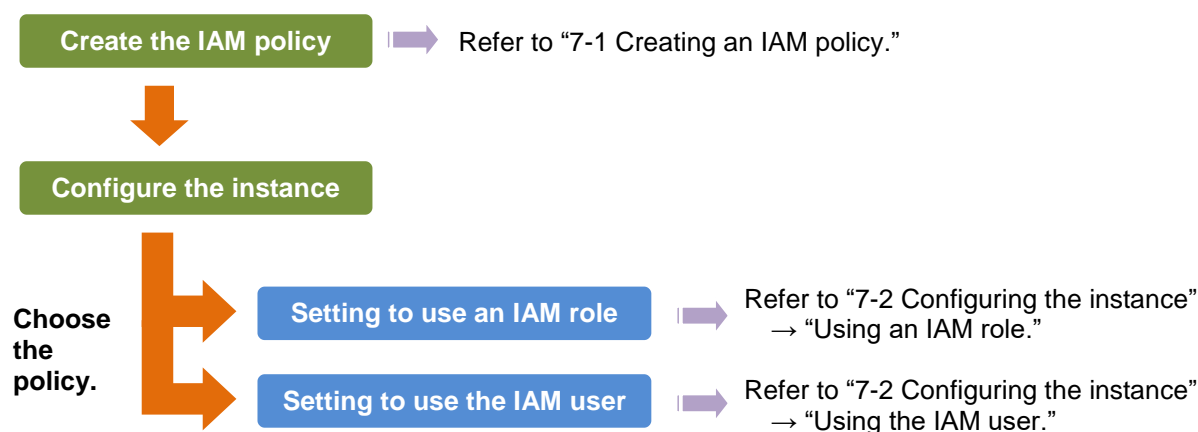
This chapter describes the Identity & Access Management (IAM) settings in the AWS environment. For the resource and monitor resources such as the AWS Virtual IP resource, the AWS CLI is run in a resource to process the resource itself. To run the AWS CLI correctly, it is required to configure the IAM in advance.

There are two methods to grant access permissions to the AWS CLI: the policy to use an IAM role and the policy to use an IAM user. NEC recommends the policy to use an IAM role because it is unnecessary to store the AWS access key ID and AWS secret access key in each instance in principle, enhancing the security.

The following table describes the advantages and disadvantages of both policies.

	Advantages	Disadvantages
Policy to use an IAM role	High security Easy to manage key information.	None.
Policy to use an IAM user	Available to set access permissions to an individual instance later	High risk of key information disclosure Complicated to manage key information

The procedure to configure the IAM is as follows:



7-1. Creating an IAM policy

Create a policy in which access permissions granted to the actions for the services such as EC2 and S3 of AWS are described. Access permissions need to be granted to the following actions so that the AWS related resources and monitor resources of EXPRESSCLUSTER run the AWS CLI.

[The required policies may be changed in future.](#)

- ◇ AWS Virtual IP resource and AWS Virtual IP monitor resource

Action	Description
ec2:Describe*	Required to obtain information of a VPC, route table, and network interface.
ec2:ReplaceRoute	Required to update a route table.

- ◇ AWS Elastic IP resource and AWS Elastic IP monitor resource

Action	Description
ec2:Describe*	Required to obtain information of an EIP and network interface.
ec2:AssociateAddress	Required to assign an EIP to an ENI.
ec2:DisassociateAddress	Required to deassign an EIP from an ENI.

- ◇ AWS DNS resource/AWS DNS monitor resource

Action	Description
Route 53:ChangeResourceRecordSets	Required to add/delete a resource record set and update the setting details.
Route 53:ListResourceRecordSets	Required to obtain the information of a resource record set.

- ◇ AWS AZ monitor resource

Action	Description
ec2:Describe*	Required to obtain information of an AZ.

In the following custom policy example, access permissions are granted to all actions to be used by the AWS-related resources and monitor resources.

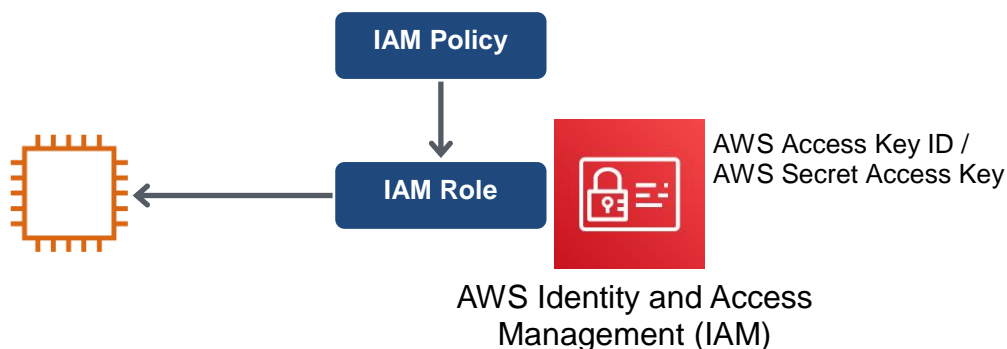
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:Describe*",
        "ec2:ReplaceRoute",
        "ec2:AssociateAddress",
        "ec2:DisassociateAddress",
        "route53:ChangeResourceRecordSets",
        "route53:ListResourceRecordSets"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

→ To create a custom policy, select **Policies > Create Policy** on the IAM Management console.

7-2. Configuring the instance

Using an IAM role

Create an IAM role and assign the created IAM role to an instance to run the AWS CLI.



- 1) Create an IAM role. Attach the IAM policy to the created role.

→ To create an IAM role, select **Roles > Create New Role** on the IAM Management console.

- 2) When creating an instance, specify the created IAM role for **IAM Role**.
(The IAM role cannot be assigned to the created instance later.)

- 3) Log on to the instance.

- 4) Install Python.

Install Python required by EXPRESSCLUSTER.

First, confirm that Python is installed.

If Python has not been installed, install it by using a command such as yum.

The installation path of the python commands must be any of the following:

/sbin, /bin, /usr/sbin, /usr/bin

- 5) Install the AWS CLI.

Install the AWS CLI by running the pip command from a shell.

```
$ pip install awscli
```

For details about the pip command, refer to the following:

<https://pip.pypa.io/en/latest/>

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 Python or the AWS CLI, be sure to restart the OS before using EXPRESSCLUSTER.)

- 6) Run the following command from the shell.

```
$ sudo aws configure
```

Enter information such as the AWS access key to the inquiries.

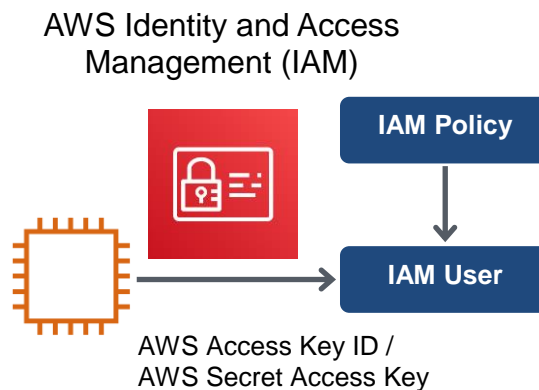
The settings to be specified vary depending on whether an IAM role is assigned to the instance or not.

```
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
```

If you specified incorrect settings, delete the directory `/root/.aws` entirely, and specify the above settings again.

Using an IAM user

Create an IAM user and store the access key ID and secret access key of the created user in an instance to run the AWS CLI. It is not required to assign the created IAM role to an instance to be created.



- 1) Create an IAM user. Attach the IAM policy to the created user.

→ To create an IAM user, select **Users > Create New Users** on the IAM Management console.

- 2) Log on to the instance.

- 3) Install Python.

Install Python required by EXPRESSCLUSTER.

First, confirm that Python is installed.

If Python has not been installed, install it by using a command such as `yum`.

The installation path of the python commands must be any of the following:

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

- 4) Install the AWS CLI.

Install the AWS CLI by running the `pip` command from a shell.

```
$ pip install awscli
```

For details about the `pip` command, refer to the following:

<https://pip.pypa.io/en/latest/>

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:
<http://docs.aws.amazon.com/cli/latest/userguide/installing.html>

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

- 5) Run the following command from the shell.

```
$ sudo aws configure
```

Enter the information required to run the AWS CLI to the inquiries. For the AWS access key ID and AWS secret access key, enter those obtained from the IAM user detailed information window.

```
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
```

If you specified incorrect settings, delete the directory `/root/.aws` entirely, and specify the above settings again.

Chapter 8 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, Python and 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 Python and the AWS CLI. In this case, restart the OS again.
- ◆ Failed to start the AWS Virtual IP resource.

Cluster WebUI message	Activating <i>awsvip1</i> resource has failed.(99 : Internal error. (status= <i>nn</i>))
Possible cause	Any of the following might be the cause. ◆ Python has not been installed, or the path does not reach python. ◆ The AWS CLI has not been installed, or the path does not reach AWS CLI.
Solution	Confirm that Python and the AWS CLI are installed. The installation path of the python commands must be any of the following: /sbin, /bin, /usr/sbin, /usr/bin 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 <i>awsvip1</i> resource has failed.(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. (<i>aws configure</i> has not been run.) ◆ The AWS CLI configuration file could not be found. (A user other than root ran <i>aws configure</i> , or A user without <i>sudo</i> ran <i>aws configure</i> .) 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. ◆ The specified VPC ID or ENI ID is invalid.
Solution	Confirm that the AWS CLI works normally. Correct the above mentioned settings.

Cluster WebUI message	Activating <i>awsvip1</i> resource has failed.(5 : The vpc ID ' <i>vpc-xxxxxxx</i> ' 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 <i>awsvip1</i> resource has failed.(5 : The networkInterface ID ' <i>eni-xxxxxxx</i> ' 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 <i>awsvip1</i> resource has failed.(6 : Timeout occurred.)
Possible cause	The AWS CLI command might not be able to communicate with the regional endpoint.
Solution	Check the following: <ul style="list-style-type: none"> ◆ The instance for NAT is running. ◆ The routing for the NAT instance has been set up. ◆ The packet is not excluded by filtering.

Cluster WebUI message	Activating <i>awsvip1</i> resource has failed.(7 : The VIP address <i>vvv.www.xxx.yyy</i> 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 <i>awsvipw1</i> . (8 : The routing for VIP <i>vvv.www.xxx.yyy</i> 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 <i>awseip1</i> resource has failed.(99 : Internal error. (status= <i>nn</i>))
Possible cause	Any of the following might be the cause. <ul style="list-style-type: none"> ◆ Python has not been installed, or the path does not reach <code>python</code>. ◆ The AWS CLI has not been installed, or the path does not reach AWS CLI.
Solution	Confirm that Python and the AWS CLI are installed. The installation path of the python commands must be any of the following: <code>/sbin, /bin, /usr/sbin, /usr/bin</code> The installation path of the AWS CLI must be any of the following: <code>/sbin, /bin, /usr/sbin, /usr/bin, /usr/local/bin</code>

Cluster WebUI message	Activating <i>awseip1</i> resource has failed.(5 : Failed in the AWS CLI command.)
-----------------------	--

Possible cause	Any of the following might be the cause. <ul style="list-style-type: none"> ◆ The AWS CLI has not been set up. (<code>aws configure</code> has not been run.) ◆ The AWS CLI configuration file could not be found. (A user other than root ran <code>aws configure</code>, or A user without <code>sudo</code> ran <code>aws configure</code>.) 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) <code>\$HOME/.aws</code> follower 2) <code>/root/.aws</code> 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. ◆ The specified EIP Allocation ID or ENI ID is invalid.
Solution	Confirm that the AWS CLI works normally. Correct the above mentioned settings.

Cluster WebUI message	Activating <i>awseip1</i> resource has failed.(5 : The allocation ID ' <i>eipalloc-xxxxxxx</i> ' 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 <i>awseip1</i> resource has failed.(5 : The networkInterface ID ' <i>eni-xxxxxxx</i> ' 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 <i>awseip1</i> resource has failed.(6 : Timeout occurred.)
Possible cause	The AWS CLI command might not be able to communicate with the regional endpoint.
Solution	Confirm that a public IP is assigned to each instance. Confirm that the AWS CLI works normally in each instance.

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

Cluster WebUI message	Detected an error in monitoring <i>awseipw1</i> . (7 : The EIP address does not exist. (EIP ALLOCATION ID= <i>eipalloc-xxxxxxx</i>))
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 <i>awsdns1</i> resource has failed.(99 : Internal error. (status= <i>nn</i>))
Possible cause	Any of the following might be the cause: <ul style="list-style-type: none"> ◆ Python has not been installed, or the path does not reach python. ◆ The AWS CLI has not been installed, or the path does not reach AWS CLI.

Solution	Confirm that Python or the AWS CLI are installed. The installation path of the python commands must be any of the following: /sbin, /bin, /usr/sbin, /usr/bin 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 <i>awsdns1</i> resource has failed. (5 : Failed in the AWS CLI command.)
Possible cause	Any of the following might be the cause: <ul style="list-style-type: none"> ◆ 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 IAM user is to be used, search for a credentials or config file by the following step: <ol style="list-style-type: none"> 1) Under <\$HOME/.aws> 2) Under </root/.aws> <ul style="list-style-type: none"> ◆ 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) ◆ The specified resource record set is invalid.
Solution	Confirm if AWS CLI works normally. Check and correct the settings mentioned above.

Cluster WebUI message	Activating <i>awsdns1</i> resource has failed. (5 : 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 <i>awsdns1</i> resource has failed (6: Timeout occurred.)
Possible cause	The AWS CLI command might not be able to communicate with the regional endpoint.
Solution	Check the following: <ul style="list-style-type: none"> ◆ If the NAT instance is running. ◆ If the routing for the NAT has been configured properly. ◆ If the packets are not blocked by filtering.

- ◆ The AWS DNS monitor resource enters the error state.

Cluster WebUI message	Detected an error in monitoring <i>awsdns1</i> . (7 : The resource record set in Amazon Route 53 does not exist.)
Possible cause	In the Host Zone, the resource record set corresponding to the AWS DNS resource has been deleted 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 <i>awsdns1</i> . (8: 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 <i>awsdns1</i> . (9 : 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: <ul style="list-style-type: none"> ◆ 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 <i>awsdns1</i> . (10 : IP address which is resolved domain name from the DNS resolver does not match 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: <ul style="list-style-type: none"> ◆ If the resolver setting is correct. ◆ If there are no entries related to the DNS name in the hosts file.

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

Cluster WebUI message	[Warning] Warn monitoring <i>awsazw1</i> . (105 : Failed in the AWS CLI command.) [Error] Detected an error in monitoring <i>awsazw1</i> . (5 : Failed in the AWS CLI command.)
Possible cause	Any of the following might be the cause. <ul style="list-style-type: none"> ◆ The AWS CLI has not been set up. (<i>aws configure</i> has not been run.) ◆ The AWS CLI configuration file could not be found. (A user other than root ran <i>aws configure</i>, or A user without sudo ran <i>aws configure</i>.) Search for a credentials file and a config file by the following order (in case of policy for which the IAM user is used). <ol style="list-style-type: none"> 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. ◆ The specified AZ is invalid.
Solution	Confirm that the AWS CLI works normally. Correct the above mentioned settings.

Cluster WebUI message	[Warning] Warn monitoring <i>awsazw1</i> . (105 : Invalid availability zone: [<i>ap-northeast-1x</i>]) [Error] Detected an error in monitoring <i>awsazw1</i> . (5 : Invalid availability zone: [<i>ap-northeast-1x</i>])
Possible cause	The specified AZ might not be correct or might not exist.
Solution	Specify a correct AZ.

Cluster WebUI message	<p>[Warning] Warn monitoring <i>awsazw1</i>. (106 : Timeout occurred.)</p> <p>[Error] Detected an error in monitoring <i>awsazw1</i>. (6 : Timeout occurred.)</p>
Possible cause	The AWS CLI command might not be able to communicate with the regional endpoint because the route table of the NAT setting is incorrect and so on.
Solution	<p>Check the following:</p> <ul style="list-style-type: none"> ◆ The NAT instance is running. ◆ The routing for the NAT instance has been set up. ◆ The packet is not excluded by filtering.