EXPRESSCLUSTER X 6.0
HA Cluster Configuration Guide for Google Cloud (Windows)

Release 1

NEC Corporation

Apr 08, 2026

TABLE OF CONTENTS:

1 Preface **1**
- 1.1 Who Should Use This Guide . . . 1
- 1.2 Scope of application . . . 2
- 1.3 How This Guide is Organized . . . 3
- 1.4 EXPRESSCLUSTER X Documentation Set . . . 4
- 1.5 Conventions . . . 5
- 1.6 Contacting NEC . . . 6

2 Overview **7**
- 2.1 Functional overview . . . 7
- 2.2 Basic configuration . . . 8
- 2.3 Network partition resolution . . . 13
- 2.4 Differences between on-premises and Google Cloud . . . 14

3 Operating Environments **15**

4 Cluster Creation Procedure (for an HA Cluster with an Internal TCP Load Balancer) **17**
- 4.1 Creation example . . . 17
- 4.2 Configuring Google Cloud . . . 21
- 4.3 Configuring EXPRESSCLUSTER . . . 23
- 4.4 Verifying the created environment . . . 26

5 Cluster Creation Procedure (for an HA Cluster with Cloud DNS) **27**
- 5.1 Creation examples . . . 27
- 5.2 Configuring Google Cloud . . . 30
- 5.3 Configuring EXPRESSCLUSTER . . . 32
- 5.4 Verifying the operations . . . 35

6 Error Messages **37**

7 Notes and Restrictions **39**
- 7.1 HA cluster with a load balancer . . . 39
- 7.2 HA cluster with Cloud DNS . . . 40
- 7.3 Shared disk/hybrid disk type cluster . . . 41

8 Legal Notice **43**
- 8.1 Disclaimer . . . 43
- 8.2 Trademark Information . . . 44

9 Revision History **45**

CHAPTER

ONE

PREFACE

1.1 Who Should Use This Guide

The *HA Cluster Configuration Guide for Google Cloud (Windows)* is intended for administrators who want to build a cluster system, and for system engineers and maintenance personnel who provide user support.

The software and setup examples introduced in this guide are for reference only, and the software is not guaranteed to run.

1.2 Scope of application

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

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

1.3 How This Guide is Organized

- "2. *Overview* ": Describes the functional overview.
- "3. *Operating Environments* ": Describes the tested operating environment of this function.
- "4. *Cluster Creation Procedure (for an HA Cluster with an Internal TCP Load Balancer)*": Describes how to create an HA cluster involving an internal TCP load balancer.
- "5. *Cluster Creation Procedure (for an HA Cluster with Cloud DNS)* ": Describes how to create an HA cluster involving Cloud DNS.
- "6. *Error Messages*": Describes the error messages and solutions.
- "7. *Notes and Restrictions* ": Describes the notes and restrictions on creating and operating a cluster.

1.4 EXPRESSCLUSTER X Documentation Set

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

EXPRESSCLUSTER X Getting Started Guide

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

EXPRESSCLUSTER X Installation and Configuration Guide

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

EXPRESSCLUSTER X Reference Guide

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

EXPRESSCLUSTER X Maintenance Guide

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

1.5 Conventions

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

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

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

See also:

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

The following conventions are used in this guide.

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


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

1.6 Contacting NEC

For the latest product information, visit our website below:

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

CHAPTER

TWO

OVERVIEW

2.1 Functional overview

This guide describes how to create an HA cluster based on EXPRESSCLUSTER X (EXPRESSCLUSTER) on the cloud service of Google Cloud.
Google Cloud allows you to use regions and zones to create an HA cluster with virtual machines, increasing the business availability.

- Region

  On Google Cloud, a region is a division: a physical and logical unit (like New York and London).
  It is possible to build all nodes in a single region. However, a network failure or a natural disaster may make all of them crash to prevent the business from continuing.
  To increase availability, distribute nodes to multiple regions.
  A region is a group of zones.

- Zone

  On Google Cloud, a zone is a logical group to which each node can be distributed.
  By distributing each node to a different zone, you can minimize the effects of planned Google Cloud maintenance and those of unplanned maintenance due to a physical hardware failure.

For more information on regions and zones, refer to the following:
https://cloud.google.com/compute/docs/regions-zones/

2.2 Basic configuration

This guide assumes an HA cluster (uni-directional standby cluster configuration) with a load balancer.
For the HA cluster, the following EXPRESSCLUSTER resource and Google Cloud service are to be used:

Purpose	EXPRESSCLUSTER resource to be chosen	Necessary Google Cloud service
Accessing the cluster at a virtual/internal IP address from a client	LB probe port resource	Internal TCP load balancing
Accessing the cluster in a DNS name from a client	Google Cloud DNS resource	Cloud DNS

HA cluster with a load balancer

For virtual machines in a Google Cloud environment, client applications can use a virtual IP (VIP) address to access nodes that constitute a cluster. Using the VIP address eliminates the need for the clients to be aware of switching between the virtual machines even after a failover or a group migration occurs.

As Fig. 2.1 HA cluster with an internal TCP load balancer shows, the cluster in the Google Cloud environment can be accessed by specifying the VIP address (front-end IP address for Cloud Load Balancing) of the Google Cloud load balancer (for Cloud Load Balancing).

The Google Cloud load balancer switches between the active server and the standby server, with its health check. The health check is performed through a port provided by the LB probe port resource.

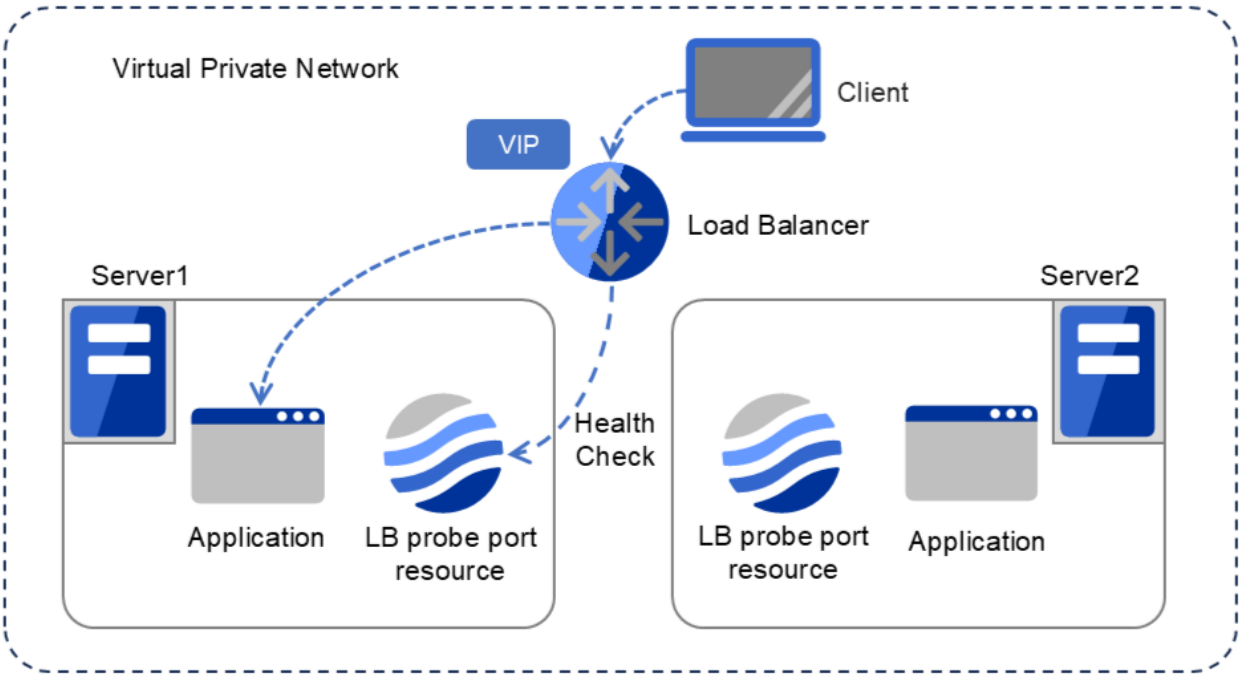

Fig. 2.1: HA cluster with an internal TCP load balancer

SubNetwork-1	10.0.1.0/24
IP Address (Client)	10.0.1.200
Virtual IP Address (VIP)	10.0.1.100
SubNetwork-11	10.0.11.0/24
IP Address (Server1)	10.0.11.101
IP Address (Server2)	10.0.11.102
Health Check Port	12345

For more information on Cloud Load Balancing, refer to the following:
https://cloud.google.com/load-balancing/

The following is an example of an HA cluster with a load balancer:

Purpose	Load balancer to be used	Creation procedure
Sharing business within the Google Cloud network	Internal TCP load balancer	See "4. *Cluster Creation Procedure (for an HA Cluster with an Internal TCP Load Balancer)*" of this guide.

An HA cluster configuration with a load balancer requires the following resources and monitor resources.

Resource/monitor resource	Description	Setting
LB probe port resource	Provides a mechanism for awaiting access from the load balancer to a specific port for the alive monitoring (health check)--over the port, an application works on a node. At activation, this resource starts up a control process to await access from the Google Cloud load balancer for its alive monitoring. At deactivation, the resource stops the control process.	Required

continues on next page

Table 2.4 – continued from previous page

Resource/monitor resource	Description	Setting
LB probe port monitor resource	Performs alive monitoring of a control process to be started in activating a LB probe port resource, for the node where the LB probe port resource is started. Checks whether the same port as that for the health check is opened, for a node where the LB probe port resource is not started.	Required
Network Partition Resolution resource	Please refer to *Network partition resolution*.	Recommendation
Other resources and monitor resources	Depends on the configuration of the application (such as a mirror disk) to be used in the HA cluster.	Optional

HA cluster with Cloud DNS

This configuration uses Cloud DNS to make an HA cluster accessible via a DNS name.

Each of the two virtual machines is placed in a different zone in order to minimize the effects of planned Google Cloud maintenance and those of unplanned maintenance due to a physical hardware failure.

In Fig. 2.2 HA cluster with Cloud DNS, the cluster can be accessed by specifying its DNS name.

EXPRESSCLUSTER manages the record sets (A records) of Cloud DNS so that a given IP address can be found according to the DNS name.

This eliminates the need for the client to be aware of switching between the virtual machines even after a failover or a group migration occurs.

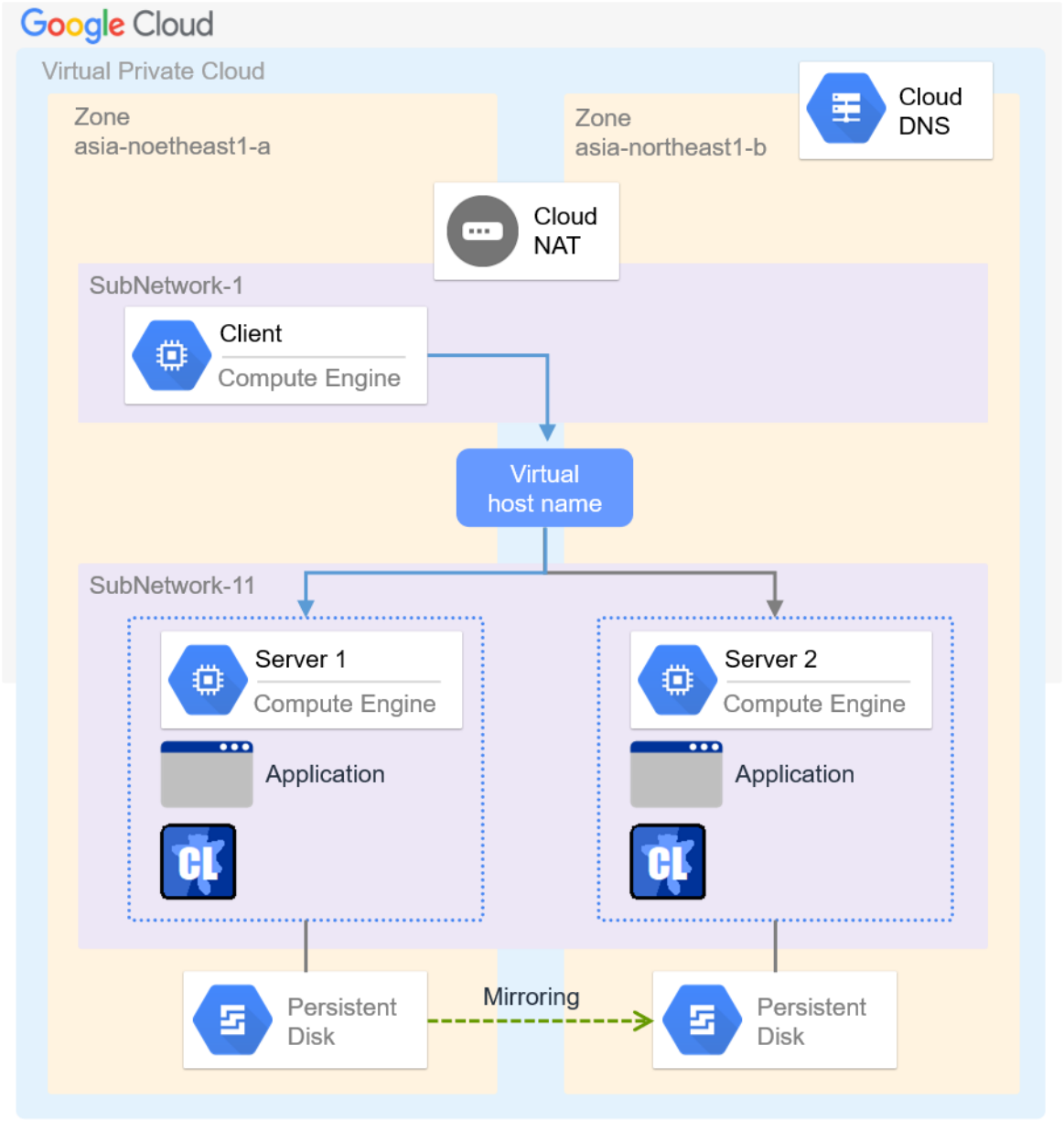

Fig. 2.2: HA cluster with Cloud DNS

SubNetwork-1	10.0.1.0/24
IP Address (Client)	10.0.1.200
SubNetwork-11	10.0.11.0/24
IP Address (Server1)	10.0.11.101
IP Address (Server2)	10.0.11.102
Virtual host name	test-cluster.example.com

1. Before updating the record (Cloud DNS)

Name	Type	Data
test-cluster.example.com	A	10.0.11.101

2. After updating the record (Cloud DNS)

Name	Type	Data
test-cluster.example.com	A	10.0.11.102

This guide describes a configuration in which instances constituting the HA cluster within the VPC network can access the Internet.

The instances need to access the Internet when executing the gcloud CLI used with a script for Cloud DNS.

The Internet can be accessed through a NAT gateway or a NAT instance. This guide uses the former (Cloud NAT).

For more information on the procedures for creating the VPC network, configuring the NAT gateway/NAT instance, and configuring the firewall rules, refer to the documents of Google Cloud.

An HA cluster configuration with Cloud DNS requires the following resources and monitor resources.

Resource or monitor resource type	Description	Setting
Google Cloud DNS resource	Manages the record sets (A records) of Cloud DNS so that a given IP address can be found according to the DNS name.	Required
Google Cloud DNS monitor resource	Checks that Google Cloud DNS has the record sets (A records) controlled by the Google Cloud DNS resource specified as the target resource for monitoring at activation.	Required
Network partition resolution	Please refer to *Network partition resolution*.	Recommendation
Other resources and monitor resources	Depends on the configuration of applications, such as mirror disks or shared disks, which are used in an HA cluster.	Optional

2.3 Network partition resolution

Virtual machines constituting an HA cluster mutually perform alive monitoring with heartbeat.
If heartbeat ceases with each virtual machine existing on a different subnet, an undesirable event (such as double-launching a service) occurs.
Its prevention requires determining whether any of the virtual machines has been isolated from the network, in a network partition (NP) state, or another virtual machine has crashed.

An NP state is determined to have occurred when there is no response to a check with such a method as HTTP or Ping from a constantly running device (response destination). In this case, a specified action (e.g., warning, recovery processing, or a server shutdown) is performed. This mechanism is called network partition resolution (hereinafter called NP resolution).
The following are examples of NP resolution configurations:

- Configuration 1: HTTP NP resolution resource + Witness server service (compute instance)
- Configuration 2: HTTP NP resolution resource + Cloud Storage (static website hosting)
- Configuration 3: PING NP resolution resource + ICMP response server (compute instance)

	Advantage	Disadvantage
Configuration 1	The communication path for the heartbeat is the same as that for the NP resolution resource, ensuring high reliability of NP resolution.	Requires preparing an additional instance. Requires setting up the Witness server service.
Configuration 2	No need to prepare an additional instance.	The communication path for the heartbeat may differ from that for the NP resolution resource; therefore the reliability of NP resolution is lower than that in Configuration 1.
Configuration 3	No need to set up the Witness server service.	Requires preparing an additional instance.

The target and method of NP resolution needs to be individually considered, in accordance with the locations of clients accessing the cluster system and with the conditions for connecting to an on-premise environment (e.g. using a leased line).
For details on the heartbeat resource and NP resolution, refer to the following:

- "Installation and Configuration Guide" -> "Understanding network partition resolution resources"
- "Reference Guide" -> "Heartbeat resources"
- "Reference Guide" -> "Details on network partition resolution resources"

2.4 Differences between on-premises and Google Cloud

The following table describes the functional differences of EXPRESSCLUSTER between on-premises and Google Cloud. "✓" indicates that the relevant function can be used and "n/a" indicates that the relevant function cannot be used.

Function	On-premise	Google Cloud
Creating a shared disk type cluster	✓	✓[1]
Creating a mirror disk type cluster	✓	✓
Using the management group	✓	n/a
Using the floating IP resource	✓	n/a
Using the virtual IP resource	✓	n/a
Using the virtual computer name resource	✓	n/a
Using the LB probe port resource	n/a	✓
Using the Google Cloud DNS resource	n/a	✓

There is no difference in the procedure for creating a cluster between an on-premise environment and an Google Cloud environment except that Google Cloud needs to be configured in advance.

[1] Depending on the controller and volume type of the shared disk, it may not work properly. For details, refer to "7. *Notes and Restrictions*".

CHAPTER

THREE

OPERATING ENVIRONMENTS

Refer to the following:

- "EXPRESSCLUSTER X Getting Started Guide" > "Installation requirements for EXPRESSCLUSTER" > "System requirements for the EXPRESSCLUSTER Server" > "Operation environments for Google Cloud DNS resource, Google Cloud DNS monitor resource"

CHAPTER

FOUR

CLUSTER CREATION PROCEDURE (FOR AN HA CLUSTER WITH AN INTERNAL TCP LOAD BALANCER)

4.1 Creation example

This guide describes how to create a two-node, uni-directional standby cluster with EXPRESSCLUSTER.
Through this procedure, you are to create an HA cluster accessible from clients within the same VPC network on Google Cloud.
This procedure is intended to create a mirror-disk type configuration in which server1 is used as the active server.

The following tables list parameters which do not have their default values, and parameters whose values are changed from their default values.
Of the firewall rules, **IP range** is necessary for allowing communication from the Google Cloud health check system (130.211.0.0/22, 35.191.0.0/16).

- Google Cloud settings (common to server1 and server2)

Item	Value
Configuration of the VPC network	
– Name	test-vpc
– New subnet (name)	subnetwork-1, subnetwork-11
– New subnet (region)	asia-northeast1
– New subnet (IP address range)	10.0.1.0/24, 10.0.11.0/24
Configuration of the firewall rules	
– Name	test-allow-health-check
– Network	test-vpc

continues on next page

Table 4.1 – continued from previous page

Item	Value
– Traffic direction	Upstream
– Action in response to agreement	Allow
– Target	Specified target tag
– Target tag	test-allow-health-check
– Source filter	IP range
– Source IP range	130.211.0.0/22, 35.191.0.0/16
– Specified protocol and port	Allow all
Configuration of the load balancer	
– Type	TCP load balancing
– For internet connection or private use	Only between VMs
– Multi- or mono-region	Only mono-region
– Name	test-lb
Configuration of the load balancer (back end)	
– Region	asia-northeast1
– Network	test-vpc
– Instance group	test-ig-a, test-ig-b
– Health check (name)	test-health-check
– Health check (protocol)	TCP
– Health check (port)	12345
– Health check (proxy protocol)	None
– Session affinity	None

continues on next page

Table 4.1 – continued from previous page

Item	Value
Configuration of the load balancer (front end)	
– Name	test-frontend
– Subnetwork	subnetwork-1
– Internal IP address	10.0.1.100
– Port	80 (number of the port through which the application is available)

- Google Cloud settings (to be set separately on server1 and server2)

Item	Value server1	server2
Configuration of the instances		
– Region	asia-northeast1	asia-northeast1
– Zone	asia-northeast1-a	asia-northeast1-b
– New disk	server1-datadisk-0	server2-datadisk-0
Configuration of the instance groups		
– Name	test-ig-a	test-ig-b
– Group type	Unmanaged instance group	Unmanaged instance group
– Region	asia-northeast1	asia-northeast1
– Zone	asia-northeast1-a	asia-northeast1-b
– Network	test-vpc	test-vpc
– Subnetwork	subnetwork-11	subnetwork-11
– VM instance	server1	server2
Network configuration		
– Network	test-vpc	test-vpc

continues on next page

Table 4.2 – continued from previous page

Item	Value server1	server2
– Subnetwork	subnetwork-11	subnetwork-11
– Internal IP address	10.0.11.101	10.0.11.102

- EXPRESSCLUSTER settings (cluster properties)

Item	Value server1	server2
– Cluster name	Cluster1	Cluster1
– Server name	server1	server2

- EXPRESSCLUSTER settings (failover group)

Resource name	Item	Value
Mirror disk resource	Resource name	md
Mirror disk resource	**Details** tab - drive letter of the data partition	G:
Mirror disk resource	**Details** tab - drive letter of the cluster partition	F:
LB probe port resource	Resource name	lbpp1
LB probe port resource	Port number	12345: as specified for **Health check (port)**

- EXPRESSCLUSTER settings (monitor resource)

Monitor resource name	Item	Value
Mirror disk monitor resource	Monitor resource name	mdw1
LB probe port monitor resource	Monitor resource name	lbppw1
LB probe port monitor resource	Recovery target	lbpp1

4.2 Configuring Google Cloud

1. **Creating the VPC network**

   Access Google Cloud Console (https://console.cloud.google.com/).
   Create the VPC network and subnets.
   For more information on the procedure, refer to the following:
   https://cloud.google.com/vpc/docs/using-vpc/

2. **Creating the instances**

   Create each of the instances based on a public image.
   During this creation, add a secondary disk for the mirror disk (cluster partition and data partition).
   Create as many instances as the number of virtual machines constituting the cluster.
   For more information on the procedure, refer to the following:
   https://cloud.google.com/compute/docs/how-to/

3. **Configuring the instances**

   Access and log in to the created instances (server1 and server2).
   For more information on the procedure, refer to the following:
   https://cloud.google.com/compute/docs/instances/connecting-to-instance/

   Next, set the partitions for the mirror disk resource.
   Create the cluster partition and data partition on the secondary disk added to the instance.
   For more information on setting the partitions for the mirror disk resource, refer to the following:
   - "Installation and Configuration Guide" -> "Determining a system configuration" -> "Settings after configuring hardware" -> "Mirror partition settings (Required for mirror disks)"

4. **Creating the firewall rules**

   Create the firewall rules for allowing communication from the Google Cloud health check system (130.211.0.0/22, 35.191.0.0/16), where the health check is to be performed by the load balancer to the instance.
   In addition, add the target tag to the network tag of the instances (server1 and server2).
   For more information on the procedure, refer to the following:
   Using firewall rules:
   https://cloud.google.com/vpc/docs/using-firewalls/
   Creating health checks:
   https://cloud.google.com/load-balancing/docs/health-checks/

5. **Creating the instance groups**

   Create the instance groups to be specified as the back ends of Cloud Load Balancing. To the group, add the instances (server1 and server2).
   For more information on the procedure, refer to the following:
   https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-unmanaged-instances

6. **Creating the load balancer**

   Create the load balancer. Select **TCP Load Balancing**.
   For more information on the procedure, refer to the following:
   https://cloud.google.com/load-balancing/docs/network/setting-up-network/

Next, configure the back end and the front end.

For **Ports** of the front end, specify the number of the port through which the application is available.

For more information on the procedure, refer to the following:

https://cloud.google.com/load-balancing/docs/internal/setting-up-internal

7. **Adjusting the EXPRESSCLUSTER service startup time, verifying the network settings, verifying the firewall settings, synchronizing the server clock, and turning off the power-saving function**

   For information on each of the procedures, refer to the following:

   - "Installation and Configuration Guide" -> "Determining a system configuration" -> "Settings after configuring hardware"

8. **Installing EXPRESSCLUSTER**

   For information on the procedure, refer to the following document. After completing the installation, reboot the OS.

   - "Installation and Configuration Guide"

9. **Registering the EXPRESSCLUSTER license**

   For information on the procedure, refer to the following document:

   - "Installation and Configuration Guide"

4.3 Configuring EXPRESSCLUSTER

For information on how to set up and access Cluster WebUI, refer to the following:

- "Installation and Configuration Guide" -> "Creating the cluster configuration data"

This section describes how to add the following resources and monitor resources:

- Mirror disk resource
- LB probe port resource
- LB probe port monitor resource

For information on other settings, refer to the following:

- "Installation and Configuration Guide"
- "Reference Guide"

1. **Creating a cluster**

   To create a cluster, start the cluster generation wizard first.

   - Creating a cluster

     1. Access Cluster WebUI, and click **Cluster generation wizard**.
     2. **Cluster** of **Cluster generation wizard** is displayed.
        Enter a desired name in **Cluster Name**.
        Select an appropriate language in **Language**. Click **Next**.
     3. **Basic Settings** is displayed.
        The instance connected to Cluster WebUI is displayed as a registered master server.
        Click **Add** to add the remaining instances (by specifying the private IP address of each instance). Click **Next**.
     4. The **Interconnect** window is displayed.
        Specify the IP addresses (the private IP address of each instance) to be used for interconnect, and a Witness heartbeat.
        For **MDC**, select mdc1 as the communication path of a mirror disk resource to be created later. Click **Next**.
        For more information, refer to the following:
        - "Reference Guide" -> "Understanding Witness heartbeat resources"
     5. The **Fencing** window is displayed.
        Specify HTTPNP and click **Next**.
        For more information, refer to the following:
        - "Reference Guide" -> "Understanding network partition resolution by HTTP method"

2. **Adding group resources**

- Defining a group

  Create a failover group.

  1. The **Group List** window is displayed.
     Click **Add**.
  2. The **Group Definition** window is displayed.
     In **Name**, enter failover1 as a failover group name. 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 List** window is displayed.
   On this page, add a group resource following the procedure below.

- Mirror disk resource

  Create a mirror disk resource.
  For more information, refer to the following:
  - "Reference Guide" -> "Understanding Mirror disk resources"

  1. Click **Add** on the **Group Resource List** page.
  2. The **Resource Definition of Group | failover1** window is displayed.
     From the **Type** box, select **Mirror disk resource** as a group resource type. In the **Name** box, enter the resource name. 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.
     In **Data Partition Device Name** and **Cluster Partition Device Name**, enter the device name of the partition created in "4. **Creating a block volume**". Specify **Mount Point** and **File System**. Click **Finish** to finish the settings.

- LB probe port resource

  In using EXPRESSCLUSTER in Google Cloud, provides a mechanism to wait for the alive monitoring by a load balancer on a specific port of a node where operations are running.
  For details on the LB probe port resource, refer to the following:
  - "Reference Guide" -> "Understanding LB probe port resources"

  1. Click **Add** on the **Group Resource List** page.
  2. The **Resource Definition of Group | failover1** window is displayed.
     In the **Type** box, select **LB probe port resource** as a group resource type. In the **Name** box, enter the resource name. Click **Next**.
  3. The **Dependency** window is displayed. Click **Next** without specifying anything.
  4. The **Recovery Operation** window is displayed. Click **Next**.
  5. In **Port Number**, enter the value specified in **Health check policy: port** in the load balancer settings (the backend set settings).
  6. Click **Finish**.

3. **Adding monitor resources**

- LB probe port monitor resource

Provides a mechanism for monitoring the alive-monitoring port for the node where an LB probe port resource has been activated.

Adding one LB probe port resource automatically creates one LB probe port monitor resource.

For details on the LB probe port monitor resource, refer to the following:

- "Reference Guide" -> "Understanding LB probe port monitor resources"

4. **Applying the settings and starting the cluster**

Refer to the following:

- "Installation and Configuration Guide" -> "How to create a cluster"

4.4 Verifying the created environment

Verify whether the created environment works properly, by producing a monitoring error for a failover of the failover group.
With the cluster running normally, the verification procedure is as follows:

1. On the active node (server1), start the failover group (failover1).
   In the **Status** tab of Cluster WebUI, make sure that the status of failover1 is **Online** on server1.
   From a client, access the front-end IP address to make sure of being able to connect to the active node.
2. In the pull-down menu of Cluster WebUI, change the mode option from **Operation mode** to **Verification mode**.
3. In the **Status** tab of Cluster WebUI, select the **Enable dummy failure** icon of lbppw1.
4. The LB probe port resource (lbpp1) is reactivated three times. Then the failover group (failover1) fails, being failed over to the corresponding node (server2).
   In the **Status** tab of Cluster WebUI, make sure that the status of failover1 is **Online** on server2.
   Also make sure that, after the failover, the front-end IP address of the load balancer can be normally accessed.

That is all for testing the failover through a dummy failure. If necessary, perform operation checks for other failures as well.

CHAPTER

FIVE

CLUSTER CREATION PROCEDURE (FOR AN HA CLUSTER WITH CLOUD DNS)

5.1 Creation examples

This guide describes how to create a two-node, uni-directional standby cluster with EXPRESSCLUSTER.

Through this procedure, you are to create an HA cluster accessible from clients within the same VPC network on Google Cloud.

This procedure is intended to create a mirror-disk type configuration in which server1 is used as the active server.

The following tables list the parameters which do not have their default values, and the parameters whose values are changed from their default values.

- Google Cloud settings (common to each instance)

Setting item	Setting value
VCN settings	
– Name	test-vpc
– New subnet name	subnetwork-1, subnetwork-11
– New subnet region	asia-northeast1
– New subnet IP address range	10.0.1.0/24, 10.0.11.0/24
Cloud DNS settings (DNS zone)	
– Zone type	Undisclosed
– Zone name	test-zone
– DNS name	example.com
– Option	Default (limitedly disclosed)

continues on next page

Table 5.1 – continued from previous page

Setting item	Setting value
– Network	test-vpc

- Google Cloud settings (individually configured for each instance)

Setting item	Setting value server1	server2
Instance settings		
– Region	asia-northeast1	asia-northeast1
– Zone	asia-northeast1-a	asia-northeast1-b
– New disk	server1-datadisk-0	server2-datadisk-0
Network settings		
– Network	test-vpc	test-vpc
– Subnetwork	subnetwork-11	subnetwork-11
– Private IP address	10.0.11.101	10.0.11.102

- EXPRESSCLUSTER settings (cluster properties)

Setting item	Setting value server1	server2
– Cluster name	Cluster1	Cluster1
– Server name	server1	server2

- EXPRESSCLUSTER settings (failover group)

Resource name	Setting item	Setting value
Mirror disk resource	Resource name	md1
	Details tab - drive letter of the data partition	G:
	Details tab - drive letter of the cluster partition	F:
Google Cloud DNS resource	Resource name	gcdns1

continues on next page

Table 5.4 – continued from previous page

Resource name	Setting item	Setting value
	Zone name	test-zone
	DNS name	test-cluster.example.com
	IP Address (server1)	10.0.11.101
	IP Address (server2)	10.0.11.102

- EXPRESSCLUSTER settings (monitor resource)

Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	Monitor resource name	mdw1
Mirror disk connect monitor resource	Monitor resource name	mdnw1
Google Cloud DNS monitor resource	Monitor resource name	gcdnsw1

5.2 Configuring Google Cloud

1. **Creating a VPC**

   Log in to Google Cloud Console (https://console.cloud.google.com/)
   Create a VCN and a subnet.
   For details on the procedure, refer to the following:
   Overview:
   https://cloud.google.com/vpc/docs/using-vpc/

2. **Creating an Instance**

   Create each of the instances based on a public image.
   During this creation, add a secondary disk for the mirror disk (cluster partition and data partition).
   Create as many instances as the number of virtual machines constituting the cluster.
   For more information on the procedure, refer to the following:
   https://cloud.google.com/compute/docs/how-to/

3. **Setting an instance**

   Connect to the created server1 and server2 instances and log in.
   For detailed instructions, refer to the following:
   https://cloud.google.com/compute/docs/instances/connecting-to-instance/

   Next, set the partitions for the mirror disk resource.
   Create the cluster partition and data partition on the secondary disk added to the instance.
   For more information on setting the partitions for the mirror disk resource, refer to the following:
   - "Installation and Configuration Guide" -> "Determining a system configuration" -> "Settings after configuring hardware" -> "Mirror partition settings (Required for mirror disks)"

4. **Creating a DNS zone**

   Create a DNS zone.
   For details on the procedure, refer to the following:
   https://cloud.google.com/dns/zones/

   From **Zone type**, select **Undisclosed**. For more information on **Zone type**, refer to the following:
   https://cloud.google.com/dns/docs/overview/

5. **Setting up the gcloud CLI**

   Log in to server1 and server2, install the gcloud CLI, and then initialize the SDK.
   If already installed, the gcloud CLI does not have to be reinstalled.
   Before using the gcloud CLI, you as the root user must authorize gcloud CLI.
   For more information on this procedure, refer to the following:
   https://cloud.google.com/sdk/docs/authorizing/

   For more information on other procedures, refer to the following:
   Installation:

https://cloud.google.com/sdk/install/
Initialization:
https://cloud.google.com/sdk/docs/initializing/
Quickstarts:
https://cloud.google.com/sdk/docs/quickstarts/

6. **Configuring Cloud IAM**

   Cloud IAM allows you to authorize the user account or service account used for authorizing gcloud CLI, to manage the record sets of Cloud DNS.
   Use Cloud IAM to give authority for the following:
   - dns.changes.create
   - dns.changes.get
   - dns.managedZones.get
   - dns.resourceRecordSets.create
   - dns.resourceRecordSets.update
   - dns.resourceRecordSets.delete
   - dns.resourceRecordSets.list

   Or give the /roles/dns.admin role.

   For more information on Cloud IAM, refer to the following:
   Authentication and Authorization:
   https://cloud.google.com/iam/
   Access rights management:
   https://cloud.google.com/iam/docs/granting-changing-revoking-access/
   Access rights:
   https://cloud.google.com/dns/docs/access-control/

7. **Adjusting the EXPRESSCLUSTER service startup time, verifying the network settings, verifying the firewall settings, synchronizing the server clock, and turning off the power-saving function**

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

8. **Installing EXPRESSCLUSTER**

   For details on the installation procedure, refer to the following. Restart the OS upon the completion of the installation.
   - "Installation and Configuration Guide"

9. **Registering the EXPRESSCLUSTER license**

   For details on the license registration procedure, refer to the following:
   - "Installation and Configuration Guide"

5.3 Configuring EXPRESSCLUSTER

For Cluster WebUI setup and connection procedures, refer to the following:

- "Installation and Configuration Guide" -> "Creating the cluster configuration data"

This section describes the procedure to add the following resources and monitor resources:

- Mirror disk resource
- Google Cloud DNS resource
- Google Cloud DNS monitor resource

For the settings of other resources and monitor resources, refer to the following:

- "Installation and Configuration Guide"
- "Reference Guide"

1. **Creating a cluster**

   Start the Cluster generation wizard to create a cluster.

   - Creating a cluster

     1. Access Cluster WebUI, and click **Cluster generation wizard**.
     2. **Cluster** of **Cluster generation wizard** is displayed.
        Enter a desired name in **Cluster Name**.
        Select an appropriate language in **Language**. Click **Next**.
     3. **Basic Settings** is displayed.
        The instance connected to Cluster WebUI is displayed as a registered master server.
        Click **Add** to add the remaining instances (by specifying the private IP address of each instance). Click **Next**.
     4. The **Interconnect** window is displayed.
        Specify the IP address (the private IP address of each instance) to be used for interconnect, and a Witness heartbeat.
        For **MDC**, select mdc1 as the communication path to a mirror disk resource to be created later. Click **Next**.
        For more information, refer to the following:
        - "Reference Guide" -> "Understanding Witness heartbeat resources"
     5. The **Fencing** window is displayed.
        Specify HTTPNP and click **Next**.
        For more information, refer to the following:
        - "Reference Guide" -> "Understanding network partition resolution by HTTP method"

2. **Adding group resources**

- Defining a group

  Create a failover group.

  1. The **Group List** window is displayed.
     Click **Add**.
  2. The **Group Definition** window is displayed.
     In **Name**, enter failover1 as a failover group name. 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 List** window is displayed.
   On this page, add a group resource following the procedure below.

- Mirror disk resource

  Create a mirror disk resource.
  For more information, refer to the following:
  - "Reference Guide" -> "Understanding Mirror disk resources"

  1. Click **Add** on the **Group Resource List** page.
  2. The **Resource Definition of Group | failover1** window is displayed.
     From the **Type** box, select **Mirror disk resource** as a group resource type. In the **Name** box, enter the resource name. 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.
     In **Data Partition Drive Letter** and **Cluster Partition Drive Letter**, enter the drive letters of the partition created in "4. **Creating a block volume**". Click **Finish** to finish the settings.

- Google Cloud DNS resource

  Provides a mechanism to register records when active and delete records when inactive for Cloud DNS.
  For more information, refer to the following:
  - "Reference Guide" -> "Understanding Google Cloud DNS resources"

  1. Click **Add** on the **Group Resource List** page.
  2. The **Resource Definition of Group | failover1** window is displayed.
     In the **Type** box, select **Google Cloud DNS resource** as a group resource type. In the **Name** box, enter the resource name. Click **Next**.
  3. The **Dependency** window is displayed. Click **Next** without specifying anything.
  4. The **Recovery Operation** window is displayed. Click **Next**.
  5. In **Zone Name**, enter the value specified as the zone name when configuring Cloud DNS (DNS zone).
     In **DNS Name** and **IP Address**, enter the DNS name of the record set to be added to the Cloud DNS zone and the IP address corresponding to the DNS name.
  6. Click **Finish**.

3. **Adding monitoring resources**

- Google Cloud DNS monitoring resource

Confirms the existence of the record set (A record) controlled by the specified Google Cloud DNS resource as the target resource during active monitoring.

For more information on Google Cloud DNS monitoring resources, refer to the following:

- "Reference Guide" -> "Understanding Google Cloud DNS monitor resources"

1. Click **Add** on the **Monitor Resource List** page.
2. The **Monitor Resource Definition** window is displayed. From the **Type** box, select **Google Cloud DNS monitoring resource** as the monitoring resource type. In the **Name** box, enter the resource name. Click **Next**.
3. The **Monitoring (Common)** window is displayed. Specify the resource name of the Google Cloud DNS resource as the target resource.
4. The **Recovery Operation** window is displayed. Specify the recovery target and recovery operation for the monitoring resource in case of abnormality.
5. Click **Finish**.

4. **Applying the settings and starting the cluster**

Refer to the following:

- "Installation and Configuration Guide" -> "How to create a cluster"

5.4 Verifying the operations

Verify whether the created environment works properly by generating a monitoring error to fail over a failover group. If the cluster is running normally, the verification procedure is as follows:

1. On the active node (server1), start the failover group (failover1). In the **Status** tab of Cluster WebUI, make sure that the status of failover1 is **Online** on server1.
2. From a client, access test-cluster.example.com to make sure of being able to connect to the active node.

   ```
   $ nslookup test-cluster.example.com <DNS_servers_checked_in_the_above_step>
   ```

3. In Cluster WebUI, manually move the failover group from the active node to the standby node. In the **Status** tab of Cluster WebUI, make sure that the status of failover1 is **Online** on server2.
4. From a client, access test-cluster.example.com to make sure of being able to connect to the standby node.

   ```
   $ nslookup test-cluster.example.com <DNS_servers_checked_in_the_above_step>
   ```

Verifying the failover operation when an A record is deleted from the DNS server is now complete. Verify the operations in case of other failures if necessary.

CHAPTER

SIX

ERROR MESSAGES

For information on error messages of the resources/monitor resources, refer to the following:

- "Reference Guide" -> "Error messages"

CHAPTER

SEVEN

NOTES AND RESTRICTIONS

7.1 HA cluster with a load balancer

7.1.1 Notes on Google Cloud

- In designing a performance-oriented system, keep this in mind: Google Cloud tends to increase its performance deterioration rate in multi-tenant cloud environments, compared with that in physical environments or general and virtualized (non-cloud) environments.

7.1.2 Notes on EXPRESSCLUSTER

- Google Cloud's specification requires HTTP-protocol-based legacy health checks for external TCP network load balancing.

  The LB probe port resource, which supports only TCP-protocol-based health checks, cannot respond to health checks by an external TCP network load balancer.

  Therefore, use an internal TCP load balancer instead of an external TCP network load balancer, with which and the LB probe port resource the HA cluster cannot be used.

  Refer to the following:

  https://cloud.google.com/load-balancing/docs/health-check-concepts/

- For an HA cluster configuration with an internal TCP load balancer, the HA cluster cannot be accessed from any client which belongs to a region different from that of the HA cluster--due to Google Cloud's specification.

  Refer to the following:

  https://cloud.google.com/load-balancing/docs/internal/#architecture

- Make the OS startup time longer than the time of **Heartbeat Timeout**.

  Refer to the following:

  - "Reference Guide" -> "Cluster properties" -> "Timeout tab"

  - "Getting Started Guide" -> "Notes and Restriction" -> "Adjusting OS startup time"

See also:

- "Getting Started Guide" -> "Notes and Restriction" -> "Communication port number"
- "Getting Started Guide" -> "Notes and Restriction" -> "Setting up LB probe port resources"
- "Reference Guide" -> "Notes on LB probe port resources"
- "Reference Guide" -> "Notes on LB probe port monitor resources"

7.2 HA cluster with Cloud DNS

7.2.1 Notes on Google Cloud

- In designing a performance-oriented system, keep this in mind: Google Cloud tends to increase its performance deterioration rate in multi-tenant cloud environments, compared with that in physical environments or general and virtualized (non-cloud) environments.
- If a client takes time to resolve a name, its possible causes are as below. Check their corresponding settings:
  - The OS-side resolver takes time.
  - The TTL value is high.
  - If a name resolution is tried prior to the completion of Cloud DNS change propagation, the DNS returns NXDOMAIN (non-existing domain). In this case, the name resolution fails until the valid period of the negative cache expires.

7.2.2 Notes on EXPRESSCLUSTER

- Have only one EXEC resource with the scripts for Cloud DNS.
  If multiple actions are simultaneously taken to the record sets of Cloud DNS, some of the actions may fail. This is due to Google Cloud's specification.
- Make the OS startup time longer than the time of **Heartbeat Timeout**.
  Refer to the following:
  - "Reference Guide" -> "Cluster properties" -> "Timeout tab"
  - "Getting Started Guide" -> "Notes and Restriction" -> "Adjusting OS startup time"

7.3 Shared disk/hybrid disk type cluster

7.3.1 Notes on EXPRESSCLUSTER

- Currently, there is a known issue where shared disks do not work properly when using NVMe controllers and Hyperdisk Balanced volumes (multi-writer mode). Therefore, it is recommended to use SSD Persistent Disk volumes (multi-writer mode) for shared disks.
- When configuring HBA settings to restrict access to shared disks, ensure that partitions other than the shared disk (especially system areas) are excluded from cluster management.

CHAPTER

EIGHT

LEGAL NOTICE

8.1 Disclaimer

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

8.2 Trademark Information

- EXPRESSCLUSTER® is a registered trademark of NEC Corporation.
- Microsoft, Windows, Windows Server, Internet Explorer, Azure, and Hyper-V are registered trademarks of Microsoft Corporation in the United States and other countries.
- Google Cloud is a trademark or a registered trademark of Google LLC.
- Other product names and slogans written in this manual are trademarks or registered trademarks of their respective companies.

CHAPTER

NINE

REVISION HISTORY

Edition	Revised Date	Description
1st	Apr 08, 2026	New Guide