EXPRESSCLUSTER X 5.0 for Windows
Getting Started Guide

Release 4

NEC Corporation

Nov 04, 2022

TABLE OF CONTENTS:

CHAPTER

ONE

PREFACE

1.1 Who Should Use This Guide

EXPRESSCLUSTER X Getting Started Guide is intended for first-time users of the EXPRESSCLUSTER. The guide covers topics such as product overview of the EXPRESSCLUSTER, how the cluster system is installed, and the summary of other available guides. In addition, latest system requirements and restrictions are described.

1.2 How This Guide is Organized

- 2. *What is a cluster system?*: Helps you to understand the overview of the cluster system.
- 3. *Using EXPRESSCLUSTER*: Provides instructions on how to use EXPRESSCLUSTER and other related-information.
- 4. *Installation requirements for EXPRESSCLUSTER*: Provides the latest information that needs to be verified before starting to use EXPRESSCLUSTER.
- 5. *Latest version information*: Provides information on latest version of the EXPRESSCLUSTER.
- 6. *Notes and Restrictions*: Provides information on known problems and restrictions..
- 7. *Glossary*

1.3 EXPRESSCLUSTER X Documentation Set

The EXPRESSCLUSTER X manuals consist of the following four 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.

1.4 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 fields, list boxes, menu selections, buttons, labels, icons, etc.	In User Name, type your name. On the File menu, click Open Database.
Angled bracket within the command line	Indicates that the value specified inside of the angled bracket can be omitted.	`clpstat -s [-h host_name]`
Monospace	Indicates path names, commands, system output (message, prompt, etc), directory, file names, functions and parameters.	`c:\Program files\ EXPRESSCLUSTER`
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.	`clpstat -s [-h host_name]`

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

1.5 Contacting NEC

For the latest product information, visit our website below:

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

CHAPTER

TWO

WHAT IS A CLUSTER SYSTEM?

This chapter describes overview of the cluster system.

This chapter covers:

2.1 Overview of the cluster system

A key to success in today's computerized world is to provide services without them stopping. A single machine down due to a failure or overload can stop entire services you provide with customers. This will not only result in enormous damage but also in loss of credibility you once had.

Introducing a cluster system allows you to minimize the period during which your system stops (down time) or to improve availability by load distribution.

As the word "cluster" represents, a system aiming to increase reliability and performance by clustering a group (or groups) of multiple computers. There are various types of cluster systems, which can be classified into following three listed below. EXPRESSCLUSTER is categorized as a high availability cluster.

- **High Availability (HA) Cluster**
  In this cluster configuration, one server operates as an active server. When the active server fails, a stand-by server takes over the operation. This cluster configuration aims for high-availability. The high availability cluster is available in the shared disk type and the mirror disk type.
- **Load Distribution Cluster**
  This is a cluster configuration where requests from clients are allocated to each of the nodes according to appropriate load distribution rules. This cluster configuration aims for high scalability. Generally, data cannot be passed. The load distribution cluster is available in a load balance type or parallel database type.
- **High Performance Computing (HPC) Cluster**
  This is a cluster configuration where the computation amount is huge and a single operation is performed with a super computer. CPUs of all nodes are used to perform a single operation.

2.2 High Availability (HA) cluster

To enhance the availability of a system, it is generally considered that having redundancy for components of the system and eliminating a single point of failure is important. "Single point of failure" is a weakness of having a single computer component (hardware component) in the system. If the component fails, it will cause interruption of services. The high availability (HA) cluster is a cluster system that minimizes the time during which the system is stopped and increases operational availability by establishing redundancy with multiple nodes.

The HA cluster is called for in mission-critical systems where downtime is fatal. The HA cluster can be divided into two types: shared disk type and mirror disk type. The explanation for each type is provided below.

The HA cluster can be divided into two types: shared disk type and data mirror type. The explanation for each type is provided below.

2.2.1 Shared disk type

Data must be inherited from one server to another in cluster systems. A cluster typology where data is stored in an external disk (shared disk) accessible from two or more servers and inherited among them through the disk (for example, FibreChannel disk array device of SAN connection) is called shared disk type.

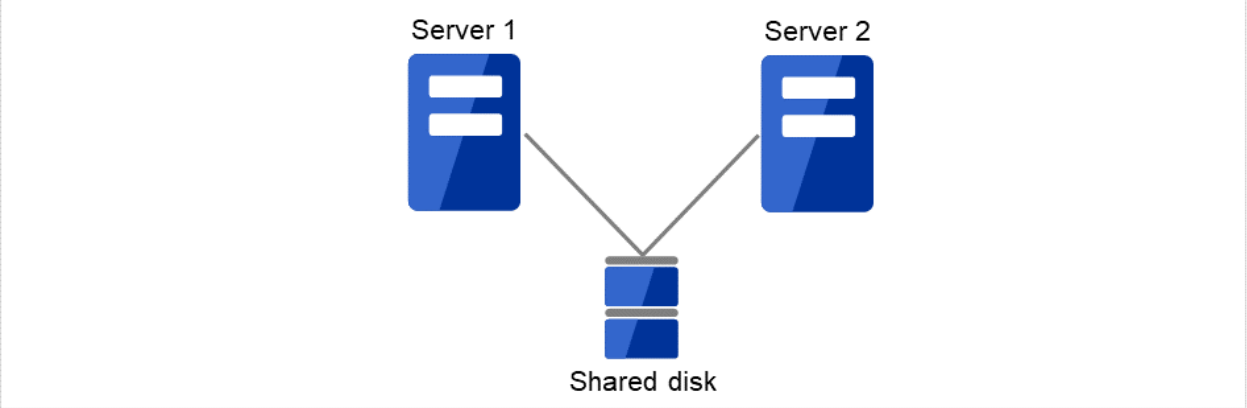


Fig. 2.1: HA cluster configuration (Shared disk type)

- Expensive since a shared disk is necessary.
- Ideal for the system that handles large data

If a failure occurs on a server where applications are running (active server), the cluster system automatically detects the failure and starts applications in a stand-by server to take over operations. This mechanism is called failover. Operations to be inherited in the cluster system consist of resources including disk, IP address, and application.

In a non-clustered system, a client needs to access a different IP address if an application is restarted on a server other than the server where the application was originally running. In contrast, many cluster systems allocate a virtual IP address of another network but not of an IP address given to a server on an operational basis. A server where the operation is running, be it an active or a stand-by server, remains transparent to a client. The operation is continued as if it has been running on the same server.

If a failover occurs because an active server is down, data on the shared disk is inherited to a stand-by server without necessary application-ending processing being completed. For this reason, it is required to check logic of data on a stand-by server. Usually this processing is the same as the one performed when a non-clustered system is rebooted after its shutdown. For example, roll-back or roll-forward is necessary for databases. With these actions, a client can continue operation only by re-executing the SQL statement that has not been committed yet.

After a failure occurs, a server with the failure can return to the cluster system as a stand-by server if it is physically separated from the system, fixed, and then succeeds to connect the system. It is not necessary to failback a group to the original server when continuity of operations is important. If it is essentially required to perform the operations on the original server, move the group.

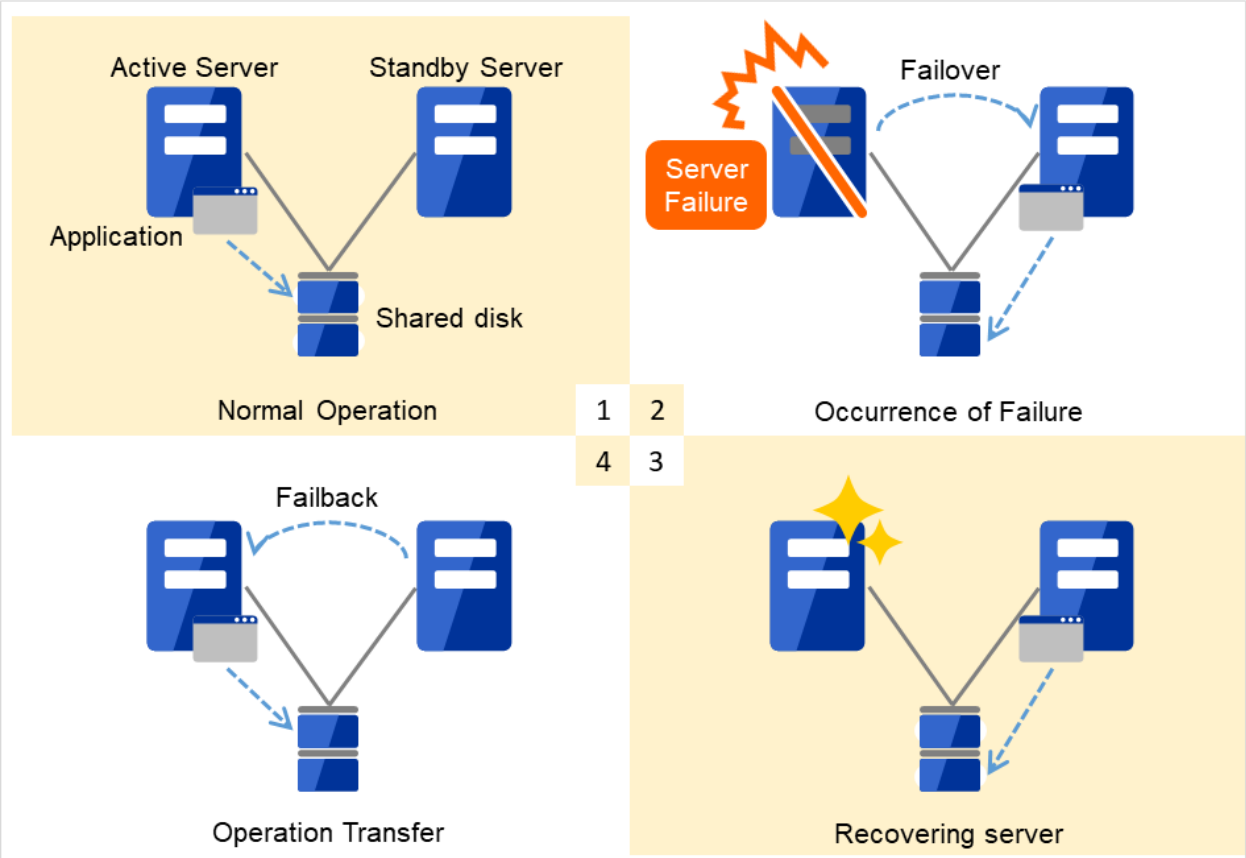


Fig. 2.2: From occurrence of a failure to recovery

1. Normal operation
2. Occurrence of failure
3. Recovering server
4. Operation transfer

When the specification of the failover destination server does not meet the system requirements or overload occurs due to multi-directional stand-by, operations on the original server are preferred. In such a case, after finishing the recovery of the original node, stop the operations and start them again on the original node. Returning a failover group to the original server is called failback.

A stand-by mode where there is one operation and no operation is active on the stand-by server, as shown in Figure 2.3 HA cluster topology, is referred to as uni-directional stand-by.

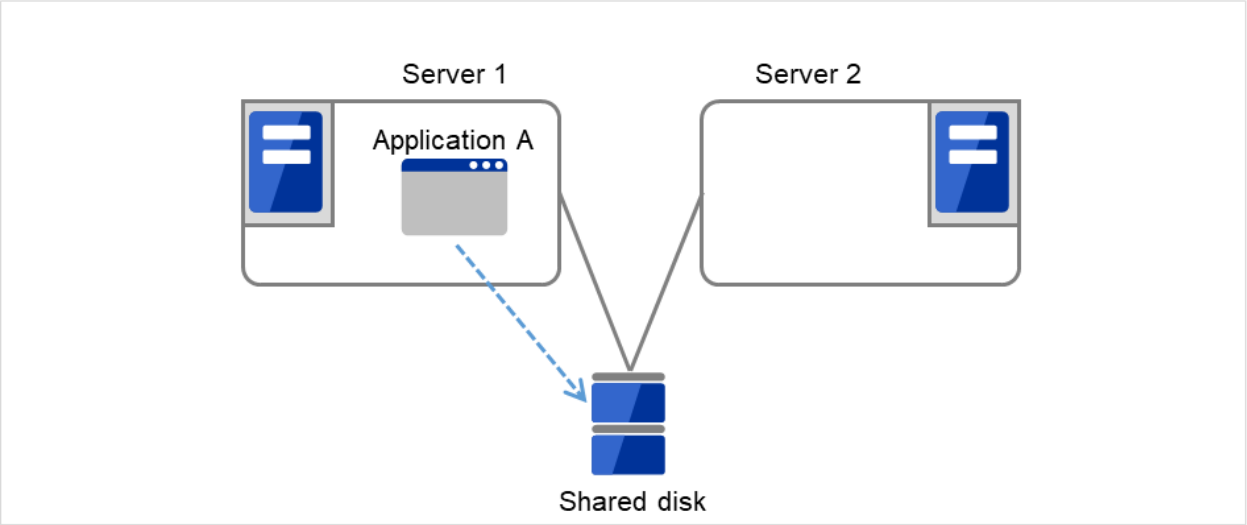


Fig. 2.3: HA cluster topology (Uni-directional standby)

A mode where there are two or more operations with each server in the cluster serving as both active and standby server, as shown in Fig. 2.4 HA cluster topology (Multi-directional standby), is referred to as multi-directional standby.

Server 1 is the active server for Application A and also the standby server for Application B.

Server 2 is the active server for Application B and also the standby server for Application A.

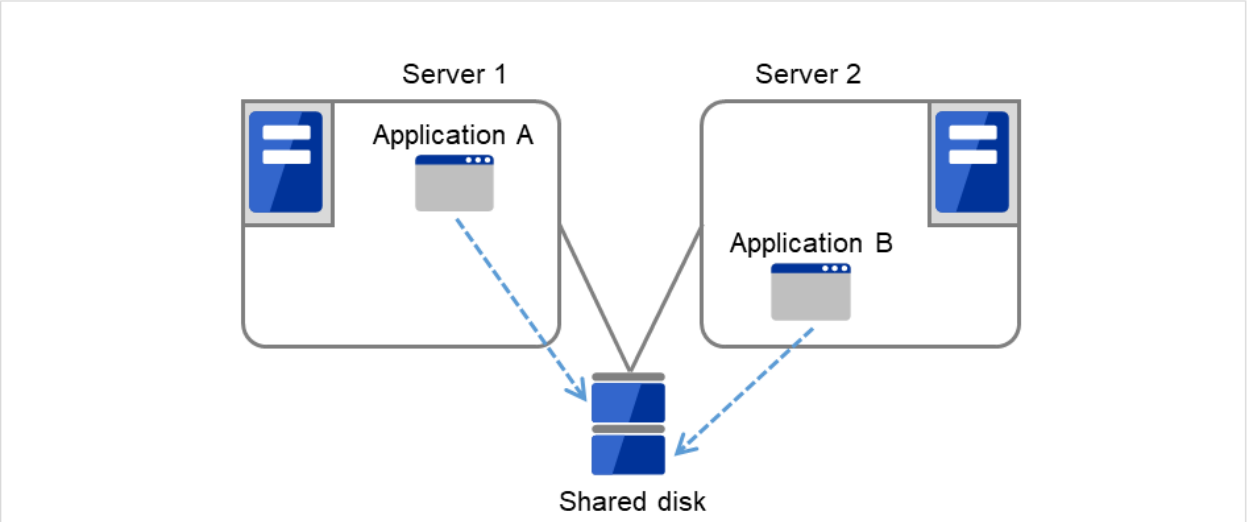


Fig. 2.4: HA cluster topology (Multi-directional standby)

2.2.2 Mirror disk type

The shared disk type cluster system is good for large-scale systems. However, creating a system with this type can be costly because shared disks are generally expensive. The mirror disk type cluster system provides the same functions as the shared disk type with smaller cost through mirroring of server disks.

The mirror disk type is not recommended for large-scale systems that handle a large volume of data since data needs to be mirrored between servers.

When a write request is made by an application, the data mirror engine writes data in the local disk and sends the written data to the stand-by server via the interconnect. Interconnect is a cable connecting servers. It is used to monitor whether the server is activated or not in the cluster system. In addition to this purpose, interconnect is sometimes used to transfer data in the data mirror type cluster system. The data mirror engine on the stand-by server achieves data synchronization between stand-by and active servers by writing the data into the local disk of the stand-by server.

For read requests from an application, data is simply read from the disk on the active server.

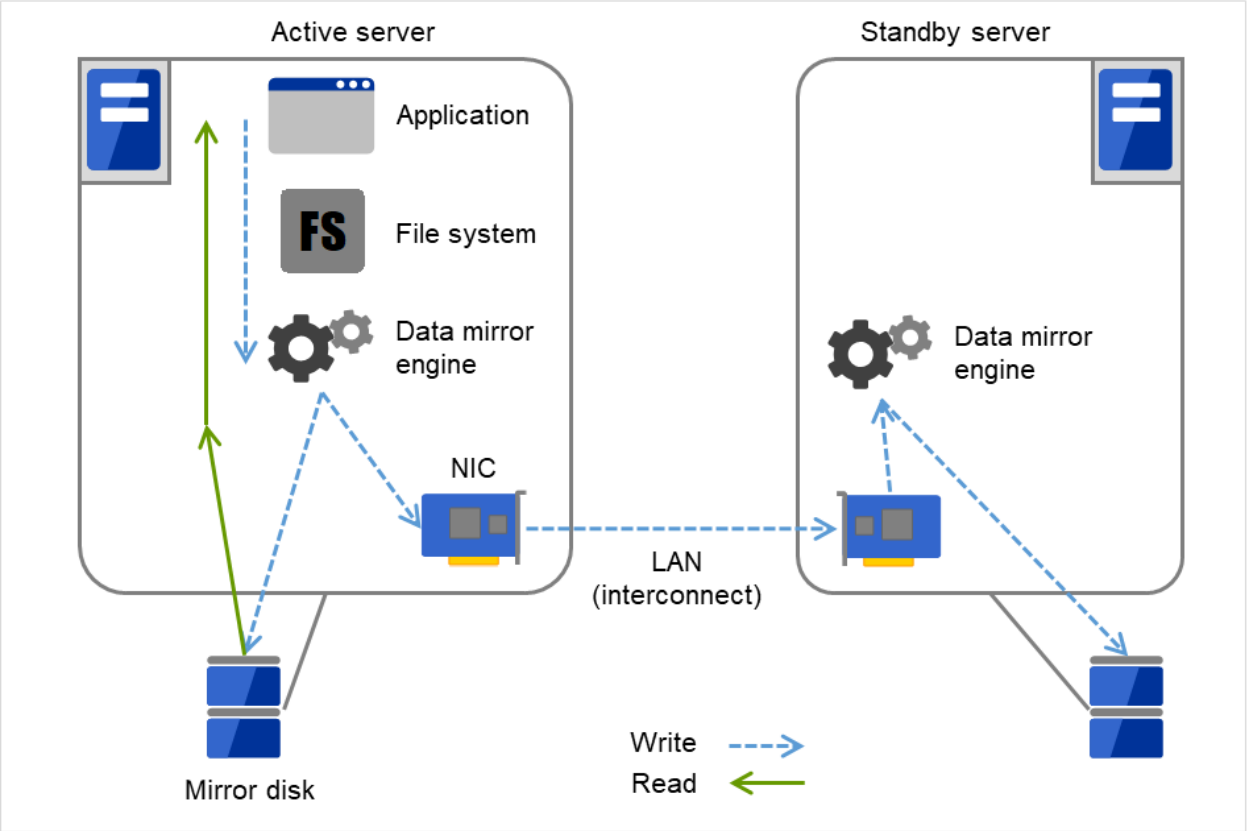


Fig. 2.5: Data mirror mechanism

Snapshot backup is applied usage of data mirroring. Because the data mirror type cluster system has shared data in two locations, you can keep the data of the stand-by server as snapshot backup by simply separating the server from the cluster.

HA cluster mechanism and problems

The following sections describe cluster implementation and related problems.

2.3 System configuration

In a shared disk-type cluster, a disk array device is shared between the servers in a cluster. When an error occurs on a server, the standby server takes over the applications using the data on the shared disk.

In the mirror disk type cluster, a data disk on the cluster server is mirrored via the network. When an error occurs on a server, the applications are taken over using the mirror data on the stand-by server. Data is mirrored for every I/O. Therefore, the mirror disk type cluster appears the same as the shared disk viewing from a high level application.

The following the shared disk type cluster configuration.

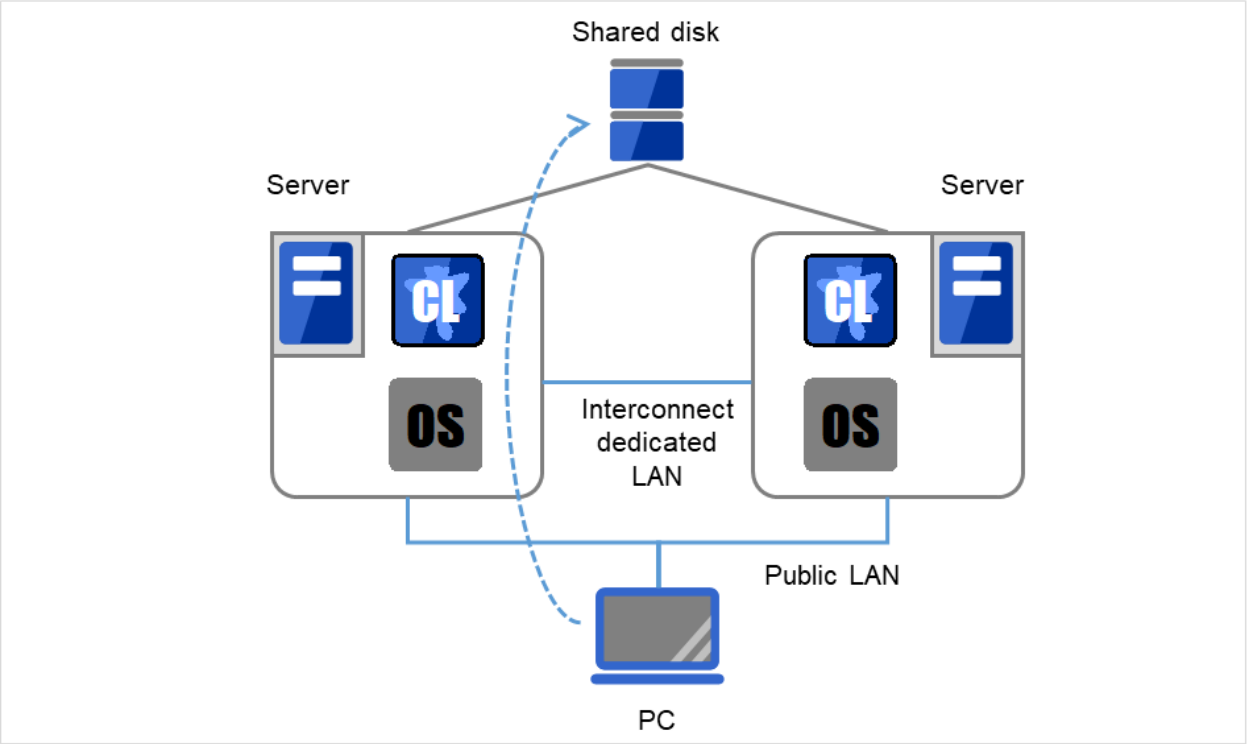


Fig. 2.6: System configuration

A failover-type cluster can be divided into the following categories depending on the cluster topologies:

Uni-Directional Standby Cluster System

In the uni-directional standby cluster system, the active server runs applications while the other server, the standby server, does not. This is the simplest cluster topology and you can build a high-availability system without performance degradation after failing over.

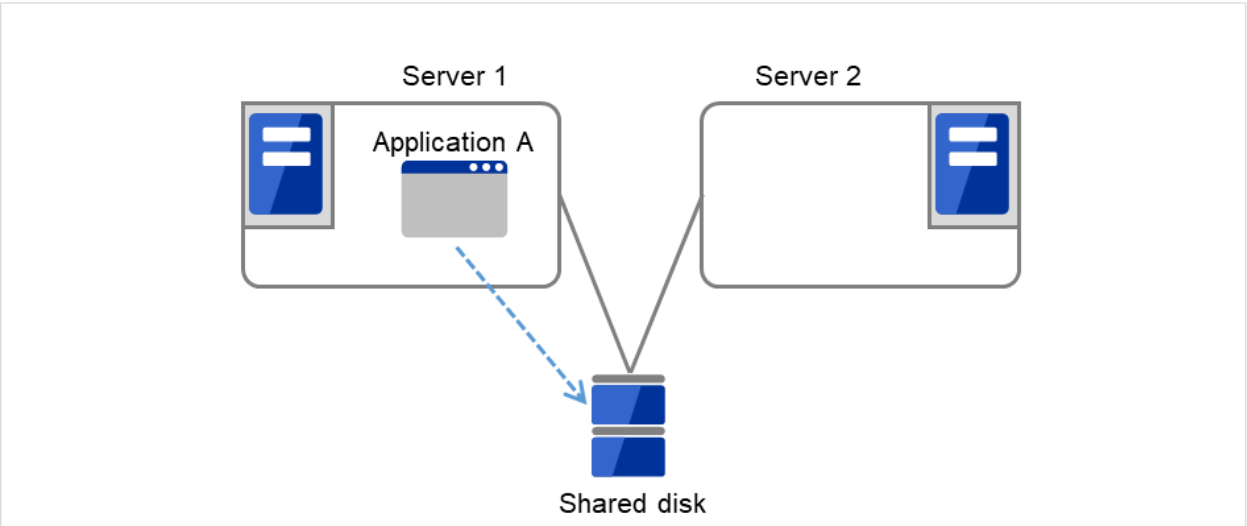


Fig. 2.7: Uni-directional standby cluster (1)

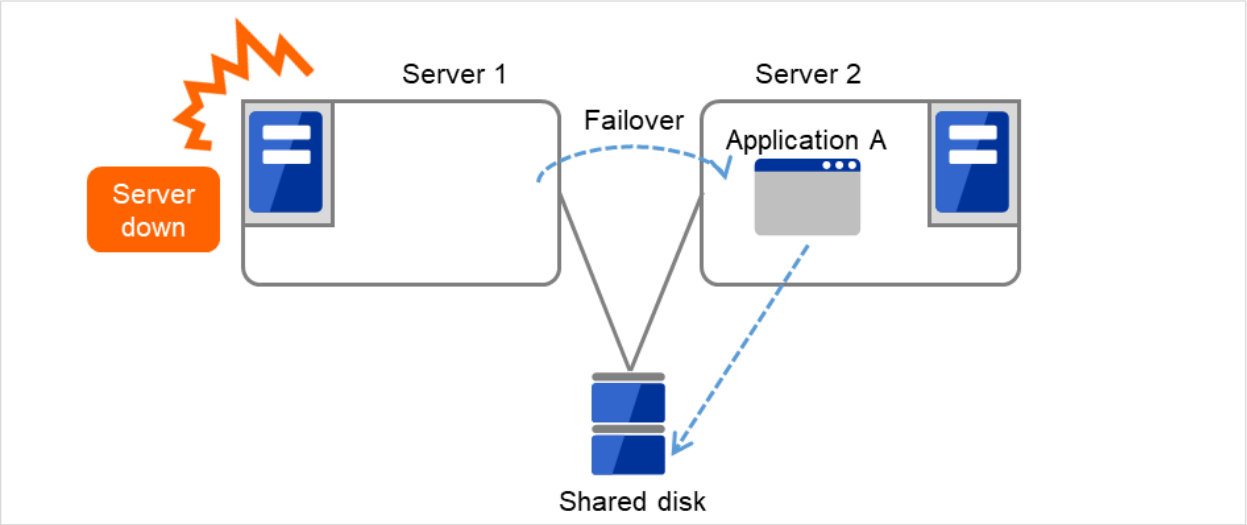


Fig. 2.8: Uni-directional standby cluster (2)

Multi-directional standby cluster system with the same application

In the same application multi-directional standby cluster system, the same applications are activated on multiple servers. These servers also operate as standby servers. These applications are operated on their own. When a failover occurs, the same applications are activated on one server. Therefore, the applications that can be activated by this operation need to be used. When the application data can be split into multiple data, depending on the data to be accessed, you can build a load distribution system per data partitioning basis by changing the client's connecting server.

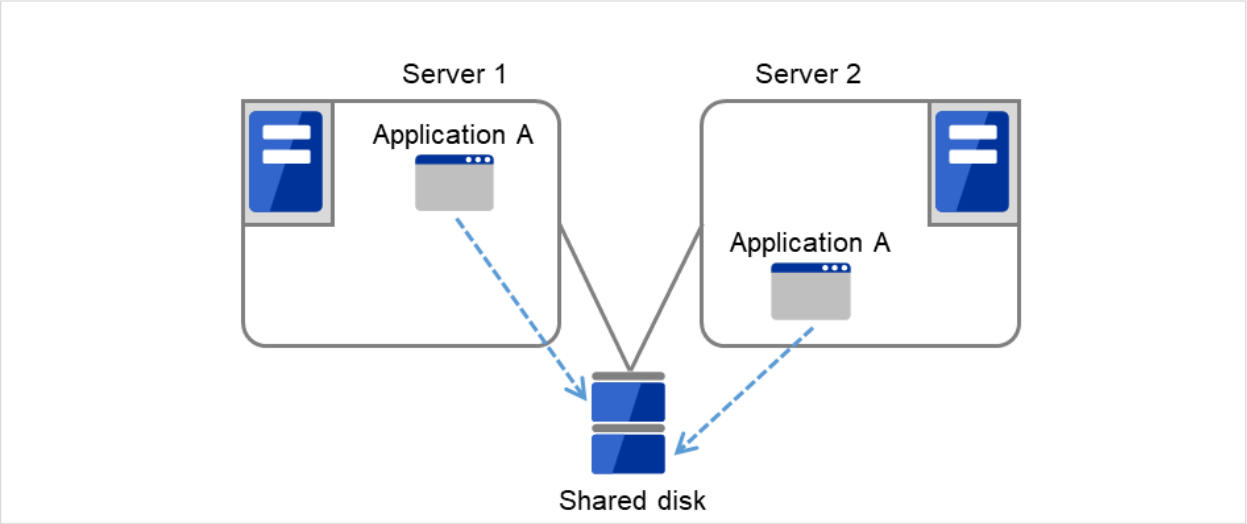


Fig. 2.9: Multi-directional standby cluster system with the same application (1)

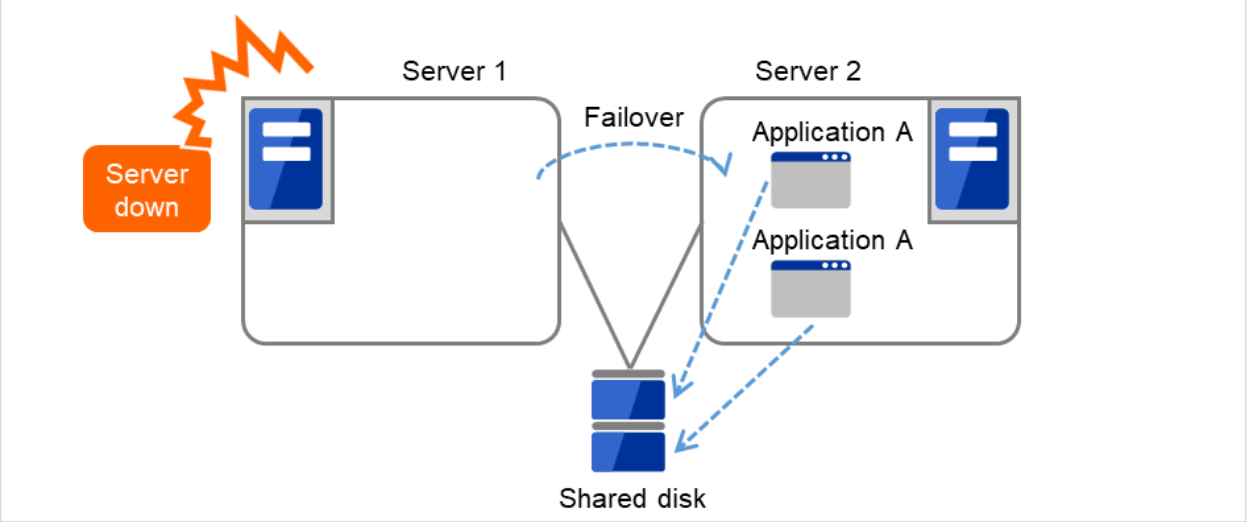


Fig. 2.10: Multi-directional standby cluster system with the same application (2)

Multi-directional standby cluster system with different applications

In the different application multi-directional standby cluster system, different applications are activated on multiple servers and these servers operate as standby servers. When a failover occurs, two or more applications are activated on one server. Therefore, these applications need to be able to coexist. You can build a load distribution system per application unit basis.

Application A and Application B are different applications.

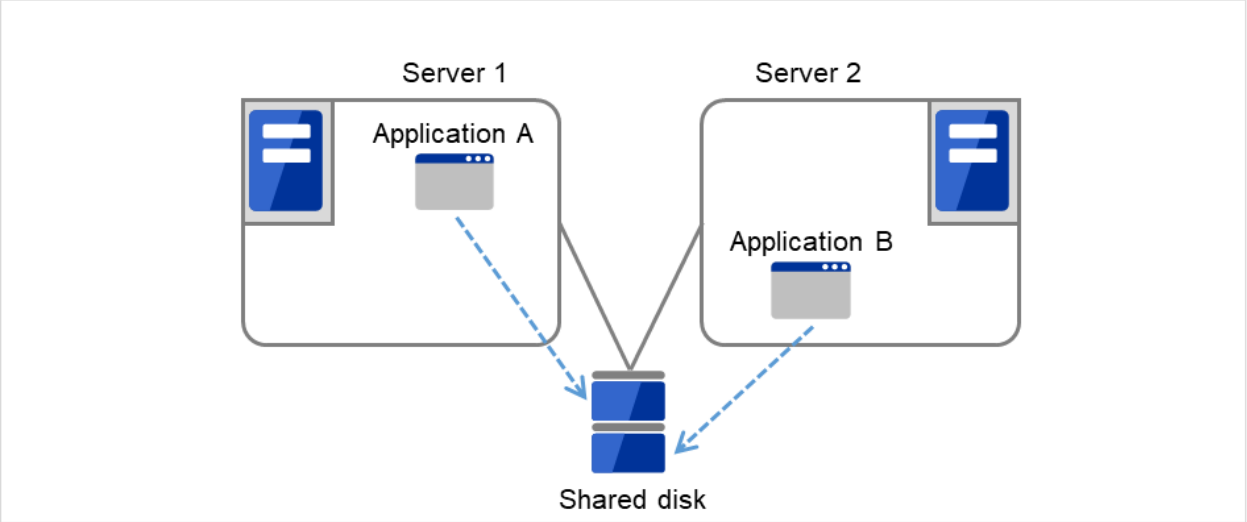


Fig. 2.11: Multi-directional standby cluster system with different applications (1)

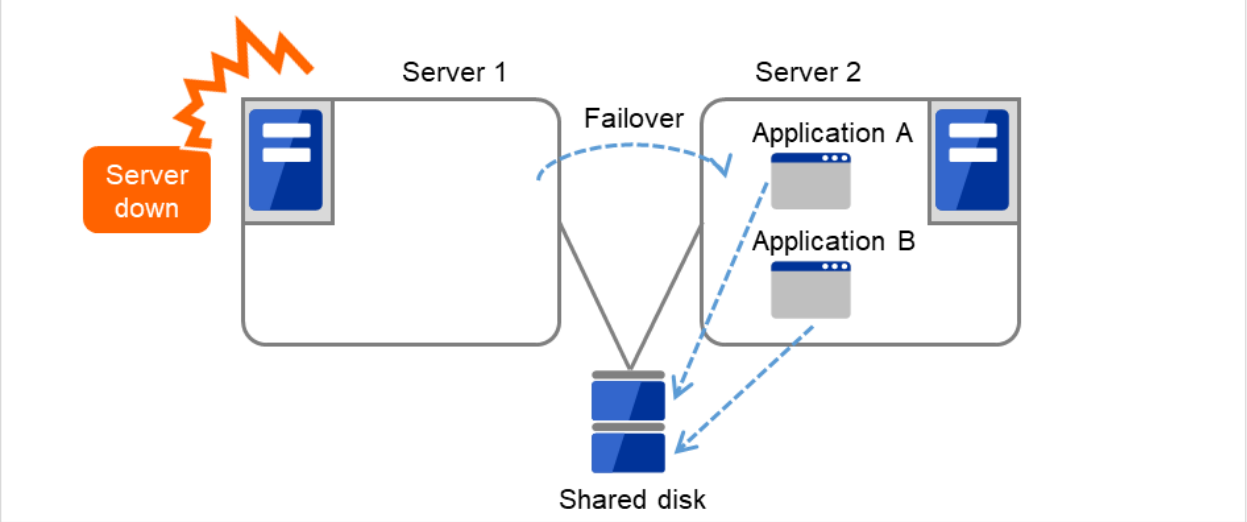


Fig. 2.12: Multi-directional standby cluster system with different applications (2)

N-to-N Configuration

The configuration can be expanded with more nodes by applying the configurations introduced thus far. In an N-to-N configuration described below, three different applications are run on three servers and one standby server takes over the application if any problem occurs. In a uni-directional standby cluster system, the stand-by server does not operate anything, so one of the two server functions as a stand-by server. However, in an N-to N configuration, only one of the four servers functions as a stand-by server. Performance deterioration is not anticipated if an error occurs only on one server.

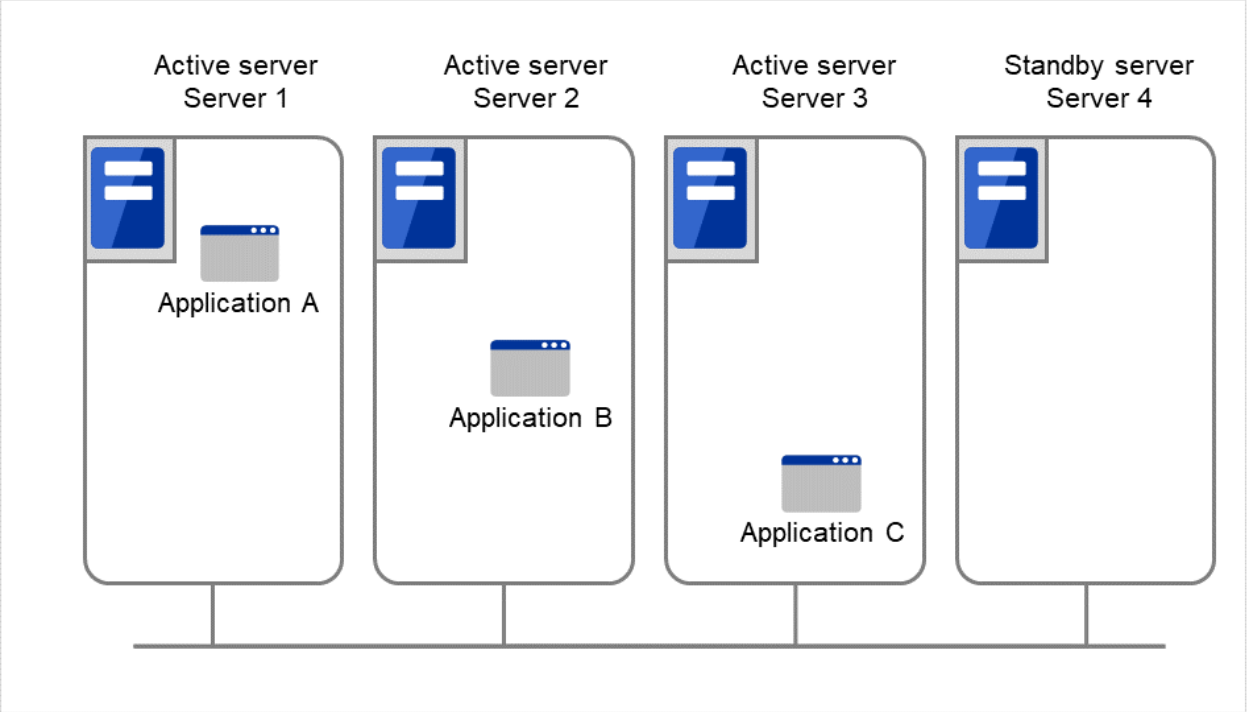


Fig. 2.13: Node to node configuration (1)

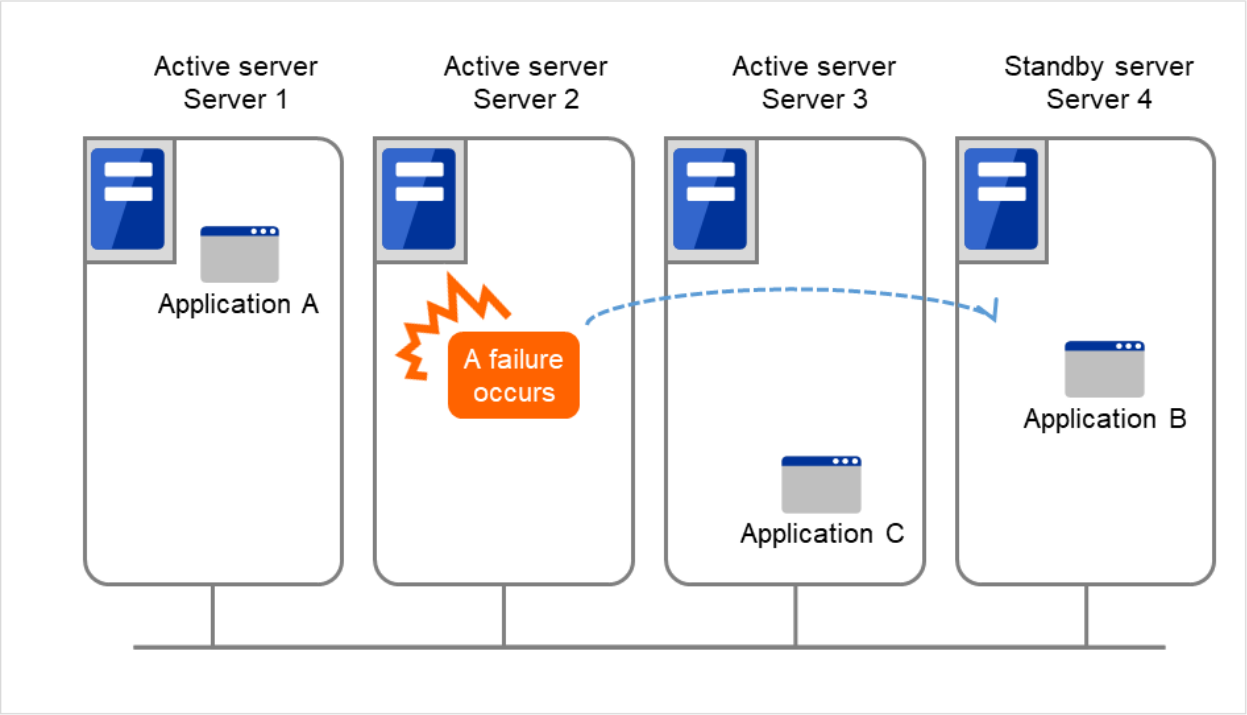


Fig. 2.14: Node to node configuration (2)

2.4 Error detection mechanism

Cluster software executes failover (for example, passing operations) when a failure that can affect continued operation is detected. The following section gives you a quick view of how the cluster software detects a failure.

EXPRESSCLUSTER regularly checks whether other servers are properly working in the cluster system. This function is called "heartbeat communication."

Heartbeat and detection of server failures

Failures that must be detected in a cluster system are failures that can cause all servers in the cluster to stop. Server failures include hardware failures such as power supply and memory failures, and OS panic. To detect such failures, the heartbeat is used to monitor whether the server is active or not.

Some cluster software programs use heartbeat not only for checking if the target is active through ping response, but for sending status information on the local server. Such cluster software programs begin failover if no heartbeat response is received in heartbeat transmission, determining no response as server failure. However, grace time should be given before determining failure, since a highly loaded server can cause delay of response. Allowing grace period results in a time lag between the moment when a failure occurred and the moment when the failure is detected by the cluster software.

Detection of resource failures

Factors causing stop of operations are not limited to stop of all servers in the cluster. Failure in disks used by applications, NIC failure, and failure in applications themselves are also factors that can cause the stop of operations. These resource failures need to be detected as well to execute failover for improved availability.

Accessing a target resource is used to detect resource failures if the target is a physical device. For monitoring applications, trying to service ports within the range not affecting operation is a way of detecting an error in addition to monitoring if application processes are activated.

2.4.1 Shared disk lock

In a failover cluster system of the shared disk type, multiple servers physically share the disk device. Typically, a file system enjoys I/O performance greater than the physical disk I/O performance by keeping data caches in a server.

What if happens a file system is accessed by multiple servers simultaneously?

Because a general file system assumes no server other than the local updates data on the disk, inconsistency between caches and the data on the disk arises. Ultimately the data will be destroyed. The failover cluster system locks the disk device to prevent multiple servers from mounting a file system simultaneously due to a network partition explained below.

2.4.2 Network partition (Split-Brain Syndrome)

When all interconnects between servers are disconnected, it is not possible to tell if a server is down, only by monitoring if it is activated by a heartbeat. In this status, if a failover is performed and multiple servers mount a file system simultaneously considering the server has been shut down, data on the shared disk may be corrupted.

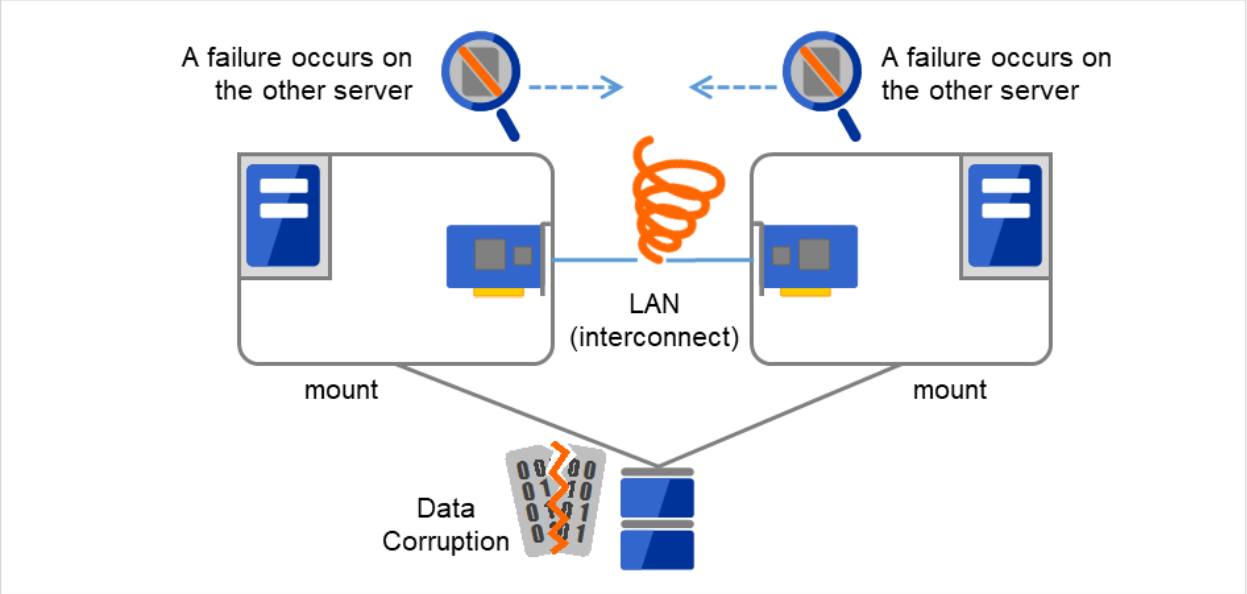


Fig. 2.15: Network partition

The problem explained in the section above is referred to as "network partition" or "Split Brain Syndrome." To resolve this problem, the failover cluster system is equipped with various mechanisms to ensure shared disk lock at the time when all interconnects are disconnected.

2.5 Inheriting cluster resources

As mentioned earlier, resources to be managed by a cluster include disks, IP addresses, and applications. The functions used in the failover cluster system to inherit these resources are described below.

2.5.1 Inheriting data

In the shared disk type cluster, data to be passed from a server to another in a cluster system is stored in a partition in a shared disk. This means inheriting data is re-mounting the file system of files that the application uses from a healthy server. What the cluster software should do is simply mount the file system because the shared disk is physically connected to a server that inherits data.

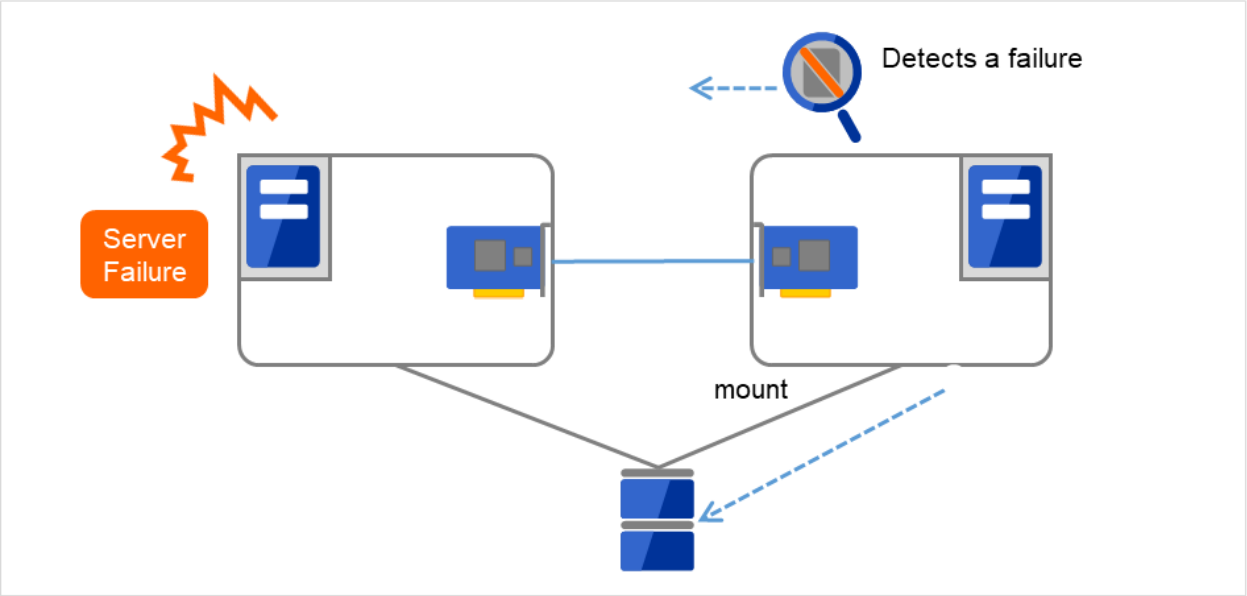


Fig. 2.16: Inheriting data

The diagram above (Figure 2.16 Inheriting data) may look simple. Consider the following issues in designing and creating a cluster system.

One issue to consider is recovery time for a file system or database. A file to be inherited may have been used by another server or to be updated just before the failure occurred. For this reason, a cluster system may need to do consistency checks to data it is moving on some file systems, as well as it may need to rollback data for some database systems. These checks are not cluster system-specific, but required in many recovery processes, including when you reboot a single server that has been shut down due to a power failure. If this recovery takes a long time, the time is wholly added to the time for failover (time to take over operation), and this will reduce system availability.

Another issue you should consider is writing assurance. When an application writes data into the shared disk, usually the data is written through a file system. However, even though the application has written data - but the file system only stores it on a disk cache and does not write into the shared disk - the data on the disk cache will not be inherited to a stand-by server when an active server shuts down. For this reason, it is required to write important data that needs to be inherited to a stand-by server into a disk, by using a function such as synchronous writing. This is same as preventing the data becoming volatile when a single server shuts down. Namely, only the data registered in the shared disk is inherited to a stand-by server, and data on a memory disk such as a disk cache is not inherited. The cluster system needs to be configured considering these issues.

2.5.2 Inheriting IP addresses

When a failover occurs, it does not have to be concerned which server is running operations by inheriting IP addresses. The cluster software inherits the IP addresses for this purpose.

2.5.3 Inheriting applications

The last to come in inheritance of operation by cluster software is inheritance of applications. Unlike fault tolerant computers (FTC), no process status such as contents of memory is inherited in typical failover cluster systems. The applications running on a failed server are inherited by rerunning them on a healthy server.

For example, when the database instance is failed over, the database that is started in the stand-by server can not continue the exact processes and transactions that have been running in the failed server, and roll-back of transaction is performed in the same as restarting the database after it was down. It is required to connect to the database again from the client. The time needed for this database recovery is typically a few minutes though it can be controlled by configuring the interval of DBMS checkpoint to a certain extent.

Many applications can restart operations by re-execution. Some applications, however, require going through procedures for recovery if a failure occurs. For these applications, cluster software allows to start up scripts instead of applications so that recovery process can be written. In a script, the recovery process, including cleanup of files half updated, is written as necessary according to factors for executing the script and information on the execution server.

2.5.4 Summary of failover

To summarize the behavior of cluster software:

(a) Detects a failure (heartbeat/resource monitoring)

(b) Performs fencing (resolves a network partition (NP resolution) and disconnects the failed server)

(c) Pass data

(d) Pass IP address

(e) Pass applications

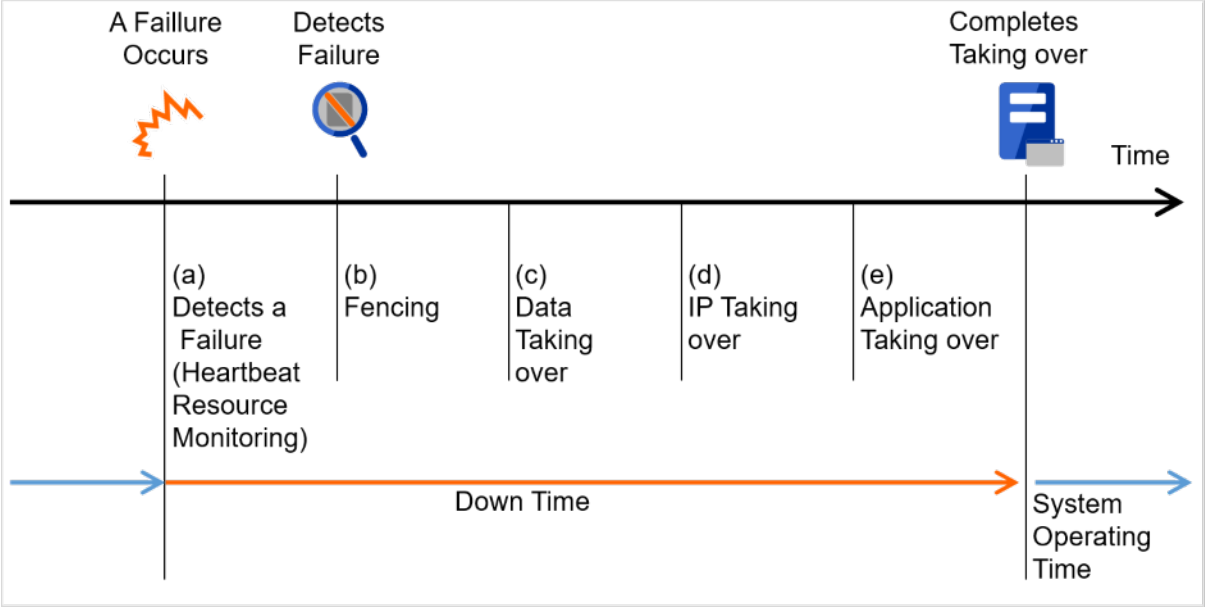


Fig. 2.17: Failover time chart

Cluster software is required to complete each task quickly and reliably (see Figure 2.17 Failover time chart) Cluster software achieves high availability with due consideration on what has been described so far.

2.6 Eliminating single point of failure

Having a clear picture of the availability level required or aimed is important in building a high availability system. This means when you design a system, you need to study cost effectiveness of countermeasures, such as establishing a redundant configuration to continue operations and recovering operations within a short period, against various failures that can disturb system operations.

Single point of failure (SPOF), as described previously, is a component where failure can lead to stop of the system. In a cluster system, you can eliminate the system's SPOF by establishing server redundancy. However, components shared among servers, such as shared disk may become a SPOF. The key in designing a high availability system is to duplicate or eliminate this shared component.

A cluster system can improve availability but failover will take a few minutes for switching systems. That means time for failover is a factor that reduces availability. Solutions for the following three, which are likely to become SPOF, will be discussed hereafter although technical issues that improve availability of a single server such as ECC memory and redundant power supply are important.

- Shared disk
- Access path to the shared disk
- LAN

2.6.1 Shared disk

Typically a shared disk uses a disk array for RAID. Because of this, the bare drive of the disk does not become SPOF. The problem is the RAID controller is incorporated. Shared disks commonly used in many cluster systems allow controller redundancy.

In general, access paths to the shared disk must be duplicated to benefit from redundant RAID controller. There are still things to be done to use redundant access paths in Linux (described later in this chapter). If the shared disk has configuration to access the same logical disk unit (LUN) from duplicated multiple controllers simultaneously, and each controller is connected to one server, you can achieve high availability by failover between nodes when an error occurs in one of the controllers.

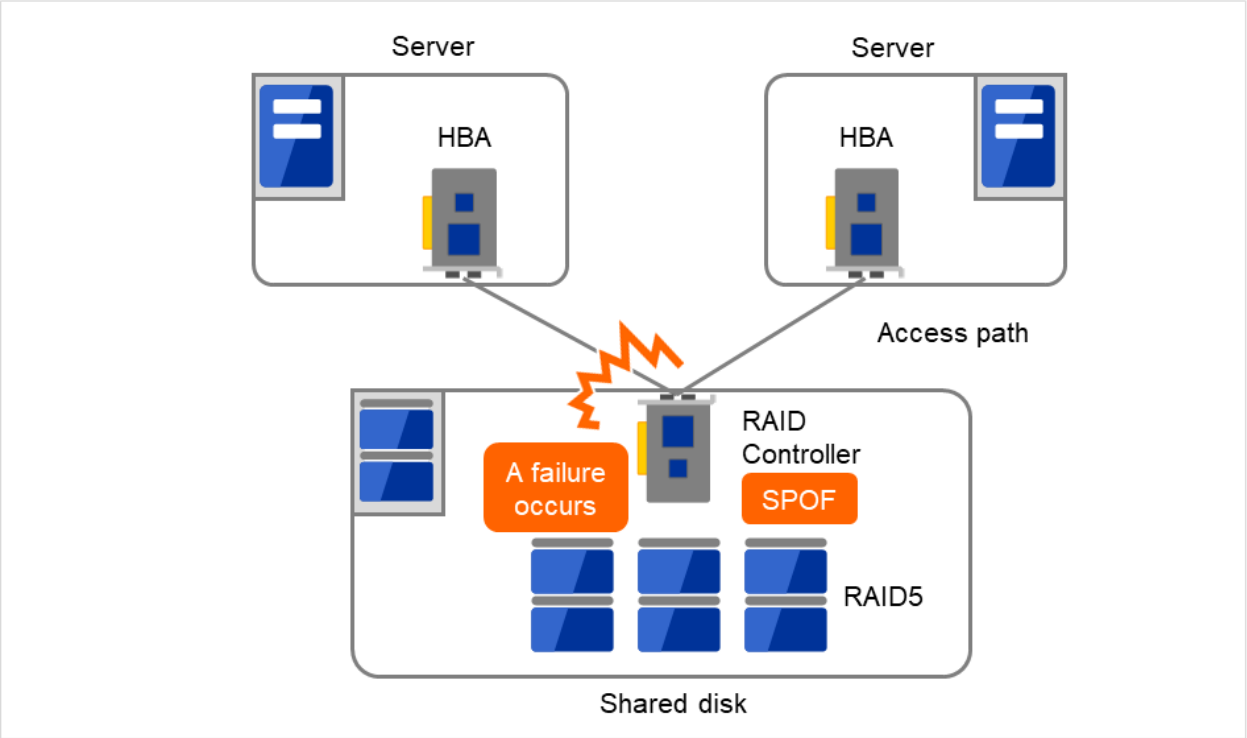


Fig. 2.18: Example of a RAID controller and access paths both being SPOF

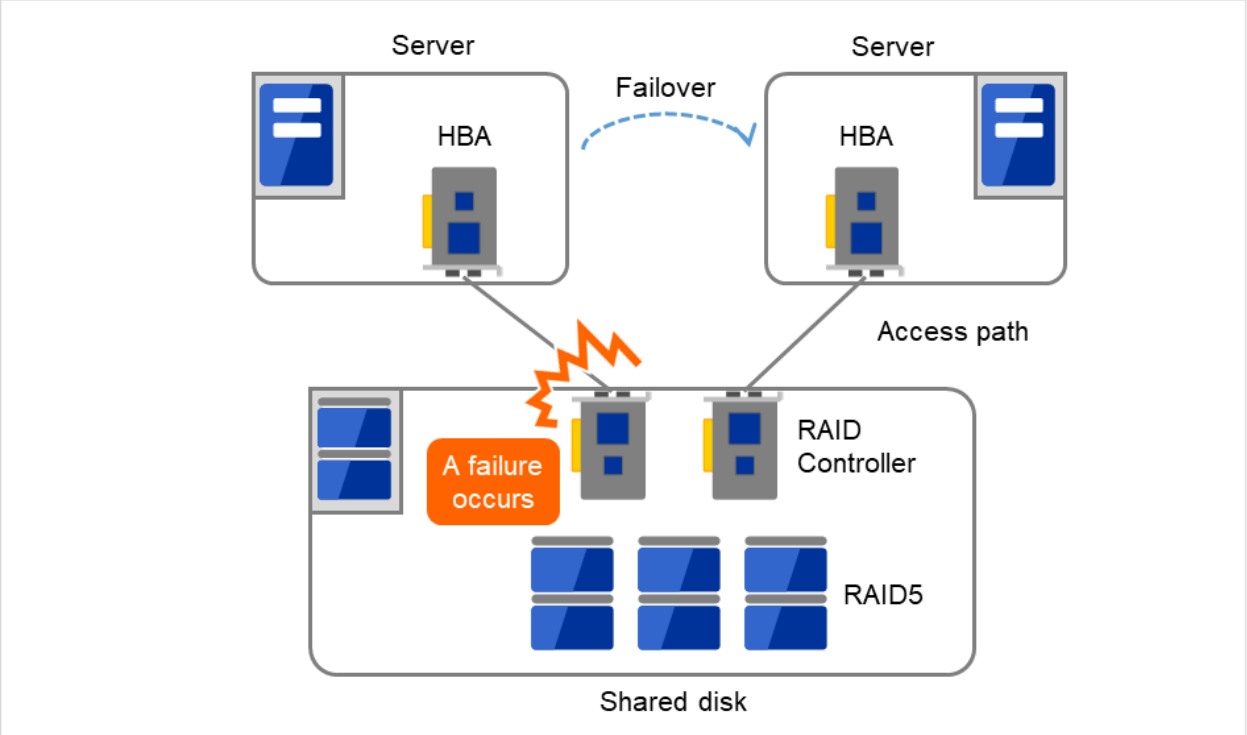


Fig. 2.19: Example of RAID controllers and access paths both being redundant

* HBA stands for Host Bus Adapter. This is an adapter of the server not of the shared disk.

With a failover cluster system of data mirror type, where no shared disk is used, you can create an ideal system having no SPOF because all data is mirrored to the disk in the other server. However you should consider the following issues:

- Degradation of disk I/O performance in mirroring data over the network (especially writing performance)
- Degradation of system performance during mirror resynchronization in recovery from server failure (mirror copy is done in the background)
- Time for mirror resynchronization (failover cannot be done until mirror resynchronization is completed)

In a system with frequent data viewing and a relatively small volume of data, choosing the failover cluster of data mirror type is effective to increase availability.

2.6.2 Access path to the shared disk

In a typical configuration of the shared disk type cluster system, the access path to the shared disk is shared among servers in the cluster. To take SCSI as an example, two servers and a shared disk are connected to a single SCSI bus. A failure in the access path to the shared disk can stop the entire system.

What you can do for this is to have a redundant configuration by providing multiple access paths to the shared disk and make them look as one path for applications. The device driver allowing such is called a path failover driver.

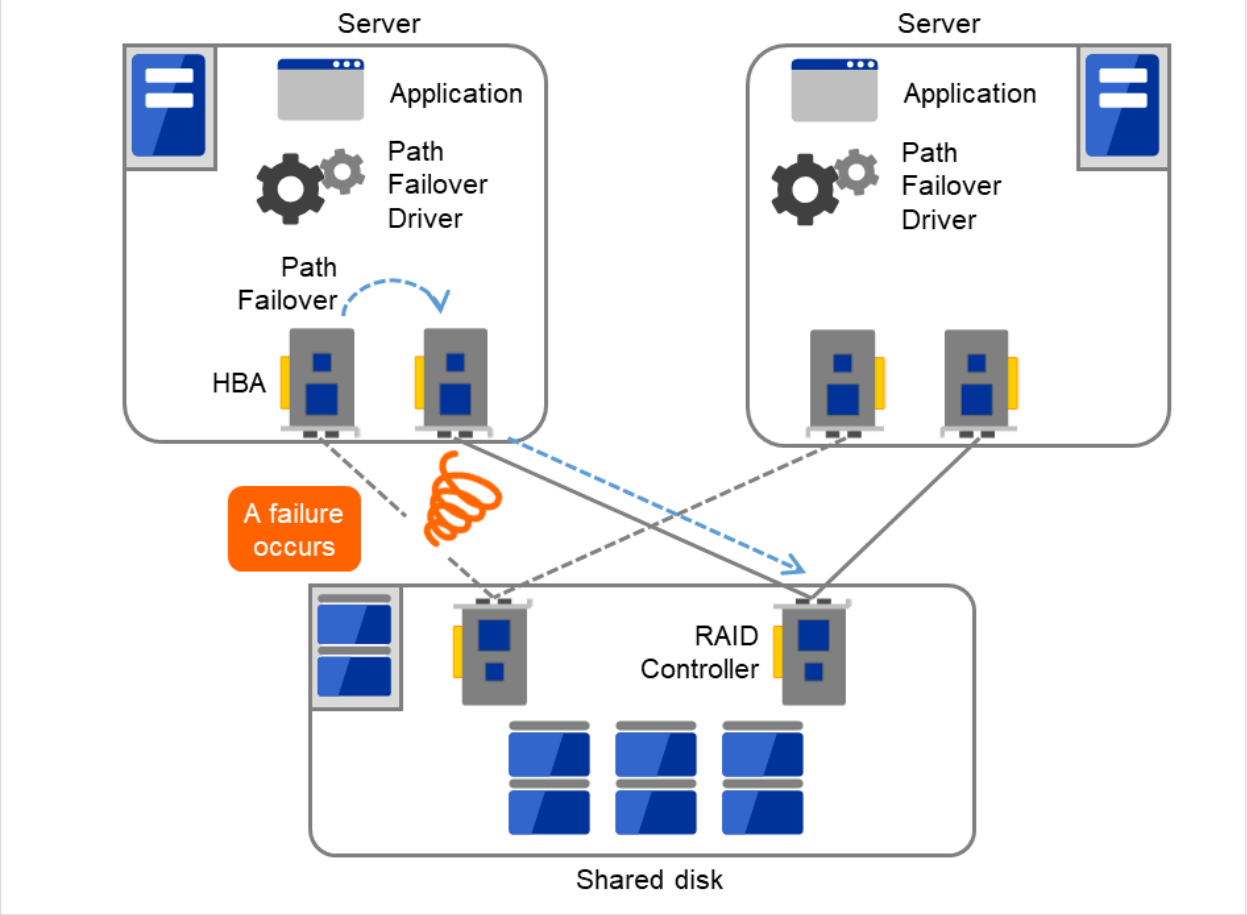


Fig. 2.20: Path failover driver

2.6.3 LAN

In any systems that run services on a network, a LAN failure is a major factor that disturbs operations of the system. If appropriate settings are made, availability of cluster system can be increased through failover between nodes at NIC failures. However, a failure in a network device that resides outside the cluster system disturbs operation of the system.

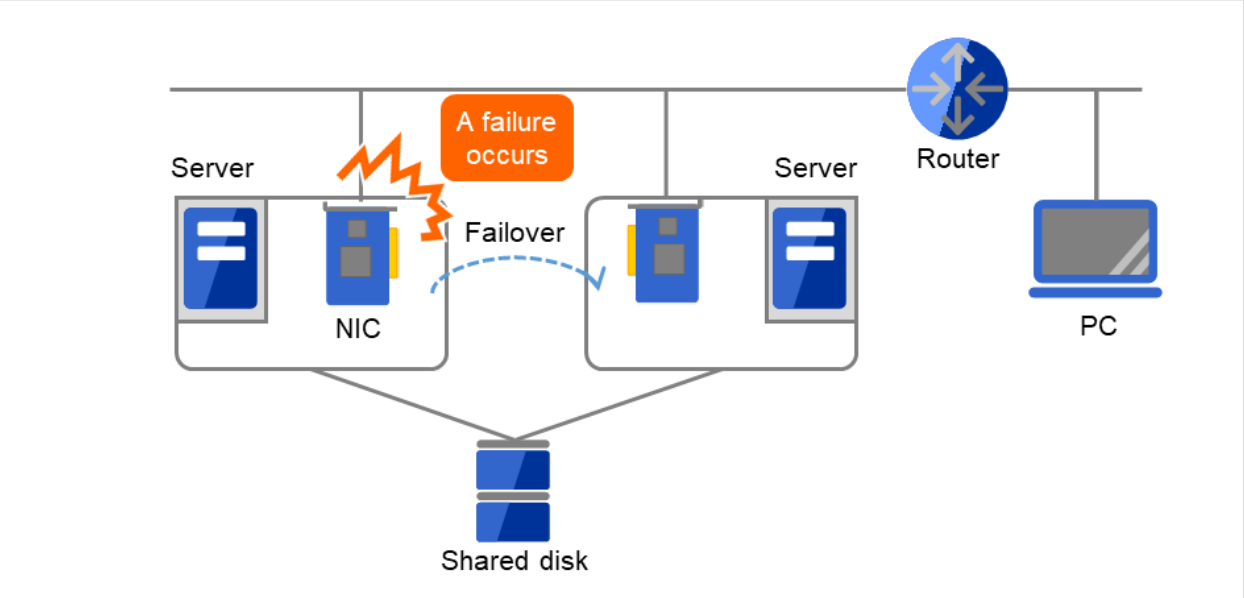


Fig. 2.21: Example of a failure with LAN (NIC)

In the case of this above figure, even if NIC on the server has a failure, a failover will keep the access from the PC to the service on the server.

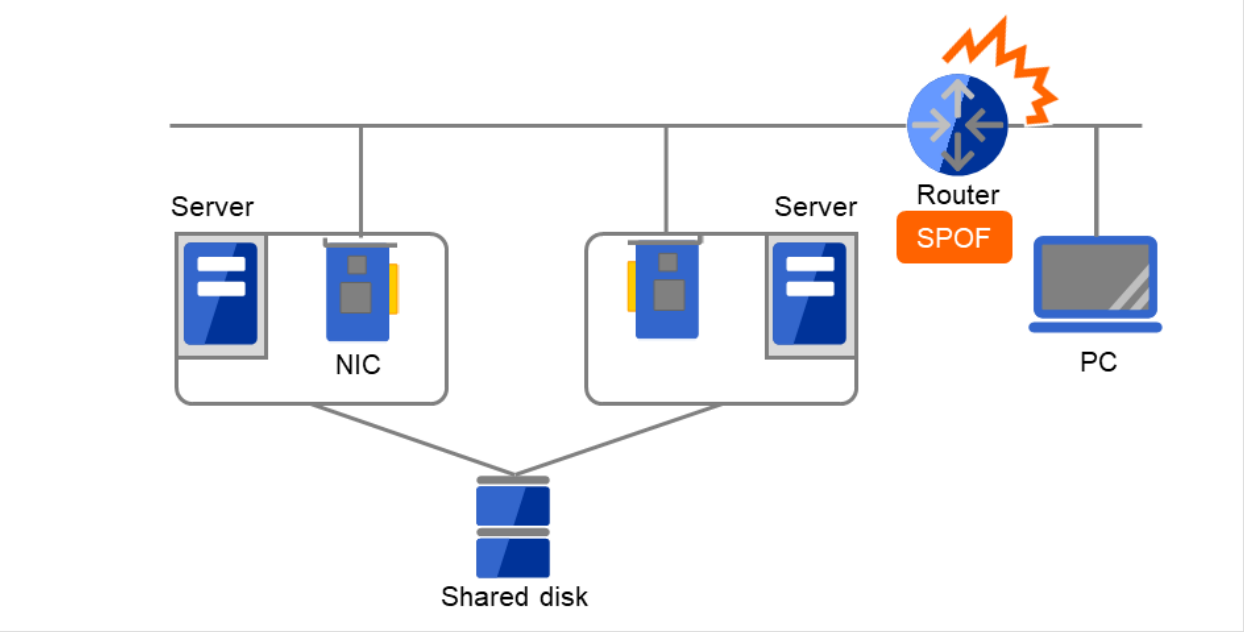


Fig. 2.22: Example of a failure with LAN (Router)

In the case of this above figure, if the router has a failure, the access from the PC to the service on the server cannot be maintained (Router becomes a SPOF).

LAN redundancy is a solution to tackle device failure outside the cluster system and to improve availability. You can apply ways used for a single server to increase LAN availability. For example, choose a primitive way to have a spare network device with its power off, and manually replace a failed device with this spare device. Choose to have a multiplex network path through a redundant configuration of high-performance network devices, and switch paths automatically. Another option is to use a driver that supports NIC redundant configuration such as Intel's ANS driver.

Load balancing appliances and firewall appliances are also network devices that are likely to become SPOF. Typically, they allow failover configurations through standard or optional software. Having redundant configuration for these devices should be regarded as requisite since they play important roles in the entire system.

2.7 Operation for availability

2.7.1 Evaluation before starting operation

Given many of factors causing system troubles are said to be the product of incorrect settings or poor maintenance, evaluation before actual operation is important to realize a high availability system and its stabilized operation. Exercising the following for actual operation of the system is a key in improving availability:

- Clarify and list failures, study actions to be taken against them, and verify effectiveness of the actions by creating dummy failures.
- Conduct an evaluation according to the cluster life cycle and verify performance (such as at degenerated mode)
- Arrange a guide for system operation and troubleshooting based on the evaluation mentioned above.

Having a simple design for a cluster system contributes to simplifying verification and improvement of system availability.

2.7.2 Failure monitoring

Despite the above efforts, failures still occur. If you use the system for long time, you cannot escape from failures: hardware suffers from aging deterioration and software produces failures and errors through memory leaks or operation beyond the originally intended capacity. Improving availability of hardware and software is important yet monitoring for failure and troubleshooting problems is more important. For example, in a cluster system, you can continue running the system by spending a few minutes for switching even if a server fails. However, if you leave the failed server as it is, the system no longer has redundancy and the cluster system becomes meaningless should the next failure occur.

If a failure occurs, the system administrator must immediately take actions such as removing a newly emerged SPOF to prevent another failure. Functions for remote maintenance and reporting failures are very important in supporting services for system administration.

To achieve high availability with a cluster system, you should:

- Remove or have complete control on single point of failure.
- Have a simple design that has tolerance and resistance for failures, and be equipped with a guide for operation and troubleshooting.
- Detect a failure quickly and take appropriate action against it.

CHAPTER

THREE

USING EXPRESSCLUSTER

This chapter explains the components of EXPRESSCLUSTER, how to design a cluster system, and how to use EXPRESSCLUSTER.

This chapter covers:

3.1 What is EXPRESSCLUSTER?

EXPRESSCLUSTER is software that enables the HA cluster system.

3.2 EXPRESSCLUSTER modules

EXPRESSCLUSTER consists of following two modules:

- EXPRESSCLUSTER Server

  A core component of EXPRESSCLUSTER. Install this to the server machines that constitute the cluster system. This includes all high availability functions of EXPRESSCLUSTER. The server functions of the Cluster WebUI are also included.

- Cluster WebUI

  This is a tool to create the configuration data of EXPRESSCLUSTER and to manage EXPRESSCLUSTER operations. Uses a Web browser as a user interface. The Cluster WebUI is installed in EXPRESSCLUSTER Server, but it is distinguished from the EXPRESSCLUSTER Server because the Cluster WebUI is operated from the Web browser on the management PC.

3.3 Software configuration of EXPRESSCLUSTER

The software configuration of EXPRESSCLUSTER should look similar to the figure below. Install the EXPRESSCLUSTER Server (software) on a server that constitutes a cluster. Because the main functions of Cluster WebUI are included in EXPRESSCLUSTER Server, it is not necessary to separately install them. The Cluster WebUI can be used through the web browser on the management PC or on each server in the cluster.

(a) EXPRESSCLUSTER Server (Main module)

(b) Cluster WebUI

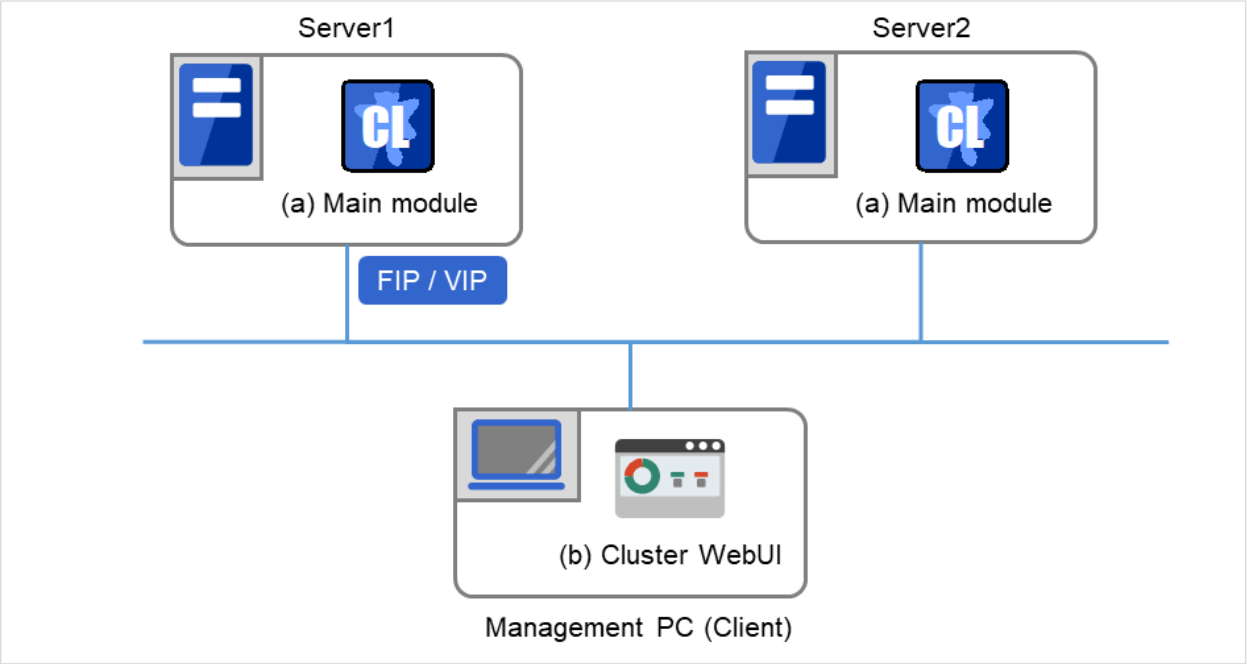


Fig. 3.1: Software configuration of EXPRESSCLUSTER

3.3.1 How an error is detected in EXPRESSCLUSTER

There are three kinds of monitoring in EXPRESSCLUSTER: (1) server monitoring, (2) application monitoring, and (3) internal monitoring. These monitoring functions let you detect an error quickly and reliably. The details of the monitoring functions are described below.

3.3.2 What is server monitoring?

Server monitoring is the most basic function of the failover-type cluster system. It monitors if a server that constitutes a cluster is properly working.
Server Monitoring (heartbeat) uses the following communication paths:

- Primary Interconnect
  LAN dedicated to communication between the cluster servers. This is used to exchange information between the servers as well as to perform heartbeat communication.

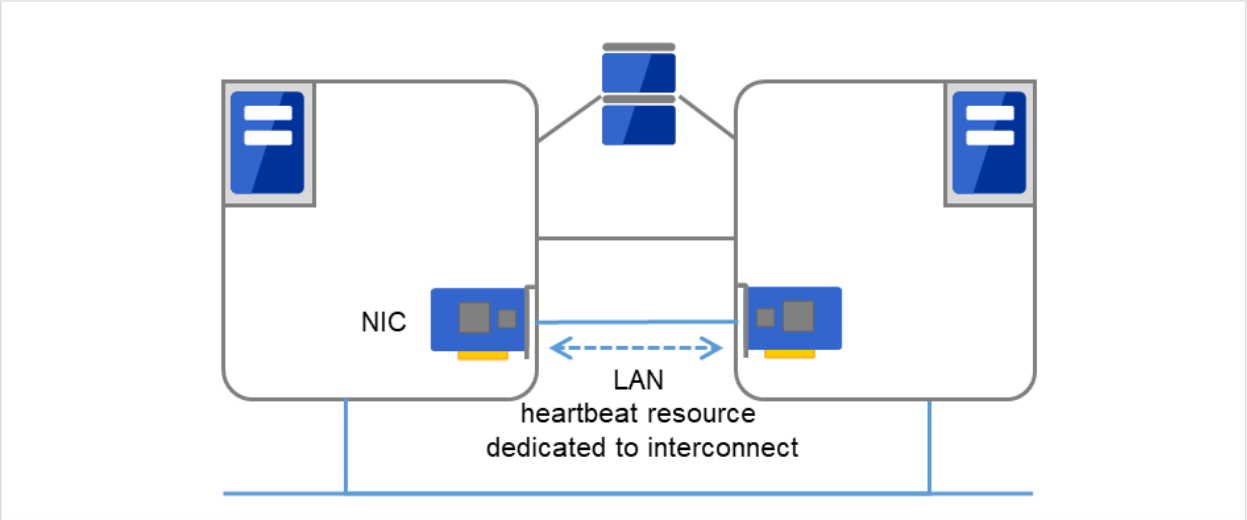


Fig. 3.2: LAN heartbeat/Kernel mode LAN heartbeat (Primary Interconnect)

- Secondary Interconnect
  This is used as a path to be used for the communicating with a client. This is used for exchanging data between the servers as well as for a backup interconnects.

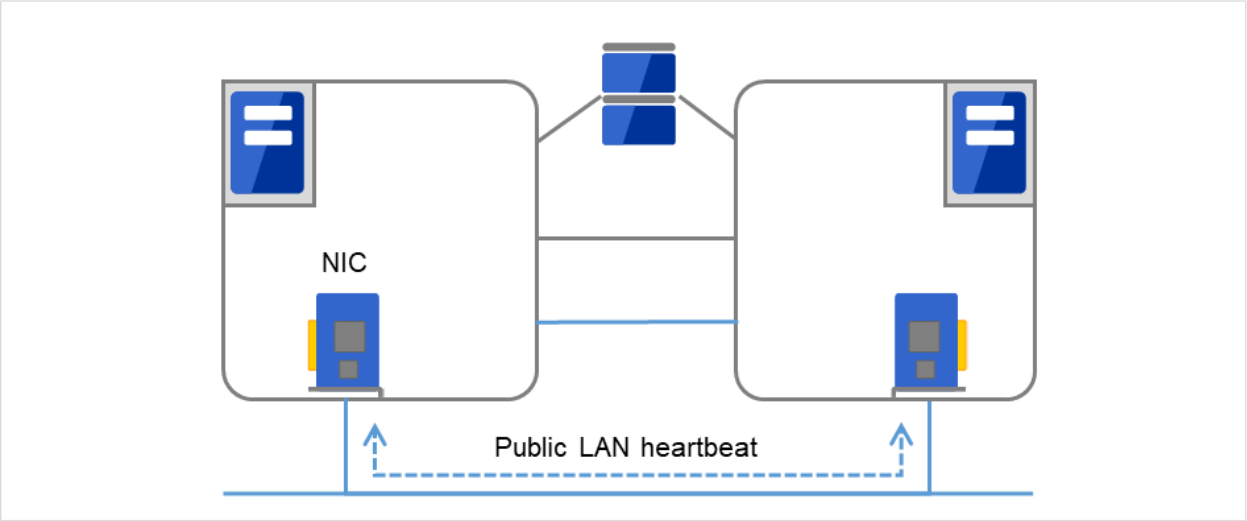


Fig. 3.3: LAN heartbeat/Kernel mode LAN heartbeat (Secondary Interconnect)

- Witness
  This is used by the external Witness server running the Witness server service to check if other servers constructing the failover-type cluster exist through communication with them.

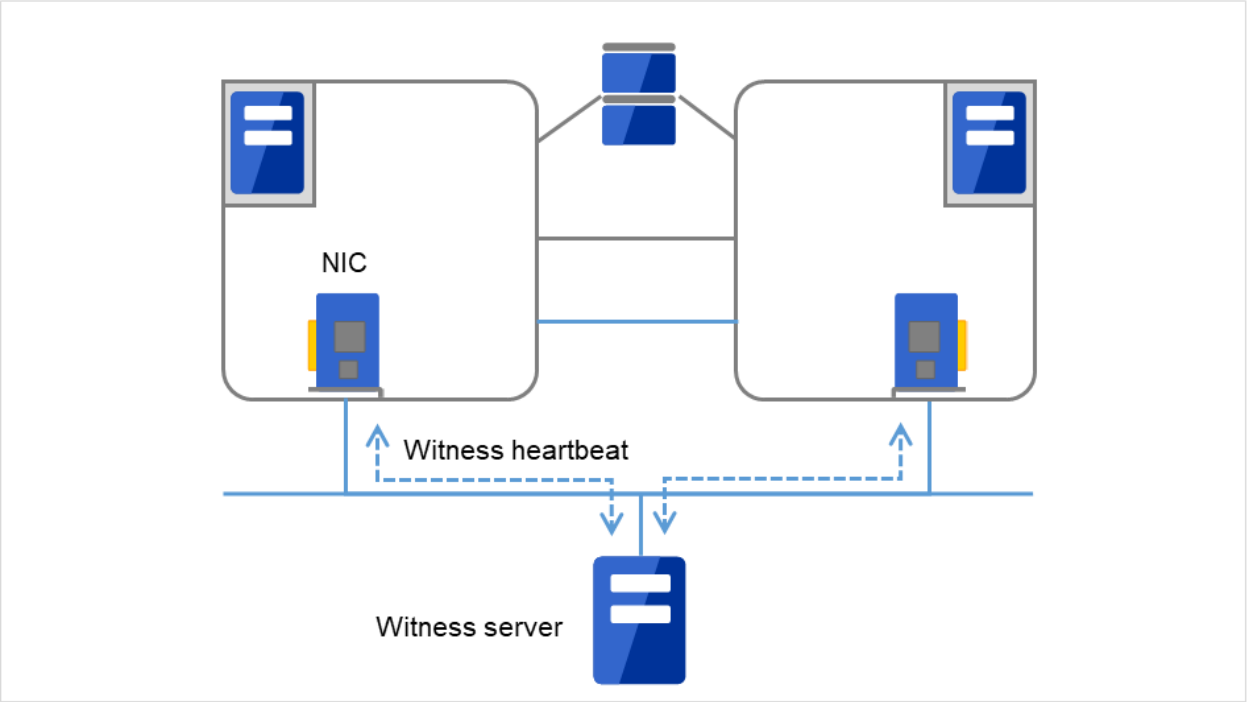


Fig. 3.4: Witness heartbeat

3.3.3 What is application monitoring?

Application monitoring is a function that monitors applications and factors that cause a situation where an application cannot run.

- Monitoring applications and/or protocols to see if they are stalled or failed by using the monitoring option.
  In addition to the basic monitoring of successful startup and existence of applications, you can even monitor stall and failure in applications including specific databases (such as Oracle, DB2), protocols (such as FTP, HTTP) and / or application servers (such as WebSphere, WebLogic) by introducing optional monitoring products of EXPRESSCLUSTER. For the details, see "Monitor resource details" in the "Reference Guide".
- Monitoring activation status of applications
  An error can be detected by starting up an application by using an application-starting resource (called application resource and service resource) of EXPRESSCLUSTER and regularly checking whether the process is active or not by using application-monitoring resource (called application monitor resource and service monitor resource). It is effective when the factor for application to stop is due to error termination of an application.

Note:

- An error in resident process cannot be detected in an application started up by EXPRESSCLUSTER.

Note:

- An internal application error (for example, application stalling and result error) cannot be detected.

- Resource monitoring

An error can be detected by monitoring the cluster resources (such as disk partition and IP address) and public LAN using the monitor resources of the EXPRESSCLUSTER. It is effective when the factor for application to stop is due to an error of a resource that is necessary for an application to operate.

3.3.4 What is internal monitoring?

Internal monitoring refers to an inter-monitoring of modules within EXPRESSCLUSTER. It monitors whether each monitoring function of EXPRESSCLUSTER is properly working. Activation status of EXPRESSCLUSTER process monitoring is performed within EXPRESSCLUSTER.

- Monitoring activation status of an EXPRESSCLUSTER process

3.3.5 Monitorable and non-monitorable errors

There are monitorable and non-monitorable errors in EXPRESSCLUSTER. It is important to know what kind of errors can or cannot be monitored when building and operating a cluster system.

3.3.6 Detectable and non-detectable errors by server monitoring

Monitoring conditions: A heartbeat from a server with an error is stopped

- Example of errors that can be monitored:
  - Hardware failure (of which OS cannot continue operating)
  - Stop error
- Example of error that cannot be monitored:
  - Partial failure on OS (for example, only a mouse or keyboard does not function)

3.3.7 Detectable and non-detectable errors by application monitoring

Monitoring conditions: Termination of application with errors, continuous resource errors, disconnection of a path to the network devices.

- Example of errors that can be monitored:
  - Abnormal termination of an application
  - Failure to access the shared disk (such as HBA failure)
  - Public LAN NIC problem
- Example of errors that cannot be monitored:
  - Application stalling and resulting in error.
    EXPRESSCLUSTER cannot monitor application stalling and error results[1]. However, it is possible to perform failover by creating a program that monitors applications and terminates itself when an error is detected, starting the program using the application resource, and monitoring application using the application monitor resource.

[1] Stalling and error results can be monitored for the database applications (such as Oracle, DB2), the protocols (such as FTP, HTTP) and application servers (such as WebSphere and WebLogic) that are handled by a monitoring option.

3.4 Fencing Function

EXPRESSCLUSTER's fencing function consists of network partition resolution and forced stopping.

3.4.1 Network partition resolution

Upon detecting that a heartbeat from a server is interrupted, EXPRESSCLUSTER determines whether the cause of this interruption is an error in a server or a network partition. If it is judged as a server failure, failover (activate resources and start applications on a healthy server) is performed. If it is judged as a network partition, protecting data is given priority over operations and a processing such as emergency shutdown is performed.
The following are the network partition resolution methods:

- PING method
- HTTP method
- Shared disk method
- PING + shared disk method
- Majority method
- Not solving the network partition

See also:

For the details on the network partition resolution method, see "Details on network partition resolution resources" in the "Reference Guide".

3.4.2 Forced stop

When a server failure is detected, a healthy server can send a stop request to the failed server. Making the failed server stop eliminates the possibility of simultaneously starting business applications on two or more servers. The forced stop is made before a failover is started.

See also:

For the details on the forced stop function, see "Forced stop resource details" in the "Reference Guide".

3.5 Failover mechanism

Upon detecting that a heartbeat from a server is interrupted, EXPRESSCLUSTER determines whether the cause of this interruption is an error in a server or a network partition before starting a failover. Then a failover is performed by activating various resources and starting up applications on a properly working server.

The group of resources which fail over at the same time is called a "failover group." From a user's point of view, a failover group appears as a virtual computer.

Note: In a cluster system, a failover is performed by restarting the application from a properly working node. Therefore, what is saved in an application memory cannot be failed over.

From occurrence of error to completion of failover takes a few minutes. See the time-chart below:

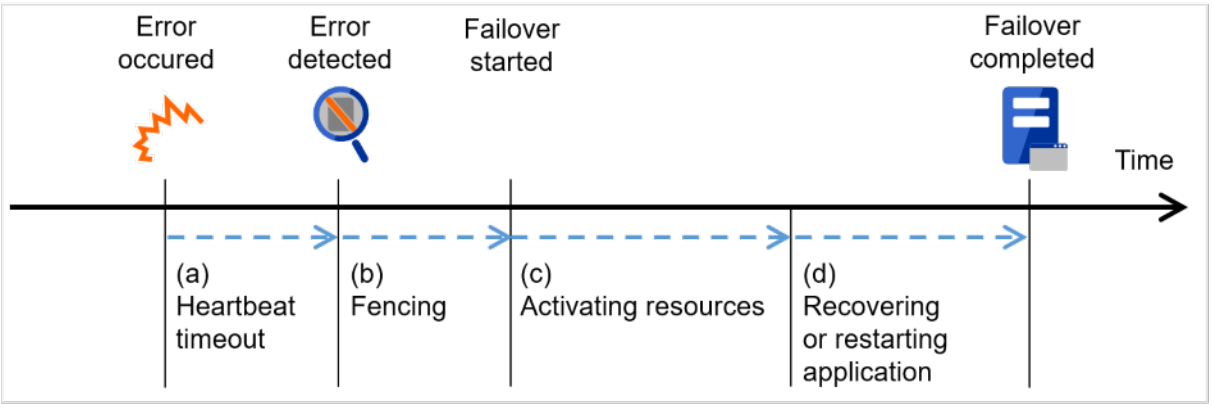


Fig. 3.5: Failover time chart

a. Heartbeat timeout

- The time for a standby server to detect an error after that error occurred on the active server.
- The setting values of the cluster properties should be adjusted depending on the delay caused by application load. (The default value is 30 seconds.)

b. Fencing

- The time for network partition resolution and forced stopping.
- For network partition resolution, EXPRESSCLUSTER checks whether stop of heartbeat (heartbeat timeout) detected from the other server is due to a network partition or an error in the other server.
  Confirmation completes immediately.
- For forced stopping, a stop request is sent to the server that is recognized to be the failure source.
  How long it will take varies depending on the cluster's operating environment such as a physical one, a virtual one, or the cloud.

c. Activating resources

- The time to activate the resources necessary for operating an application.
- The file system recovery, transfer of the data in disks, and transfer of IP addresses are performed.
- The resources can be activated in a few seconds in ordinary settings, but the required time changes depending on the type and the number of resources registered to the failover group. For more information, see the "Installation and Configuration Guide".

d. Recovering and restarting applications

- The startup time of the application to be used in operation. The data recovery time such as a roll-back or roll-forward of the database is included.
- The time for roll-back or roll-forward can be predicted by adjusting the check point interval. For more information, refer to the document that comes with each software product.

3.5.1 Hardware configuration of the shared disk type cluster configured by EXPRESSCLUSTER

The hardware configuration of the shared disk type cluster in EXPRESSCLUSTER is described below. In general, the following is used for communication between the servers in a cluster system:

- Two NIC cards (one for external communication, one for EXPRESSCLUSTER)
- Specific space of a shared disk

SCSI or FibreChannel can be used for communication interface to a shared disk; however, recently FibreChannel is more commonly used.

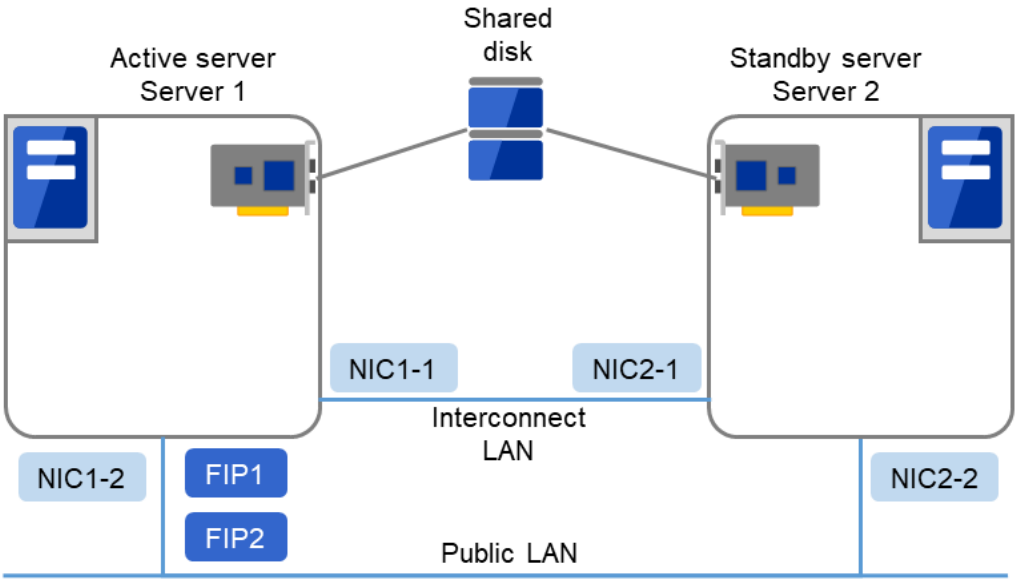


Fig. 3.6: Example of cluster configuration (Shared disk type)

FIP1	10.0.0.11 (Access destination from the Cluster WebUI client)
FIP2	10.0.0.12 (Access destination from the operation client)
NIC1-1	192.168.0.1
NIC1-2	10.0.0.1
NIC2-1	192.168.0.2
NIC2-2	10.0.0.2

- Shared disk:

Drive letter of the partition for disk heartbeat	E
Drive letter of the disk resource	F
File system	NTFS

3.5.2 Hardware configuration of the mirror disk type cluster configured by EXPRESSCLUSTER

The mirror disk type cluster is an alternative to the shared disk device, by mirroring the partition on the server disks. This is good for the systems that are smaller-scale and lower-budget, compared to the shared disk type cluster.

Note: To use a mirror disk, it is a requirement to purchase the Replicator option or the Replicator DR option.

A network for copying mirror disk data is required, but normally interconnect (NIC for EXPRESSCLUSTER internal communication) is used for this purpose.
The hardware configuration of the data mirror type cluster configured by EXPRESSCLUSTER is described below.

- Sample cluster environment with mirror disks used (when the cluster partitions and data partitions are allocated to the OS-installed disks)

  In the following configuration, free partitions of the OS-installed disks are used as cluster partitions and data partitions.

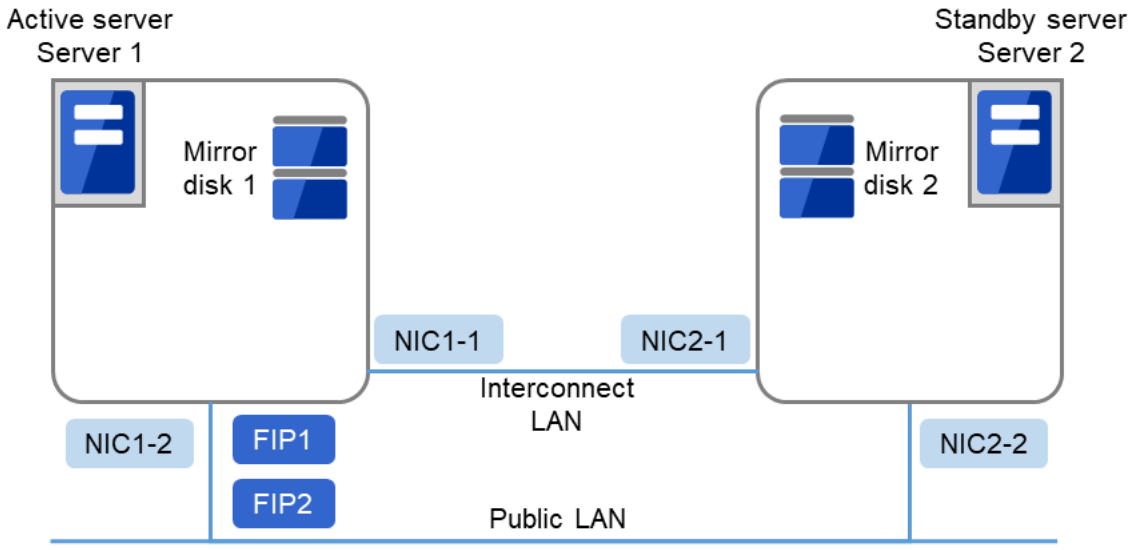


Fig. 3.7: Example of cluster configuration (1) (Mirror disk type)

FIP1	10.0.0.11 (Access destination from the Cluster WebUI client)
FIP2	10.0.0.12 (Access destination from the operation client)
NIC1-1	192.168.0.1
NIC1-2	10.0.0.1
NIC2-1	192.168.0.2
NIC2-2	10.0.0.2

Drive letter of the cluster partition	E
File system	RAW
Drive letter of the data partition	F
File system	NTFS

- Sample cluster environment with mirror disks used (when disks are prepared for cluster partitions and data partitions)

  In the following configuration, disks are prepared for cluster partitions and data partitions and connected to the servers.

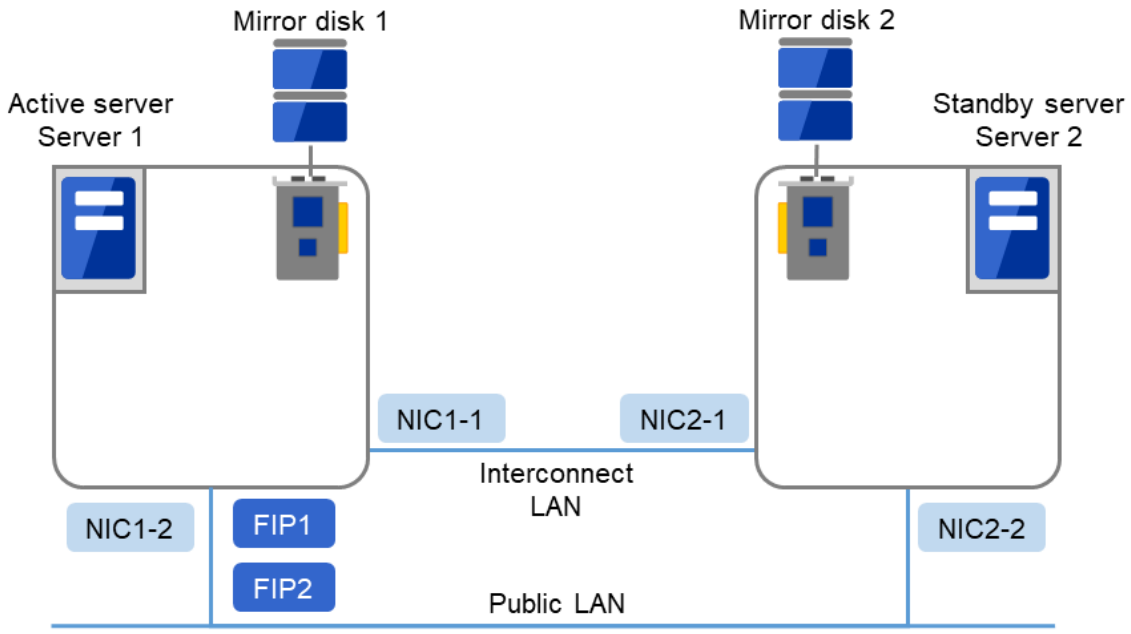


Fig. 3.8: Example of cluster configuration (2) (Mirror disk type)

FIP1	10.0.0.11 (Access destination from the Cluster WebUI client)
FIP2	10.0.0.12 (Access destination from the operation client)
NIC1-1	192.168.0.1
NIC1-2	10.0.0.1
NIC2-1	192.168.0.2
NIC2-2	10.0.0.2

Drive letter of the cluster partition	E
File system	RAW
Drive letter of the data partition	F
File system	NTFS

3.5.3 Hardware configuration of the hybrid disk type cluster configured by EXPRESSCLUSTER

By combining the shared disk type and the mirror disk type and mirroring the partitions on the shared disk, this configuration allows the ongoing operation even if a failure occurs on the shared disk device. Mirroring between remote sites can also serve as a disaster countermeasure.

Note: To use the hybrid disk type configuration, it is a requirement to purchase the Replicator DR option.

As is the case with the mirror disk configuration, a network to copy the data is necessary. In general, NIC for internal communication in EXPRESSCLUSTER is used to meet this purpose.
The hardware configuration of the hybrid disk type cluster configured by EXPRESSCLUSTER is as follows:

- Sample cluster environment with hybrid disks used (a shared disk is used by two servers and the data is mirrored to the normal disk of the third server)

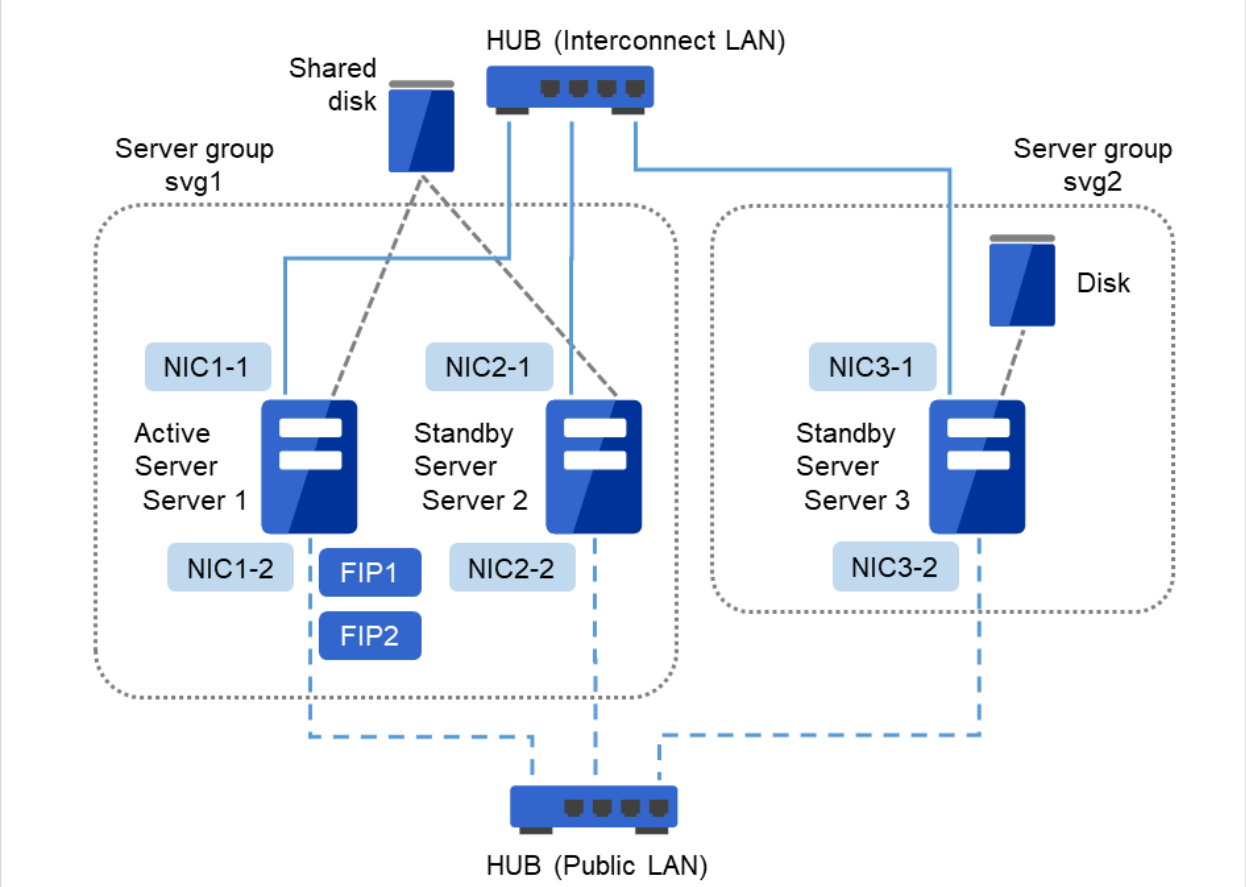


Fig. 3.9: Example of cluster configuration (Hybrid disk type)

FIP1	10.0.0.11 (Access destination from the Cluster WebUI client)
FIP2	10.0.0.12 (Access destination from the operation client)
NIC1-1	192.168.0.1
NIC1-2	10.0.0.1
NIC2-1	192.168.0.2
NIC2-2	10.0.0.2
NIC3-1	192.168.0.3
NIC3-2	10.0.0.3

- Shared disk

Drive letter of the partition for heartbeat	E
File system	RAW
Drive letter of the cluster partition	F
File system	RAW
Drive letter of the data partition	G

Continued on next page

Table 3.8 – continued from previous page

File system	NTFS

The above figure shows a sample of the cluster environment where a shared disk is mirrored in the same network. While the hybrid disk type configuration mirrors between server groups that are connected to the same shared disk device, the sample above mirrors the shared disk to the local disk in server3. Because of this, the stand-by server group svg2 has only one member server, server3.

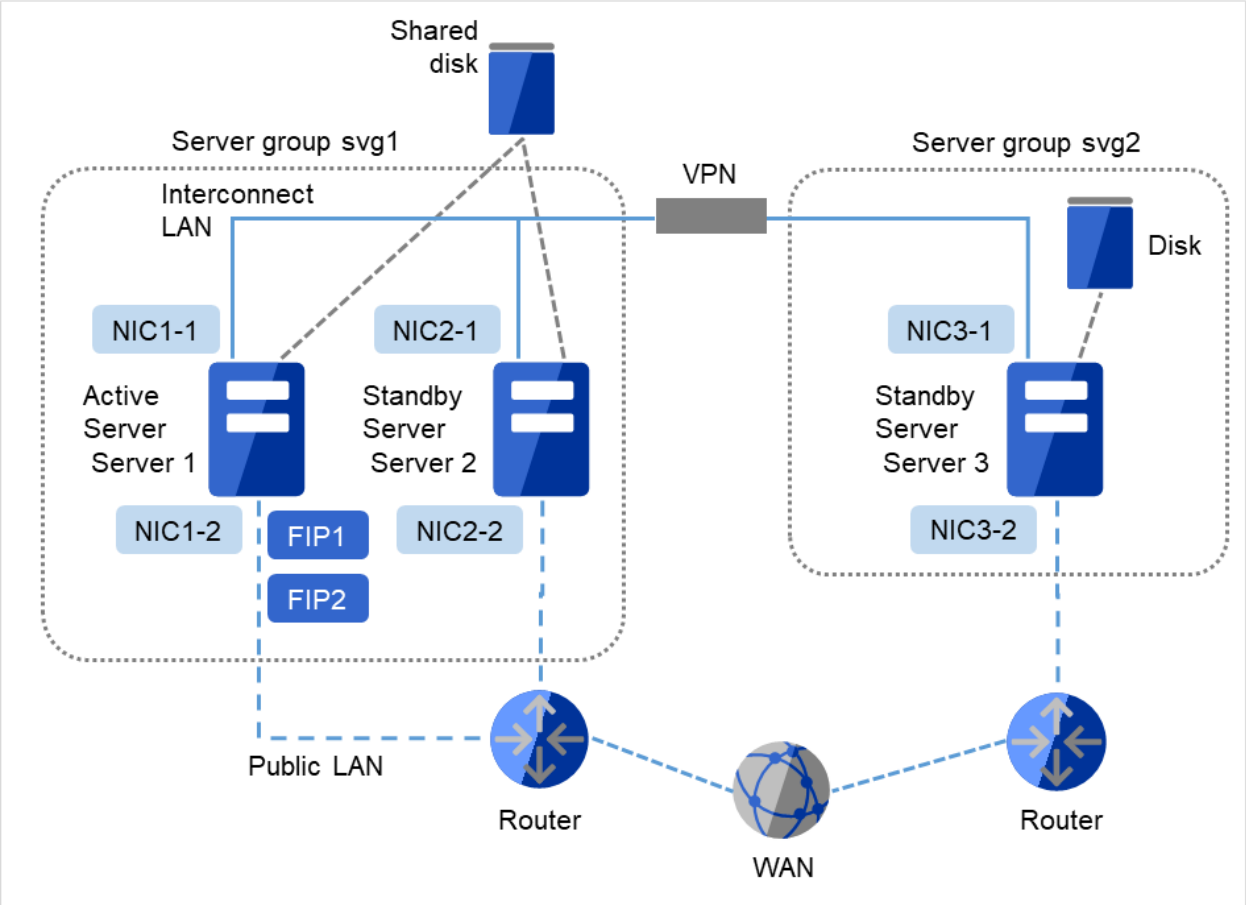


Fig. 3.10: Example of cluster configuration (Hybrid disk type, remote cluster)

FIP1	10.0.0.11 (Access destination from the Cluster WebUI client)
FIP2	10.0.0.12 (Access destination from the operation client)
NIC1-1	192.168.0.1
NIC1-2	10.0.0.1
NIC2-1	192.168.0.2
NIC2-2	10.0.0.2
NIC3-1	192.168.0.3
NIC3-2	10.0.0.3

- Shared disk

Drive letter of the partition for heartbeat	E
File system	RAW

Continued on next page

Table 3.10 – continued from previous page

Drive letter of the cluster partition	F
File system	RAW
Drive letter of the data partition	G
File system	NTFS

The above sample shows a sample of the cluster environment where mirroring is performed between remote sites. This sample uses virtual IP addresses but not floating IP addresses because the server groups have different network segments of the Public-LAN. When a virtual IP address is used, all the routers located in between must be configured to pass on the host route. The mirror connect communication transfers the write data to the disk as it is. It is recommended to enable use a VPN with a dedicated line or the compression and encryption functions.

3.5.4 What is cluster object?

In EXPRESSCLUSTER, the various resources are managed as the following groups:

- **Cluster object**
  Configuration unit of a cluster.
- **Server object**
  Indicates the physical server and belongs to the cluster object.
- **Server group object**
  Indicates a group that bundles servers and belongs to the cluster object. This object is required when a hybrid disk resource is used.
- **Heartbeat resource object**
  Indicates the network part of the physical server and belongs to the server object.
- **Network partition resolution resource object**
  Indicates the network partition resolution mechanism and belongs to the server object.
- **Group object**
  Indicates a virtual server and belongs to the cluster object.
- **Group resource object**
  Indicates resources (network, disk) of the virtual server and belongs to the group object.
- **Monitor resource object**
  Indicates monitoring mechanism and belongs to the cluster object.

3.6 What is a resource?

In EXPRESSCLUSTER, a group used for monitoring the target is called "resources." The resources that perform monitoring and those to be monitored are classified into two groups and managed. There are four types of resources and are managed separately. Having resources allows distinguishing what is monitoring and what is being monitored more clearly. It also makes building a cluster and handling an error easy. The resources can be divided into heartbeat resources, network partition resolution resources, group resources, and monitor resources.

See also:

For the details of each resource, see the "Reference Guide".

3.6.1 Heartbeat resources

Heartbeat resources are used for verifying whether the other server is working properly between servers. The following heartbeat resources are currently supported:

- **LAN heartbeat resource**
  Uses Ethernet for communication.
- **Witness heartbeat resource**
  Uses the external server running the Witness server service to show the status (of communication with each server) obtained from the external server.

3.6.2 Network partition resolution resources

The following resource is used to resolve a network partition:

- **DISK network partition resolution resource**
  This is a network partition resolution resource by the DISK method and can be used only for the shared disk configuration.
- **PING network partition resolution resource**
  This is a network partition resolution resource by the PING method.
- **HTTP network partition resolution resource**
  Uses the external server running the Witness server service to show the status (of communication with each server) obtained from the external server.
- **Majority network partition resolution resource**
  This is a network partition resolution resource by the majority method.

3.6.3 Group resources

A group resource constitutes a unit when a failover occurs. The following group resources are currently supported:

- **Application resource (appli)**
  Provides a mechanism for starting and stopping an application (including user creation application.)
- **Floating IP resource (fip)**
  Provides a virtual IP address. A client can access a virtual IP address the same way as accessing a regular IP address.
- **Mirror disk resource (md)**

Provides a function to perform mirroring a specific partition on the local disk and control access to it. It can be used only on a mirror disk configuration.

- **Registry synchronization resource (regsync)**
  Provides a mechanism to synchronize specific registries of more than two servers, to set the applications and services in the same way among the servers that constitute a cluster.
- **Script resource (script)**
  Provides a mechanism for starting and stopping a script (BAT) such as a user creation script.
- **Disk resource (sd)**
  Provides a function to control access to a specific partition on the shared disk. This can be used only when the shared disk device is connected.
- **Service resource (service)**
  Provides a mechanism for starting and stopping a service such as database and Web.
- **Virtual computer name resource (vcom)**
  Provides a virtual computer name. This can be accessed from a client in the same way as a general computer name.
- **Dynamic DNS resource (ddns)**
  Registers a virtual host name and the IP address of the active server to the dynamic DNS server.
- **Virtual IP resource (vip)**
  Provides a virtual IP address. This can be accessed from a client in the same way as a general IP address. This can be used in the remote cluster configuration among different network addresses.
- **CIFS resource (cifs)**
  Provides a function to disclose and share folders on the shared disk and mirror disks.
- **Hybrid disk resource (hd)**
  A resource in which the disk resource and the mirror disk resource are combined. Provides a function to perform mirroring on a certain partition on the shared disk or the local disk and to control access.
- **AWS elastic ip resource (awseip)**
  Provides a system for giving an elastic IP (referred to as EIP) when EXPRESSCLUSTER is used on AWS.
- **AWS virtual ip resource (awsvip)**
  Provides a system for giving a virtual IP (referred to as VIP) when EXPRESSCLUSTER is used on AWS.
- **AWS secondary ip resource (awssip)**
  Provides a system for giving a secondary IP when EXPRESSCLUSTER is used on AWS.
- **AWS DNS resource (awsdns)**
  Registers the virtual host name and the IP address of the active server to Amazon Route 53 when EXPRESSCLUSTER is used on AWS.
- **Azure probe port resource (azurepp)**
  Provides a system for opening a specific port on a node on which the operation is performed when EXPRESSCLUSTER is used on Microsoft Azure.
- **Azure DNS resource (azuredns)**
  Registers the virtual host name and the IP address of the active server to Azure DNS when EXPRESSCLUSTER is used on Microsoft Azure.
- **Google Cloud virtual IP resource (gcvip)**
  Provides a system for opening a specific port on a node on which the operation is performed when EXPRESSCLUSTER is used on Google Cloud Platform.

- **Google Cloud DNS resource (gcdns)**
  Registers the virtual host name and the IP address of the active server to Cloud DNS when EXPRESSCLUSTER is used on Google Cloud Platform.
- **Oracle Cloud virtual IP resource (ocvip)**
  Provides a system for opening a specific port on a node on which the operation is performed when EXPRESSCLUSTER is used on Oracle Cloud Infrastructure.

Note:

To use a mirror disk resource, the EXPRESSCLUSTER X Replicator license or the EXPRESSCLUSTER X Replicator DR license is required.
To use a hybrid disk resource, the EXPRESSCLUSTER X Replicator DR license is required.
Above resources are not listed on the resource list of the Cluster WebUI if the licenses of those are not registered.

3.6.4 Monitor resources

A monitor resource monitors a cluster system. The following monitor resources are currently supported:

- **Application monitor resource (appliw)**
  Provides a monitoring mechanism to check whether a process started by application resource is active or not.
- **Disk RW monitor resource (diskw)**
  Provides a monitoring mechanism for the file system and function to perform a failover by resetting the hardware or an intentional stop error at the time of file system I/O stalling. This can be used for monitoring the file system of the shared disk.
- **Floating IP monitor resource (fipw)**
  Provides a monitoring mechanism of the IP address started by floating IP resource.
- **IP monitor resource (ipw)**
  Provides a mechanism for monitoring the network communication.
- **Mirror disk monitor resource (mdw)**
  Provides a monitoring mechanism of the mirroring disks.
- **NIC Link Up/Down monitor resource (miiw)**
  Provides a monitoring mechanism for link status of LAN cable.
- **Multi target monitor resource (mtw)**
  Provides a status with multiple monitor resources.
- **Registry synchronization monitor resource (regsyncw)**
  Provides a monitoring mechanism of the synchronization process by a registry synchronization resource.
- **Disk TUR monitor resource (sdw)**
  Provides a mechanism to monitor the operation of access path to the shared disk by the TestUnitReady command of SCSI. This can be used for the shared disk of FibreChannel.
- **Service monitor resource (servicew)**
  Provides an alive monitoring mechanism for services.
- **Virtual computer name monitor resource (vcomw)**
  Provides a monitoring mechanism of the virtual computer started by a virtual computer name resource.
- **Dynamic DNS monitor resource (ddnsw)**

Periodically registers a virtual host name and the IP address of the active server to the dynamic DNS server.

- **Virtual IP monitor resource (vipw)**
  Provides a monitoring mechanism of the IP address started by a virtual IP resource.
- **CIFS resource (cifsw)**
  Provides a monitoring mechanism of the shared folder disclosed by a CIFS resource.
- **Hybrid disk monitor resource (hdw)**
  Provides a monitoring mechanism of the hybrid disk.
- **Hybrid disk TUR monitor resource (hdtw)**
  Provides a monitoring mechanism for the behavior of the access path to the shared disk device used as a hybrid disk by the TestUnitReady command. It can be used for a shared disk using FibreChannel.
- **Custom monitor resource (genw)**
  Provides a monitoring mechanism to monitor the system by the operation result of commands or scripts which perform monitoring, if any.
- **Process name monitor resource (psw)**
  Provides a monitoring mechanism for checking whether a process specified by a process name is active.
- **DB2 monitor resource (db2w)**
  Provides a monitoring mechanism for the IBM DB2 database.
- **ODBC monitor resource (odbcw)**
  Provides a monitoring mechanism for the database that can be accessed by ODBC.
- **Oracle monitor resource (oraclew)**
  Provides a monitoring mechanism for the Oracle database.
- **PostgreSQL monitor resource (psqlw)**
  Provides a monitoring mechanism for the PostgreSQL database.
- **SQL Server monitor resource (sqlserverw)**
  Provides a monitoring mechanism for the SQL Server database.
- **FTP monitor resource (ftpw)**
  Provides a monitoring mechanism for the FTP server.
- **HTTP monitor resource (httpw)**
  Provides a monitoring mechanism for the HTTP server.
- **IMAP4 monitor resource (imap4w)**
  Provides a monitoring mechanism for the IMAP server.
- **POP3 monitor resource (pop3w)**
  Provides a monitoring mechanism for the POP server.
- **SMTP monitor resource (smtpw)**
  Provides a monitoring mechanism for the SMTP server.
- **Tuxedo monitor resource (tuxw)**
  Provides a monitoring mechanism for the Tuxedo application server.
- **WebLogic monitor resource (wlsw)**
  Provides a monitoring mechanism for the WebLogic application server.
- **WebSphere monitor resource (wasw)**
  Provides a monitoring mechanism for the WebSphere application server.

- **WebOTX monitor resource (otxw)**
  Provides a monitoring mechanism for the WebOTX application server.
- **Message receive monitor resource (mrw)**
  Specifies the action to take when an error message is received and how the message is displayed on the Cluster WebUI.
- **JVM monitor resource (jraw)**
  Provides a monitoring mechanism for Java VM.
- **System monitor resource (sraw)**
  Provides a monitoring mechanism for the resources of the whole system.
- **Process resource monitor resource (psrw)**
  Provides a monitoring mechanism for running processes on the server.
- **User mode monitor resource (userw)**
  Provides a stall monitoring mechanism for the user space and a function for performing failover by an intentional STOP error or an HW reset at the time of a user space stall.
- **AWS Elastic Ip monitor resource (awseipw)**
  Provides a monitoring mechanism for the elastic ip given by the AWS elastic ip (referred to as EIP) resource.
- **AWS Virtual Ip monitor resource (awsvipw)**
  Provides a monitoring mechanism for the virtual ip given by the AWS virtual ip (referred to as VIP) resource.
- **AWS Secondary Ip monitor resource (awssipw)**
  Provides a monitoring mechanism for the secondary ip given by the AWS secondary ip resource.
- **AWS AZ monitor resource (awsazw)**
  Provides a monitoring mechanism for an Availability Zone (referred to as AZ).
- **AWS DNS monitor resource (awsdnsw)**
  Provides a monitoring mechanism for the virtual host name and IP address provided by the AWS DNS resource.
- **Azure probe port monitor resource (azureppw)**
  Provides a monitoring mechanism for ports for alive monitoring for the node where an Azure probe port resource has been activated.
- **Azure load balance monitor resource (azurelbw)**
  Provides a mechanism for monitoring whether the port number that is same as the probe port is open for the node where an Azure probe port resource has not been activated.
- **Azure DNS monitor resource (azurednsw)**
  Provides a monitoring mechanism for the virtual host name and IP address provided by the Azure DNS resource.
- **Google Cloud virtual IP monitor resource (gcvipw)**
  Provides a mechanism for monitoring the alive-monitoring port for the node where a Google Cloud virtual IP resource has been activated.
- **Google Cloud load balance monitor resource (gclbw)**
  Provides a mechanism for monitoring whether the same port number as the health-check port number has already been used, for the node where a Google Cloud virtual IP resource has not been activated.
- **Google Cloud DNS monitor resource (gcdnsw)**
  Provides a monitoring mechanism for the virtual host name and IP address provided by the Google Cloud DNS resource.

- **Oracle Cloud virtual IP monitor resource (ocvipw)**
  Provides a mechanism for monitoring the alive-monitoring port for the node where an Oracle Cloud virtual IP resource has been activated.
- **Oracle Cloud load balance monitor resource (oclbw)**
  Provides a mechanism for monitoring whether the same port number as the health-check port number has already been used, for the node where an Oracle Cloud virtual IP resource has not been activated.

Note:

To use the DB2 monitor resource, ODBC monitor resource, Oracle monitor resource, PostgreSQL monitor resource, and SQL Server monitor resource, the EXPRESSCLUSTER X Database Agent license is required.

To use the FTP monitor resource, HTTP monitor resource, IMAP4 monitor resource, POP3 monitor resource and SMTP monitor resource, the EXPRESSCLUSTER X Internet Server Agent license is required.

To use Tuxedo monitor resource, WebLogic monitor resource, WebSphere monitor resource and WebOTX monitor resource, the EXPRESSCLUSTER X Application Server Agent license is required.

To use the JVM monitor resources, the EXPRESSCLUSTER X Java Resource Agent license is required.

To use the system monitor resources and the process resource monitor resources, the EXPRESSCLUSTER X System Resource Agent license is required.

Above monitor resources are not listed on the monitor resource list of the Cluster WebUI if the licenses of those are not registered.

3.7 Getting started with EXPRESSCLUSTER

Refer to the following guides when building a cluster system with EXPRESSCLUSTER:

3.7.1 Latest information

Refer to "4. *Installation requirements for EXPRESSCLUSTER*", "5. *Latest version information*" and "6. *Notes and Restrictions*" in this guide.

3.7.2 Designing a cluster system

Refer to "Determining a system configuration" and "Configuring a cluster system" in the "Installation and Configuration Guide" and "Group resource details", "Monitor resource details", "Heartbeat resources", "Details on network partition resolution resources", and "Information on other settings" in the "Reference Guide".

3.7.3 Configuring a cluster system

Refer to the "Installation and Configuration Guide"

3.7.4 Troubleshooting the problem

Refer to "The system maintenance information" in the "Maintenance Guide", and "Troubleshooting" and "Error messages" in the "Reference Guide".

CHAPTER

FOUR

INSTALLATION REQUIREMENTS FOR EXPRESSCLUSTER

This chapter provides information on system requirements for EXPRESSCLUSTER.

This chapter covers:

4.1 System requirements for hardware

EXPRESSCLUSTER operates on the following server architectures:

- x86_64

4.1.1 General server requirements

Required specifications for the EXPRESSCLUSTER Server are the following:

- Ethernet port 2 or more ports
- Mirror disk or empty partition for mirror (required when the Replicator is used)
- DVD-ROM drive

4.2 System requirements for the EXPRESSCLUSTER Server

4.2.1 Supported operating systems

EXPRESSCLUSTER Server only runs on the operating systems listed below.

x86_64 version

OS	Remarks
Windows Server 2016 Standard	
Windows Server 2016 Datacenter	
Windows Server 2019 Standard	
Windows Server 2019 Datacenter	
Windows Server 2022 Standard	
Windows Server 2022 Datacenter	

4.2.2 Required memory and disk size

Required memory size (User mode)	256MB([2])
Required memory size (Kernel mode)	32 MB + 4 MB ([3]) x (number of mirror/hybrid resources)
Required disk size (Right after installation)	100MB
Required disk size (During operation)	5.0GB + 9.0GB ([4])

When changing to asynchronous method, changing the queue size or changing the difference bitmap size, it is required to add more memory. Memory size increases as disk load increases because memory is used corresponding to mirror disk I/O.

For the required size of a partition for a DISK network partition resolution resource, see "*Partition for shared disk*".

For the required size of a cluster partition, see "*Partition for mirror disk*" and "*Partition for hybrid disk*".

[2] excepting for optional products.
[3] A single mirror/hybrid disk resource needs 4 MB RAM.
[4] A disk capacity required to use mirror disk resources and hybrid disk resources.

4.2.3 Application supported by the monitoring options

The following applications are the target monitoring options that are supported.

x86_64 version

Monitor resource	Application to be monitored	EXPRESSCLUSTER Version	Remarks
Oracle monitor	Oracle Database 19c (19.3)	13.00 or later	
DB2 monitor	DB2 V11.5	13.00 or later	
PostgreSQL monitor	PostgreSQL 14.1	13.00 or later	
	PowerGres on Windows V13	13.00 or later	
SQL Server monitor	SQL Server 2019	13.00 or later	
Tuxedo monitor	Tuxedo 12c Release 2 (12.1.3)	12.00 or later	
WebLogic monitor	WebLogic Server 11g R1	12.00 or later	
	WebLogic Server 11g R2	12.00 or later	
	WebLogic Server 12c R2 (12.2.1)	12.00 or later	
	WebLogic Server 14c (14.1.1)	12.20 or later	
WebSphere monitor	WebSphere Application Server 8.5	12.00 or later	
	WebSphere Application Server 8.5.5	12.00 or later	
	WebSphere Application Server 9.0	12.00 or later	
WebOTX monitor	WebOTX Application Server V9.1	12.00 or later	
	WebOTX Application Server V9.2	12.00 or later	
	WebOTX Application Server V9.3	12.00 or later	
	WebOTX Application Server V9.4	12.00 or later	
	WebOTX Application Server V9.5	12.00 or later	
	WebOTX Application Server V10.1	12.00 or later	
	WebOTX Application Server V10.3	12.30 or later	
JVM monitor	WebLogic Server 11g R1	12.00 or later	
	WebLogic Server 11g R2	12.00 or later	
	WebLogic Server 12c R2 (12.2.1)	12.00 or later	
	WebLogic Server 14c (14.1.1)	12.20 or later	
	WebOTX Application Server V9.1	12.00 or later	
	WebOTX Application Server V9.2	12.00 or later	
	WebOTX Application Server V9.3	12.00 or later	
	WebOTX Application Server V9.4	12.00 or later	
	WebOTX Application Server V9.5	12.00 or later	
	WebOTX Application Server V10.1	12.00 or later	
	WebOTX Application Server V10.3	12.30 or later	
	WebOTX Enterprise Service Bus V8.4	12.00 or later	
	WebOTX Enterprise Service Bus V8.5	12.00 or later	
	WebOTX Enterprise Service Bus V10.3	12.30 or later	
	Apache Tomcat 8.0	12.00 or later	
	Apache Tomcat 8.5	12.00 or later	
	Apache Tomcat 9.0	12.00 or later	
	Apache Tomcat 10.0	13.02 or later	
	WebSAM SVF for PDF 9.1	12.00 or later	
	WebSAM SVF for PDF 9.2	12.00 or later	
	WebSAM Report Director Enterprise 9.1	12.00 or later	
	WebSAM Report Director Enterprise 9.2	12.00 or later	
	WebSAM Universal Connect/X 9.1	12.00 or later	
	WebSAM Universal Connect/X 9.2	12.00 or later	
System monitor	N/A	12.00 or later	

Continued on next page

Table 4.3 – continued from previous page

Monitor resource	Application to be monitored	EXPRESSCLUSTER Version	Remarks
Process resource monitor	N/A	12.10 or later	

Note: Above monitor resources are executed as 64-bit application in x86_64 environment. So that, the target applications must be 64-bit binaries.

4.2.4 Operation environment for SNMP linkage functions

EXPRESSCLUSTER with SNMP Service of Windows is validated on following OS.

x86_64 version

OS	Remarks
Windows Server 2016	

4.2.5 Operation environment for JVM monitor

The use of the JVM monitor requires a Java runtime environment.

Java® Runtime Environment
Version7.0 Update 6 (1.7.0_6) or later

Java(TM) Runtime Environment
Version 8.0 Update 11 (1.8.0_11) or later

Java(TM) Runtime Environment
Version 9.0 (9.0.1) or later

Java(TM) SE Development Kit
Version 11.0 (11.0.5) or later

4.2.6 Operation environment for system monitor or process resource monitor or function of collecting system resource information

The use of the System Resource Agent requires the Microsoft .NET Framework environment.
Microsoft .NET Framework 4.5 or later

Note: On the OS of Windows Server 2012 or later, NET Framework 4.5 version or later is pre-installed (The version of the pre-installed one varies depending on the OS).

4.2.7 Operation environment for AWS Elastic IP resource, AWS virtual IP resource, AWS Elastic IP monitor resource, AWS Virtual IP monitor resource and AWS AZ monitor resource

The use of the AWS elastic ip resource, AWS virtual ip resource, AWS elastic IP monitor resource, AWS virtual IP monitor resource and AWS AZ monitor resource requires the following software.

Software	Version	Remarks
AWS CLI	1.6.0 or later 2.0.0 or later	
Python	2.7.5 or later 3.6.7 or later 3.8.2 or later	Python accompanying the AWS CLI is not allowed.

4.2.8 Operation environment for AWS secondary IP resource and AWS Secondary IP monitor resource

The use of the AWS secondary IP resource, AWS secondary IP monitor resource requires the following software.

Software	Version	Remarks
AWS CLI	2.0.0 or later	

4.2.9 Operation environment for AWS DNS resource and AWS DNS monitor resource

The use of the AWS DNS resource and AWS DNS monitor resource requires the following software.

Software	Version	Remarks
AWS CLI	1.11.0 or later	
Python	2.7.5 or later 3.6.7 or later 3.8.2 or later	Python accompanying the AWS CLI is not allowed.

4.2.10 Operation environment for AWS forced stop resource

The use of the AWS forced stop resource requires the following software.

Software	Version	Remarks
AWS CLI	2.0.0 or later	

4.2.11 Operation environment for Azure probe port resource, Azure probe port monitor resource and Azure load balance monitor resource

The following are the Microsoft Azure deployment models with which the operation of the Azure probe port resource, Azure probe port monitor resource, and Azure load balance monitor resource has been verified.

For the method to configure a load balancer, refer to "EXPRESSCLUSTER X HA Cluster Configuration Guide for Microsoft Azure (Windows)".

x86_64

Deployment model	EXPRESSCLUSTER Version	Remarks
Resource Manager	12.00 or later	Load balancer is required

4.2.12 Operation environment for Azure DNS resource and Azure DNS monitor resource

The use of the Azure DNS resource and Azure DNS monitor resource requires the following software.

Software	Version	Remarks
Azure CLI	2.0 or later	

For instructions on how to install the Azure CLI, refer to the following:

Install the Azure CLI:
https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest

The following are the Microsoft Azure deployment models with which the operation of the Azure DNS resource and Azure DNS monitor resource has been verified.
For the method to configure Azure DNS, refer to "EXPRESSCLUSTER X HA Cluster Configuration Guide for Microsoft Azure".

x86_64

Deployment model	EXPRESSCLUSTER Version	Remarks
Resource Manager	12.00 or later	Azure DNS is required.

4.2.13 Operation environments for Google Cloud virtual IP resource, Google Cloud virtual IP monitor resource, and Google Cloud load balance monitor resource

The following lists the versions of the OSs on Google Cloud Platform on which the operation of the Google Cloud virtual IP resource, the Google Cloud virtual IP monitor resource, and the Google Cloud load balance monitor resource was verified.

Distribution	EXPRESSCLUSTER Version	Remarks
Windows Server 2016	12.20 or later	
Windows Server 2019	12.20 or later	

4.2.14 Operation environments for Google Cloud DNS resource, Google Cloud DNS monitor resource

The use of the Google Cloud DNS resource, Azure Google Cloud monitor resource requires the following software.

Software	Version	Remarks
Google Cloud SDK	295.0.0~	

For the prerequisites of the Google Cloud SDK and the instructions on how to install it, refer to the following:

Install the Google Cloud SDK:
https://cloud.google.com/sdk/install

4.2.15 Operation environments for Oracle Cloud virtual IP resource, Oracle Cloud virtual IP monitor resource, and Oracle Cloud load balance monitor resource

The following lists the versions of the OSs on Oracle Cloud Infrastructure on which the operation of the Oracle Cloud virtual IP resource, the Oracle Cloud virtual IP monitor resource, and the Oracle Cloud load balance monitor resource was verified.

Distribution	EXPRESSCLUSTER Version	Remarks
Windows Server 2016	12.20 or later	

4.2.16 Operation environment for OCI forced stop resource

The use of the OCI forced stop resource requires the following software.

Software	Version	Remarks
OCI CLI	3.5.3 or later	

4.2.17 Operation environment for clpcfadm.py command

Using the clpcfadm.py command requires the following software:

Software	Version	Remarks
Python	3.6.8~	

4.3 System requirements for the Cluster WebUI

4.3.1 Supported operating systems and browsers

Browser	Language
Internet Explorer 11	English/Japanese/Chinese
Internet Explorer 10	English/Japanese/Chinese
Firefox	English/Japanese/Chinese
Google Chrome	English/Japanese/Chinese

Note: When using an IP address to connect to Cluster WebUI, the IP address must be registered to **Site** of **Local Intranet** in advance.

Note: When accessing Cluster WebUI with Internet Explorer 11, the Internet Explorer may stop with an error. In order to avoid it, please upgrade the Internet Explorer into KB4052978 or later. Additionally, in order to apply KB4052978 or later to Windows 8.1/Windows Server 2012R2, apply KB2919355 in advance. For details, see the information released by Microsoft.

Note: No mobile devices, such as tablets and smartphones, are supported.

4.3.2 Required memory size and disk size

- Required memory size: 500MB or more
- Required disk size: 200MB or more

CHAPTER

FIVE

LATEST VERSION INFORMATION

This chapter provides the latest information on EXPRESSCLUSTER. The latest information on the upgraded and improved functions is described in details.

This chapter covers:

5.1 Correspondence list of EXPRESSCLUSTER and a manual

Description in this manual assumes the following version of EXPRESSCLUSTER. Make sure to note and check how EXPRESSCLUSTER versions and the editions of the manuals are corresponding.

EXPRESSCLUSTER Internal Version	Manual	Edition	Remarks
13.02	Getting Started Guide	4th Edition	
	Installation and Configuration Guide	2nd Edition	
	Reference Guide	3rd Edition	
	Maintenance Guide	2nd Edition	

5.2 New features and improvements

The following features and improvements have been released.

No.	Internal Version	Contents
1	13.00	Windows Server 2022 is now supported.
2	13.00	Along with the major upgrade, some functions have been removed. For details, refer to the list of removed functions.
3	13.00	Added a function to suppress the automatic failover against a server crash, collectively in the whole cluster.
4	13.00	Added a function to give a notice in an alert log that the server restart count was reset as the final action against the detected activation error or deactivation error of a group resource or against the detected error of a monitor resource.
5	13.00	Added a function to exclude a server (with an error detected by a specified monitor resource) from the failover destination, for the automatic failover other than dynamic failover.
6	13.00	Added the clpfwctrl command for adding a firewall rule.
7	13.00	Added AWS secondary IP resources and AWS secondary IP monitor resources.
8	13.00	The forced stop function using BMC has been redesigned as a BMC forced-stop resource.
9	13.00	Redesigned the function for forcibly stopping virtual machines as a vCenter forced-stop resource.
10	13.00	The forced stop function in the AWS environment has been added to forced stop resources.
11	13.00	The forced stop function in the OCI environment has been added to forced stop resources.
12	13.00	Redesigned the forced stop script as a custom forced-stop resource.
13	13.00	Added a function to collectively change actions (followed by OS shutdowns such as a recovery action following an error detected by a monitor resource) into OS reboots.
14	13.00	Improved the alert message regarding the wait process for start/stop between groups.
15	13.00	The display option for the clpstat configuration information has allowed displaying the setting value of the resource start attribute.
16	13.00	The clpcl/clpstdn command has allowed specifying the -h option even when the cluster service on the local server is stopped.
17	13.00	A warning message is now displayed when Cluster WebUI is connected via a non-actual IP address and is switched to config mode.
18	13.00	In the config mode of Cluster WebUI, cluster configuration data can now be applied and exported even when information on the partition to be excluded cannot be obtained.
19	13.00	In the config mode of Cluster WebUI, a group can now be deleted with the group resource registered.
20	13.00	Changed the content of the error message that a communication timeout occurred in Cluster WebUI.
21	13.00	Changed the content of the error message that executing the full copy failed on the mirror disk screen in Cluster WebUI.

Continued on next page

Table 5.2 – continued from previous page

No.	Internal Version	Contents
22	13.00	Added a function to copy a group, group resource, or monitor resource registered in the config mode of Cluster WebUI.
23	13.00	Added a function to move a group resource registered in the config mode of Cluster WebUI, to another group.
24	13.00	The settings can now be changed at the group resource list of [Group Properties] in the config mode of Cluster WebUI.
25	13.00	The settings can now be changed at the monitor resource list of [Monitor Common Properties] in the config mode of Cluster WebUI.
26	13.00	The dependency during group resource deactivation is now displayed in the config mode of Cluster WebUI.
27	13.00	Added a function to display a dependency diagram at the time of group resource activation/deactivation in the config mode of Cluster WebUI.
28	13.00	Added a function to narrow down a range of display by type or resource name of a group resource or monitor resource on the status screen of Cluster WebUI.
29	13.00	The default value for [Errors in restoring file share setting are treated as activity failure] of CIFS resource has been changed from [On] to [Off].
30	13.00	An intermediate certificate can now be used as a certificate file when HTTPS is used for communication in the WebManager service.
31	13.00	Added the clpcfconv command, which changes the cluster configuration data file from the old version to the current one.
32	13.00	Added a function to delay the start of the cluster service for starting the OS.
33	13.00	Details such as measures can now be displayed for error results of checking cluster configuration data in Cluster WebUI.
34	13.00	The OS type can be specified for specifying the create option of the clpcfset command.
35	13.00	Added a function to delete a resource or parameter from cluster configuration data, which is enabled by adding the del option to the clpcfset command.
36	13.00	Added the clpcfadm.py command, which enhances the interface for the clpcfset command.
37	13.00	The start completion timing of an AWS DNS resource has been changed to the timing before which the following is confirmed: The record set was propagated to AWS Route 53.
38	13.00	Changed the default value for [Wait Time to Start Monitoring] of AWS DNS monitor resources to 300 seconds.
39	13.00	The clpstat command can now be run duplicately.
40	13.00	Added the Node Manager service.
41	13.00	Added a function for statistical information on heartbeat.
42	13.00	The proxy server has become available even when a Witness heartbeat resource is not used for an HTTP NP resolution resource.
43	13.00	HTTP monitor resources now support digest authentication.
44	13.00	The FTP server that uses FTPS for the FTP monitor resource can now be monitored.
45	13.00	Multiple system monitor resources can now be registered.
46	13.00	Multiple process resource monitor resources can now be registered.
47	13.00	Added a function to target only specific processes for a process resource monitor resource.
48	13.00	A single service monitor resource alone can now monitor any service.

Continued on next page

Table 5.2 – continued from previous page

No.	Internal Version	Contents
49	13.00	The options for the clpmdctrl and clpmdstat commands have been made the same as those for the clphdctrl and clphdstat commands.
50	13.02	JVM monitor resource supports Apache Tomcat 10.0.

5.3 Corrected information

Modification has been performed on the following minor versions.

Critical level:

L

Operation may stop. Data destruction or mirror inconsistency may occur.
Setup may not be executable.

M

Operation stop should be planned for recovery.
The system may stop if duplicated with another fault.

S

A matter of displaying messages.
Recovery can be made without stopping the system.

No.	Version in which the problem has been solved / Version in which the problem occurred	Phenomenon	Level	Occurrence condition/ Occurrence frequency
1	13.00 / 9.00 to 12.32	In a group, when a group resource alone is successfully activated, the restoration of another group resource may be executed.	S	This problem occurs in a group where a group resource alone is activated with another group resource failing in activation.
2	13.00 / 12.10 to 12.32	In the config mode of Cluster WebUI, modifying a comment on a group resource may not be applied.	S	This problem occurs in the following case: A comment on a group resource is modified, the [Apply] button is clicked, the change is undone, and then the [OK] button is clicked.
3	13.00 / 12.10 to 12.32	In the config mode of Cluster WebUI, modifying a comment on a monitor resource may not be applied.	S	This problem occurs in the following case: A comment on a monitor resource is modified, the [Apply] button is clicked, the change is undone, and then the [OK] button is clicked.
4	13.00 / 12.10 to 12.32	When Cluster WebUI is connected to a stopped server, the [Recover] button remains disabled for a server restarting after its crash.	S	This problem occurs in the following case: When Cluster WebUI is connected to a stopped server, there is a server restarting after its crash.

Continued on next page

Table 5.3 – continued from previous page

No.	Version in which the problem has been solved / Version in which the problem occurred	Phenomenon	Level	Occurrence condition/ Occurrence frequency
5	13.00 / 12.10 to 12.32	In the config mode of Cluster WebUI, the [Install Path] item is not required to be entered in the [Monitor (special)] tab of a WebLogic monitor resource.	S	This problem always occurs.
6	13.00 / 12.00 to 12.32	In the status screen of Cluster WebUI, a communication timeout during the operation of a cluster causes a request to be repeatedly issued.	M	This problem always occurs when a communication timeout occurs between Cluster WebUI and a cluster server.
7	13.00 / 12.10 to 12.32	Custer WebUI may freeze when dependency is set in the config mode of Cluster WebUI.	S	This problem occurs when two group resources are made dependent on each other.
8	13.00 / 12.20 to 12.32	The response of the clpstat command may be delayed.	S	This problem may occur when communication with other servers is cut off.
9	13.00 / 11.10 to 12.32	In the alert log for a delay warning of a monitor resource, the response time may read zero (0).	S	This problem may occur when the alert log for a delay warning of a monitor resource is outputted.
10	13.00 / 12.20 to 12.32	An AP error of clpwebmc may occur.	S	This problem rarely occurs when cluster configuration data with a server removed is applied in the config mode of Cluster WebUI.
11	13.00 / 12.00 to 12.32	A monitor resource may mistakenly detect a monitoring timeout.	M	This problem very rarely occurs when a monitoring process is executed by a monitor resource.
12	13.00 / 12.20 to 12.32	An error occurs when the status code of a target response is 301 in an HTTP NP resolution resource.	S	This problem occurs when the response status code is 301.
13	13.00 / 12.00 to 12.32	In [Monitoring usage of memory] for process resource monitor resources, [Duration time (min)] has been replaced with [Maximum Refresh Count (time)].	S	This problem occurs when the properties are displayed with Cluster WebUI or the clpstat command.

Continued on next page

Table 5.3 – continued from previous page

No.	Version in which the problem has been solved / Version in which the problem occurred	Phenomenon	Level	Occurrence condition/ Occurrence frequency
14	13.00 / 12.00 to 12.32	In an HTTP monitor resource, a warning instead of an error is issued in the following case: The status code of a response to an issued HEAD request is in the 400s or 500s, and a non-default URI is specified as the monitor URI.	S	This problem occurs in the following case: The status code of a response to an issued HEAD request is in the 400s or 500s, and a non-default URI is specified as the monitor URI.
15	13.00 / 12.10 to 12.32	In a custom monitor resource, when the process of a script to be monitored is cleared, the corresponding monitor resource name is not outputted to the alert message.	S	This problem occurs when the process of a script to be monitored is cleared in a custom monitor resource.
16	13.00 / 11.01 to 12.32	A response to a mirror-related command may take time.	S	This problem occurs when a mirror disk connection is disconnected or when some of servers constituting a cluster are down.
17	13.00 / 12.20 to 12.32	The EXPRESSCLUSTER Information Base service may abend.	S	This problem very rarely occurs when one of the following is performed: - Cluster startup - Cluster stop - Cluster suspension - Cluster resumption
18	13.01 / 9.00 to 12.32,13.00	The vulnerabilities of CVE-2021-20700 to 20707 may cause the following acts by third parties: - Execution of an arbitrary code - Upload of an arbitrary file - Reading of an arbitrary file	L	These problems occur when a specific process in EXPRESSCLUSTER receives a packet crafted by a malicious third party against the internal protocol of EXPRESSCLUSTER.
19	13.01 / 13.00	For the clprexec command, the --script option does not work.	S	This problem occurs when the clprexec command is executed with the --script option specified.

Continued on next page

Table 5.3 – continued from previous page

No.	Version in which the problem has been solved / Version in which the problem occurred	Phenomenon	Level	Occurrence condition/ Occurrence frequency
20	13.01 / 13.00	After a forced-stop resource is added by executing the clpcfset command, the cluster fails to start up.	S	This problem occurs during an attempt to start up a cluster to which cluster configuration data (including a forced-stop resource added by executing the clpcfset command) was applied.
21	13.02 / 13.00 to 13.01	The EXPRESSCLUSTER Node Manager service starts without waiting for a service startup delay time.	S	This problem occurs with [Service Startup Delay Time] set to a value larger than zero seconds.
22	13.02 / 13.01	Update installation registers the EXPRESSCLUSTER Old API Support service.	S	This problem occurs with the internal version 13.00 updated to 13.01.
23	13.02 / 13.00 to 13.01	After a server is removed from the [Servers that can run the Group] list of the failover group, trying to apply the configuration data does not lead to a group-stop request.	S	This problem occurs in the following case: After a server is removed from the [Servers that can run the Group] list of the failover group, applying the configuration data is tried.
24	13.02 / 13.00 to 13.01	The STOP error may occur during the application of cluster configuration data including a mirror/hybrid disk resource.	M	This problem occurs with the mirror/hybrid disk resource named with eight or more characters.
25	13.02 / 13.00 to 13.01	A monitor resource may detect a monitoring timeout by mistake.	S	This problem occurs on very rare occasions during a monitoring process by the monitor resource.
26	13.02 / 13.00 to 13.01	When [Recovery Action tab] for a monitor resource is set with [Generate an intentional stop error], the recovery action may not be performed.	S	This problem occurs on rare occasions when the recovery action is tried.
27	13.02 / 13.00 to 13.01	An initialization error may occur in a kernel mode LAN heartbeat resource during a cluster service start.	M	This problem occurs when the kernel mode LAN heartbeat resource starts up with the network device yet to become available.
28	13.02 / 12.00 to 13.01	A cluster service stop as an action at NP occurrence is not completed.	M	This problem occurs with [Action at NP Occurrence] set to [Stop the cluster service].

Continued on next page

Table 5.3 – continued from previous page

No.	Version in which the problem has been solved / Version in which the problem occurred	Phenomenon	Level	Occurrence condition/ Occurrence frequency
29	13.02 / 13.00 to 13.01	Forcibly stopping more than one server may fail.	S	This problem occurs on rare occasions when one of three or more servers in a cluster tries to forcibly stop other servers.
30	13.02 / 9.00 to 13.01	An application error may occur with the clpstat command.	S	This problem occurs in an environment where a failover group is set with no group resources registered.
31	13.02 / 13.00 to 13.01	With a cluster suspended, Cluster WebUI or the clpstat command may show the server status as stopped.	S	This problem occurs when both of the following services are restarted with the cluster suspended: - EXPRESSCLUSTER Node Manager - EXPRESSCLUSTER Information Base
32	13.02 / 13.00 to 13.01	A group/monitor resource status may be incorrectly shown.	S	This problem occurs with something wrong in the internal processing of cluster services during OS startup.
33	13.02 / 13.00 to 13.01	Cluster WebUI or the clpstat command incorrectly shows the status of a server using no forced-stop resources.	S	This problem occurs when any of three or more servers in a cluster is configured not to use the forced-stop function.
34	13.02 / 9.00 to 13.01	A STOP error may occur during OS startup or OS shutdown.	M	This problem occurs on very rare occasions during OS startup or OS shutdown.
35	13.02 / 9.00 to 13.01	The vulnerabilities of CVE-2022-34822 to 34823 may cause the following acts by third parties: - Reading of an arbitrary file - Execution of an arbitrary code	L	These problems occur when a specific process in EXPRESSCLUSTER receives a packet crafted by a malicious third party against the internal protocol of EXPRESSCLUSTER.

CHAPTER

SIX

NOTES AND RESTRICTIONS

This chapter provides information on known problems and how to troubleshoot the problems.

This chapter covers:

6.1 Designing a system configuration

Hardware selection, system configuration, and shared disk configuration are introduced in this section.

6.1.1 Hardware requirements for mirror disk and hybrid disk

- Dynamic disks cannot be used. Use basic disks.
- The partitions (data and cluster partitions) for mirror disks and hybrid disks cannot be used by mounting them on an NTFS folder.
- To use a mirror disk resource or a hybrid disk resource, partitions for mirroring (i.e. data partition and cluster partition) are required.
- There are no specific limitations on locating partitions for mirroring, but the data partition sizes need to be perfectly matched with one another on a byte basis. A cluster partition also requires space of 1024MiB or larger.
- When making data partitions as logical partitions on the extended partition, make sure to select the logical partition for both servers. Even when the same size is specified on both primary partition and logical partition, their actual sizes may different from each other.
- It is recommended to create a cluster partition and a data partition on different disks for the load distribution. (There are not any problems to create them on the same disk, but the writing performance will slightly decline, in case of asynchronous mirroring or in a state that mirroring is suspended.)
- Use the same type of disks for reserving data partitions that perform mirroring by mirror resources on both of the servers.

  Example

Combination	server1	server2
OK	SCSI	SCSI
OK	IDE	IDE
NG	IDE	SCSI

- Partition size reserved by **Disk Management** is aligned by the number of blocks (units) per disk cylinder. For this reason, if disk geometries used as disks for mirroring differ between servers, the data partition sizes cannot be matched perfectly. To avoid this problem, it is recommended to use the same hardware configurations including RAID configurations for the disks that reserve data partitions on server1 and server2.
- When you cannot synchronize the disk type or geometry on the both servers, make sure to check the exact size of data partitions by using the clpvolsz command before configuring a mirror disk resource or a hybrid disk resource. If they do not match, make the larger partition small by using the clpvolsz command.
- When RAID-disk is mirrored, it is recommended to use writeback mode because writing performance decreases a lot when the disk array controller cache is set to write-thru mode. However, when writeback mode is used, it is necessary to use disk array controller with battery installed or use with UPS.
- A partition with the OS page file cannot be mirrored.

6.1.2 IPv6 environment

The following function cannot be used in an IPv6 environment:

- AWS Elastic IP resource
- AWS Virtual IP resource
- AWS Secondary IP resource
- AWS DNS resource
- Azure probe port resource
- Azure DNS resource
- Google Cloud virtual IP resource
- Google Cloud DNS resource
- Oracle Cloud virtual IP resource
- AWS Elastic IP monitor
- AWS Virtual IP monitor
- AWS Secondary IP monitor
- AWS AZ monitor
- AWS DNS monitor
- Azure probe port monitor
- Azure load balance monitor
- Azure DNS monitor
- Google Cloud virtual IP monitor resource
- Google Cloud load balance monitor resource
- Google Cloud DNS monitor resource
- Oracle Cloud virtual IP monitor resource
- Oracle Cloud load balance monitor resource

The following functions cannot use link-local addresses:

- Kernel mode LAN heartbeat resource
- Mirror disk connect
- PING network partition resolution resource
- FIP resource
- VIP resource

6.1.3 Network configuration

The cluster configuration cannot be configured or operated in an environment, such as NAT, where an IP address of a local server is different from that of a remote server.

The following figure shows two servers connected to different networks with a NAT device set between them.
For example, assume that the NAT device is set as "the packet from the external network to 10.0.0.2 is forwarded to the internal network."
However, to build a cluster with Server 1 and Server 2 in this environment, IP addresses for different networks must be set in each server.
In the environment with each server set in different subnets like this, a cluster cannot be properly configured or operated.

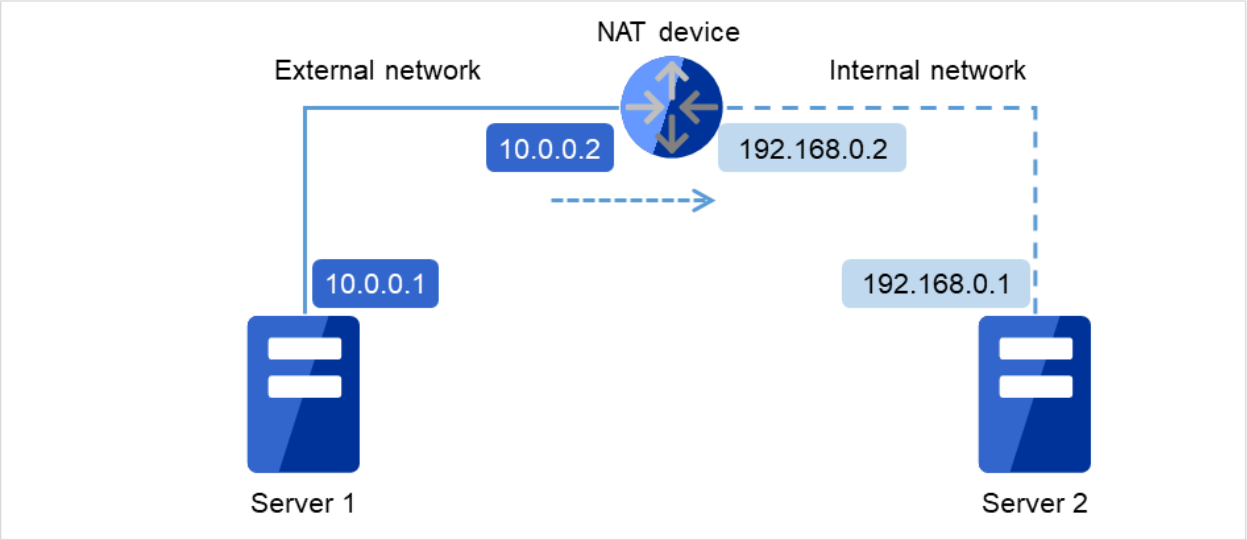


Fig. 6.1: Example of the environment where a cluster cannot be configured

- Cluster settings for Server 1
  - Local server: 10.0.0.1
  - Remote server: 10.0.0.2
- Cluster settings for Server 2
  - Local server: 192.168.0.1
  - Remote server: 10.0.0.1

6.1.4 Hardware requirements for shared disks

- Dynamic disks cannot be used. Use basic disks.
- The partitions (disk heartbeat and disk resource switchable partitions) for shared disks cannot be used by mounting them on an NTFS folder.
- Software RAID (stripe set, mirror set, stripe set with parity) and volume set cannot be used.

6.1.5 Write function of the mirror disk and hybrid disk

There are 2 types of disk mirroring of mirror disk resources and hybrid disk resources: synchronous mirroring and asynchronous mirroring.

In synchronous mirroring, data is written in the disks of both servers for every request to write data in the data partition to be mirrored and its completion is waited. Data is written in each of the servers along with this, but it is written in disks of other servers via network, so writing performance declines more significantly compared to a normal local disk that is not to be mirrored. In case of the remote cluster configuration, since the network communication speed is slow and delay is long, the writing performance declines drastically.

In asynchronous mirroring, data is written to the local server immediately. However, when writing data to other server, it is saved to the local queue first and then written in the background. Since the completion of writing data to other server is not waited for, even when the network performance is low, the writing performance will not decline significantly. However, in case of asynchronous mirror, the data to be updated is saved in the queue for every writing request as well, so the writing performance declines more significantly, compared to the normal local disk that is not to be mirrored and the shared disk. For this reason, it is recommended to use the shared disk for the system (such as the database system with lots of update systems) that is required high throughput for writing data in disks.

In case of asynchronous mirroring, the writing sequence will be guaranteed, but the data that has been updated to the latest may be lost, if an active server shuts down. For this reason, if it is required to inherit the data immediately before an error occurs for sure, use synchronous mirroring or the shared disk.

6.1.6 History file of asynchronous mirroring

In mirror disk or hybrid disk with asynchronous mode, data that cannot afford to be written in memory queue is recorded temporarily in a folder specified to save history files. When the limit of the file is not specified, history files are written in the specified folder without limitation. In this case, the line speed is too low, compared to the disk update amount of application, writing data to other server cannot catch up with updating the disk, and history files will overflow from the disk.

For this reason, it is required to reserve a communication line with enough speed in the remote cluster configuration as well, in accordance with the amount of disk application to be updated.

In case the folder with history files overflows from the disk because the communication band gets narrowed or the disk is updated continuously, it is required to reserve enough empty space in the drive and specify the limit of the history file size. This space will be specified as the destination to write history files, and to specify the drive different from the system drive as much as possible.

6.1.7 Data consistency among multiple asynchronous mirror disks

In mirror disk or hybrid disk with asynchronous mode, writing data to the data partition of the active server is performed in the same order as the data partition of the standby server.

This writing order is guaranteed except during the initial mirror disk configuration or recovery (copy) period after suspending mirroring the disks. The data consistency among the files on the standby data partition is guaranteed.

However, the writing order is not guaranteed among multiple mirror disk resources and hybrid disk resources. For example, if a file gets older than the other and files that cannot maintain the data consistency are distributed to multiple asynchronous mirror disks, an application may not run properly when it fails over due to server failure.

For this reason, be sure to place these files on the same asynchronous mirror disk or hybrid disk.

6.1.8 Multi boot

Avoid using multi boot if either of mirror disk or shared disk is used because if an operating system is started from another boot disk, access restrictions on mirroring and the shared disk become ineffective. The mirror disk consistency will not be guaranteed and data on the shared disk will not be protected.

6.1.9 JVM monitor resources

- Up to 25 Java VMs can be monitored concurrently. The Java VMs that can be monitored concurrently are those which are uniquely identified by the Cluster WebUI (with **Identifier** in the **Monitor(special)** tab)
- Connections between Java VMs and JVM monitor resources do not support SSL.
- It may not be possible to detect thread deadlocks. This is a known problem in Java VM. For details, refer to "Bug ID: 6380127" in the Oracle Bug Database
- The JVM monitor resources can monitor only the Java VMs on the server on which the JVM monitor resources are running.
- The Java installation path setting made by the Cluster WebUI (with **Java Installation Path** in the **JVM monitor** tab in **Cluster Property**) is shared by the servers in the cluster. The version and update of Java VM used for JVM monitoring must be the same on every server in the cluster.
- The management port number setting made by the Cluster WebUI (with **Management Port** in the **Connection Setting** dialog box opened from the **JVM monitor** tab in **Cluster Property**) is shared by all the servers in the cluster.
- Application monitoring is disabled when an application to be monitored on the IA32 version is running on an x86_64 version OS.
- If a large value such as 3,000 or more is specified as the maximum Java heap size by the Cluster WebUI (by using Maximum Java Heap Size on the **JVM monitor** tab in **Cluster Property**), The JVM monitor resources will fail to start up. The maximum heap size differs depending on the environment, so be sure to specify a value based on the capacity of the mounted system memory.
- If "-XX:+UseG1GC" is added as a startup option of the target Java VM, the settings on the **Memory** tab on the **Monitor(special)** tab in **Property** of JVM monitor resources cannot be monitored before Java 7.

  It's possible to monitor by choosing **Oracle Java (usage monitoring)** in **JVM Type** on the **Monitor(special)** tab after Java 8.

6.1.10 Requirements for network warning light

- When using "DN-1000S" or "DN-1500GL," do not set your password for the warning light.
- To play an audio file as a warning, you must register the audio file to a network warning light supporting audio file playback.

  For details about how to register an audio file, see the manual of the network warning light you want to use.
- Set up a network warning light so that a server in a cluster is permitted to execute the rsh command to that warning light.

6.2 Before installing EXPRESSCLUSTER

Consideration after installing an operating system, when configuring OS and disks are described in this section.

6.2.1 File system

Use NTFS for file systems of a partition to install OS, a partition to be used as a disk resource of the shared disk, and of a data partition of a mirror disk resource and a hybrid disk resource.

6.2.2 Communication port number

In EXPRESSCLUSTER, the following port numbers are used by default. You can change the port number by using the Cluster WebUI.

Make sure not to access the following port numbers from a program other than EXPRESSCLUSTER.

Configure to be able to access the port number below when setting a firewall on a server:

After installing EXPRESSCLUSTER, you can use the clpfwctrl command to configure a firewall. For more information, see "Reference Guide" -> "EXPRESSCLUSTER command reference" -> "Adding a firewall rule (clpfwctrl command)". Ports to be set with the clpfwctrl command are marked with ✓ in the clpfwctrl column of the table below. The applicable protocols are ICMPv4 and ICMPv6.

For a cloud environment, allow access to ports numbered as below, not only in a firewall configuration at the instance side but also in a security configuration at the cloud infrastructure side.

- **Server to Server**

From		To		Used for	clpfwctrl
Server	Automatic allocation[5]	Server	29001/TCP	Internal communication	✓
Server	Automatic allocation	Server	29002/TCP	Data transfer	✓
Server	Automatic allocation	Server	29003/UDP	Alert synchronization	✓
Server	Automatic allocation	Server	29004/TCP	Communication between disk agents	✓
Server	Automatic allocation	Server	29005/TCP	Communication between mirror drivers	✓
Server	Automatic allocation	Server	29008/TCP	Cluster information management	✓
Server	Automatic allocation	Server	29010/TCP	Internal communication of RESTful API	✓
Server	29106/UDP	Server	29106/UDP	Heartbeat	✓
Server	icmp	Server	icmp	Duplication check for FIP/VIP resource	

- **Client to Server**

From		To		Used for	clpfwctrl
RESTful API client	Automatic allocation	Server	29009/TCP	http communication	✓

- **Cluster WebUI to Server**

From		To		Used for	clpfwctrl
Cluster WebUI,	Automatic allocation	Server	29003/TCP	http communication	✓

- **Others**

From		To		Used for	clpfwctrl
Server	Automatic allocation	Network warning light	See the manual for each product.	Network warning light control	
Server	Automatic allocation	BMC Management LAN of the server	623/UDP	BMC control (Forced stop)	
Server	Automatic allocation	Witness server	Communication port number specified with Cluster WebUI	Connection destination host of the Witness heartbeat resource	
Server	Automatic allocation	Monitor target	icmp	IP monitor resource	
Server	Automatic allocation	Monitor target	icmp	Monitoring target of PING method of network partition resolution resource	
Server	Automatic allocation	Monitor target	Management port number set by the Cluster WebUI	Monitoring target of HTTP method of network partition resolution resource	
Server	Automatic allocation	Server	Management port number set by the Cluster WebUI	JVM monitor resource	✓
Server	Automatic allocation	Monitoring target	Connection port number set by the Cluster WebUI	JVM monitor resource	

Continued on next page

[5] In automatic allocation, a port number not being used at a given time is allocated.

Table 6.4 – continued from previous page

From		To		Used for	clpfwctrl
Server	Automatic allocation	Server	Probe port set by the Cluster WebUI	Azure probe port resource	✓
Server	Automatic allocation	AWS region endpoint	443/tcp	AWS Elastic IP resource AWS virtual IP resource AWS secondary IP resource AWS DNS resource AWS Elastic IP monitor resource AWS virtual IP monitor resource AWS secondary IP monitor resource AWS AZ monitor resource AWS DNS monitor resource AWS forced stop resource	
Server	Automatic allocation	Azure endpoint	443/tcp	Azure DNS resource	
Server	Automatic allocation	Azure authoritative name server	53/udp	Azure DNS monitor resource	
Server	Automatic allocation	Server	Port number set in Cluster WebUI	Google Cloud virtual IP resource	✓
Server	Automatic allocation	Server	Port number set in Cluster WebUI	Oracle Cloud virtual IP resource	✓

For an AWS environment, modify the Security Group setting in addition to the firewall setting.

JVM monitor uses the following two port numbers:

- This management port number is a port number that the JVM monitor resource uses internally. To set the port number, open the Cluster Properties window of the Cluster WebUI, select the JVM monitor tab, and then open the Connection Setting dialog box. For more information, refer to " Parameter details" in the "Reference Guide".

- This connection port number is the port number used to connect to the Java VM on the monitoring target (WebLogic Server or WebOTX). To set the port number, open the Properties window for the relevant JVM monitoring resource name, and then select the Monitor(special) tab. For more information, refer to "Monitor resource details" in the "Reference Guide".

The following are port numbers used by the load balancer for the alive monitoring of each server: **Probeport** of an Azure probe port resource, **Port Number** of a Google Cloud virtual IP resource, and **Port Number** of an Oracle Cloud virtual IP resource.

The above port numbers are used with the AWS CLI, which is executed by the following AWS-related resources:

- AWS Elastic IP resource
- AWS Virtual IP resource
- AWS Secondary IP resource
- AWS DNS resource
- AWS Elastic IP monitor resource
- AWS Virtual IP monitor resource
- AWS Secondary IP monitor resource
- AWS AZ monitor resource
- AWS DNS monitor resource
- AWS Forced stop resource

The Azure DNS resource runs the Azure CLI. The above port numbers are used by the Azure CLI.

6.2.3 Changing automatic allocation range of communication port numbers managed by the OS

The automatic allocation range of communication port numbers managed by the OS may overlap the communication port numbers used by EXPRESSCLUSTER.

Check the automatic allocation range of communication port numbers managed by the OS, by using the following method. If there is any overlap, change the port numbers used by EXPRESSCLUSTER or change the automatic allocation range of communication port numbers managed by the OS, by using the following method to prevent any overlap.

- Display and set the automatic allocation range by using the Windows netsh command.
- Checking the automatic allocation range of communication port numbers managed by the OS

```
netsh interface <ipv4|ipv6> show dynamicportrange <tcp|udp>
```

An example is shown below.

```
>netsh interface ipv4 show dynamicportrange tcp

Range of dynamic ports of the tcp protocol
----------------------------------------
Start port : 49152
Number of ports : 16384
```

This example indicates that the range in which communication port numbers are automatically allocated in the TCP protocol is 49152 to 68835 (allocation of 16384 ports beginning with port number 49152). If any of the port numbers used by EXPRESSCLUSTER fall within this range, change the port numbers used by

EXPRESSCLUSTER or follow description given in "Setting the automatic allocation range of communication port numbers managed by the OS," below.

- Setting the automatic allocation range of communication port numbers managed by the OS

```
netsh interface <ipv4|ipv6> set dynamicportrange <tcp|udp> [startport=]
↪<start_port_number> [numberofports=]<range_of_automatic_allocation>
```

An example is shown below.

```
>netsh interface ipv4 set dynamicportrange tcp startport=10000 numberofports=1000
```

This example sets the range in which communication port numbers are automatically allocated in the TCP protocol (ipv4) to between 10000 and 10999 (allocation of 1000 ports beginning with port number 10000).

6.2.4 Avoiding insufficient ports

If a lot of servers and resources are used for EXPRESSCLUSTER, the number of temporary ports used for internal communications by EXPRESSCLUSTER may be insufficient and the servers may not work properly as the cluster server.
Adjust the range of port number and the time before a temporary port is released as needed.

6.2.5 Clock synchronization

In a cluster system, it is recommended to synchronize multiple server clocks regularly. Synchronize server clocks by using the time server.

6.2.6 Partition for shared disk

- If multiple servers that are connected to the shared disk are started while access is not restricted by EXPRESSCLUSTER, data on the shared disk may be corrupted. When the access is restricted, make sure to start only one of the servers.
- When a disk method is used to solve network partition, create a raw partition (disk heartbeat partition) with space larger than 17 MB that disk network partition resolution resources use on the shared disk.
- Format the partition (switchable partition) used to transfer data between servers as disk resources with NTFS.
- For each partition on the shared disk, assign the same drive letter on all servers.
- Partitions on the shared disk can be formatted and created from one of the servers. It is not necessary to recreate or reformat a partition on each server. However, the drive letter needs to be set in each server.
- When you continue using the data on the shared disk at times such as server reinstallation, do not create or format a partition. The data on the shared disk gets deleted if you allocate or format a partition.

6.2.7 Partition for mirror disk

- Create a raw partition with larger than 1024MiB space on local disk of each server as a management partition for mirror disk resource (cluster partition.)
- Create a partition (data partition) for mirroring on local disk of each server and format it with NTFS. It is not necessary to recreate a partition when the existing partition is mirrored.
- Set the same data partition size to both servers. Use the clpvolsz command for checking and adjusting the partition size accurately.
- Set the same drive letter to both servers for a cluster partition and data partition.

6.2.8 Partition for hybrid disk

- As a partition for hybrid disk resource management (cluster partition), create a RAW partition of 1024MiB or larger in the shared disk of each server group (or in the local disk if there is one member server in the server group).
- Create a partition to be mirrored (data partition) in the shared disk of each server group (or in the local disk if there is one member server in the server group) and format the partition with NTFS (it is not necessary to create a partition again when an existing partition is mirrored).
- Set the same data partition size to both server groups. Use the clpvolsz command for checking and adjusting the partition size accurately.
- Set the same drive letter to cluster partitions in all servers. Set the same drive letter to data partitions in all servers..

6.2.9 Access permissions of a folder or a file on the data partition

In the workgroup environment, you must set access permission of a folder or a file on the data partition for an user on each cluster server. For example, you must set access permission for "test" user of "server1" and "server2" which are cluster servers.

6.2.10 Adjusting OS startup time

It is necessary to configure the time from power-on of each node in the cluster to the server operating system startup to be longer than the following[6]:

- The time from power-on of the shared disks to the point they become available.
- Heartbeat timeout time.

[6] 3 Refer to "3. Adjustment of the operating system startup time (Required)" in "Settings after configuring hardware" in "Determining a hardware configuration" in "Determining a system configuration" in the "Installation and Configuration Guide".

6.2.11 Verifying the network settings

- On all servers in the cluster, verify the status of the following networks using the ipconfig or ping command.
- Check the network settings by using the ipconfig and ping commands.
  - Public LAN (used for communication with all the other machines)
  - Interconnect-dedicated LAN (used for communication between servers in EXPRESSCLUSTER)
  - Mirror connect LAN (used with interconnect)
  - Host name
- The IP address does not need to be set as floating IP resource in the operating system.
- When NIC is link down, IP address will be disabled in a server that if IPv6 is specified for the EXPRESSCLUSTER configuration (such as heartbeat and mirror connect).

  In that case, EXPRESSCLUSTER may cause some problems. Type following command to disable media sense function to avoid this problem.

```
netsh interface ipv6 set global dhcpmediasense=disabled
```

6.2.12 Coordination with ESMPRO/AutomaticRunningController

The following are the notes on EXPRESSCLUSTER configuration when EXPRESSCLUSTER works together with ESMPRO/AutomaticRunningController (hereafter ESMPRO/AC). If these notes are unmet, EXPRESSCLUSTER may fail to work together with ESMPRO/AC.

The function to use EXPRESSCLUSTER with ESMPRO/AC does not work on the OS of x64 Edition.

- You cannot specify only the DISK-method resource as a network partition resolution resource. When you specify the DISK method, do so while combining with other network partition resolution method such as PING method.
- When creating a disk TUR monitor resource, do not change the default value (No Operation) for the final action.
- When creating a Disk RW monitor resource, if you specify a path on the shared disk for the value to be set for file name, do not change the default value (active) for the monitor timings.
- After recovery from power outage, the following alerts may appear on the EXPRESSCLUSTER manager. This does not affect the actual operation due to the configuring the settings mentioned above.
  - ID:18
    Module name: nm
    Message: Failed to start the resource <resource name of DiskNP>. (server name:xx)
  - ID:1509
    Module name: rm
    Message: Monitor <disk TUR monitor resource name> detected an error. (4 : device open failed. Check the disk status of the volume of monitoring target.)
- For information on how to configure ESMPRO/AC and notes etc, see the chapter for ESMPRO/AC in the *EXPRESSCLUSTER X for Windows PP Guide*.

6.2.13 About ipmiutil

- The following functions use IPMI Management Utilities (ipmiutil), an open source of the BSD license, to control the BMC firmware servers. To use these functions, it is necessary to install ipmiutil in each server:
  - Forcibly stopping a physical machine
- When you use any of the above functions, configure Baseboard Management Controller (BMC) in each server so that the IP address of the management LAN port for the BMC can communicate with the IP address which the OS uses. These functions cannot be used on a server where there is no BMC installed, or when the network for the BMC management is obstructed. For information on how to configure the settings for the BMC, see the manuals for servers.
- EXPRESSCLUSTER does not come with ipmiutil. For information on how to acquire and install ipmiutil, see "Setup of BMC and ipmiutil (Required for using the forced stop function of a physical machine)" in "Settings after configuring hardware" in "Determining a system configuration" in the "Installation and Configuration Guide".
- Users are responsible for making decisions and assuming responsibilities. NEC does not support or assume any responsibilities for:
  - Inquires about ipmiutil itself
  - Operations of ipmiutil
  - Malfunction of ipmiutil or any error caused by such malfunction
  - Inquiries about whether or not ipmiutil is supported by a given server
- Check if your server (hardware) supports ipmiutil in advance. Note that even if the machine complies with the IPMI standard as hardware, ipmiutil may not run when you actually try to run it.

6.2.14 Installation on Server Core

When installing EXPRESSCLUSTER on Server Core environment in Windows Server 2008, execute menu.exe just under the root of CD media at a command prompt. This displays the menu screen.

Although the procedures hereafter are the same as those in normal installation, you cannot select **Register with License File** in license registration. Make sure to select **Register with License Information**.

6.2.15 Mail reporting

The mail reporting function is not supported by STARTTLS and SSL.

6.2.16 Access restriction for an HBA to which a system disk is connected

When an HBA to which a system disk is connected is listed in **HBAs to be managed by the cluster system**, access to the system partition in which the OS is installed is restricted and the OS may not start.

When an HBA to which a system disk is connected is added to **HBAs to be managed by the cluster system** in such an environment that enables SAN boot, the system partition should be added to **Partition excluded from cluster management** so that the access to it will not be restricted.

For details, see "Server Properties" in "Parameter details" in the "Reference Guide".

6.2.17 Time synchronization in the AWS environtment

The following AWS-related resources execute the AWS CLI during activation, deactivation, or monitoring:

- AWS Elastic IP resource
- AWS Virtual IP resource
- AWS Secondary IP resource
- AWS DNS resource
- AWS Elastic IP monitor resource
- AWS Virtual IP monitor resource
- AWS Secondary IP monitor resource
- AWS AZ monitor resource
- AWS DNS monitor resource
- AWS Forced stop resource

If the date and time of an instance is not correctly set, executing the AWS CLI may fail due to the specification of AWS.
In such a case, correct the date and time of the instance by using a server such as an NTP server. For details, refer to "Setting the Time for a Windows Instance" (
http://docs.aws.amazon.com/en_us/AWSEC2/latest/WindowsGuide/windows-set-time.html)

6.2.18 IAM settings in the AWS environtment

This section describes the settings of IAM (Identity & Access Management) in AWS environment.

Some of EXPRESSCLUSTER's functions internally run AWS CLI for their processes. To run AWS CLI successfully, you need to set up IAM in advance.

You can give access permissions to AWS CLI by using IAM role or IAM user. IAM role method offers a high-level of security because you do not have to store AWS access key ID and AWS secret access key in an instance. Therefore, it is recommended to use IAM role basically.

Advantages and disadvantages of the two methods are as follows:

	Advantages	Disadvantages
IAM role	- This method is more secure than using IAM user - The procedure for for maintaining key information is simple.	None
IAM user	You can set access permissions for each instance later.	The risk of key information leakage is high. The procedure for maintaining key information is complicated.

The procedure of setting IAM is shown below.

1. First, create IAM policy by referring to "Creating IAM policy" explained below.
2. Next, configure the instance settings.
   To use IAM role, refer to "Setting up an instance by using IAM role" described later.

To use IAM user, refer to "Setting up an instance by using IAM user" described later.

Creating IAM policy

Create a policy that describes access permissions for the actions to the services such as EC2 and S3 of AWS. The actions required for AWS-related resources and monitor resources to execute AWS CLI are as follows:

The necessary policies are subject to change.

- AWS virtual IP resources / AWS virtual IP monitor resources

Action	Description
ec2:DescribeNetworkInterfaces ec2:DescribeVpcs ec2:DescribeRouteTables	This is required for obtaining information of VPC, route table and network interfaces.
ec2:ReplaceRoute	This is required for updating the route table.

- AWS Elastic IP resources /AWS Elastic IP monitor resource

Action	Description
ec2:DescribeNetworkInterfaces ec2:DescribeAddresses	This is required for obtaining information of EIP and network interfaces.
ec2:AssociateAddress	This is required for associating EIP with ENI.
ec2:DisassociateAddress	This is required for disassociating EIP from ENI.

- AWS secondary IP resources / AWS secondary IP monitor resources

Action	Description
ec2:DescribeNetworkInterfaces ec2:DescribeSubnets	This is required for obtaining information on network interfaces and subnets.
ec2:AssignPrivateIpAddresses	This is required for assigning secondary IP addresses.
ec2:UnassignPrivateIpAddresses	This is required for deassigning secondary IP addresses.

- AWS AZ monitor resource

Action	Description
ec2:DescribeAvailabilityZones	This is required for obtaining information of the availability zone.

- AWS DNS resource / AWS DNS monitor resource

Action	Description
route53:ChangeResourceRecordSets	This is required for a resource record set is added or deleted or when the resource record set configuration is updated.
route53:GetChange	This is required for a resource record set is added or when the resource record set configuration is updated.
route53:ListResourceRecordSets	This is required for obtaining information of a resource record set.

- AWS forced stop resource

Action	Description
ec2:DescribeInstances	This is required for obtaining information on instances.
ec2:StopInstances	This is required for stopping instances.
ec2:RebootInstances	This is required for restarting instances.

- Function for sending data on the monitoring process time taken by the monitor resource, to Amazon CloudWatch.

Action	Description
cloudwatch:PutMetricData	This is required for sending custom metrics.

- Function for sending alert service messages to Amazon SNS

Action	Description
sns:Publish	This is required for sending messages.

The example of a custom policy as shown below permits actions used by all the AWS-related resources and monitor resources.

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

(continues on next page)

(continued from previous page)

```
}
```

You can create a custom policy from [Policies] - [Create Policy] in IAM Management Console

Setting up an instance by using IAM role

In this method, you can execute execute AWS CLI after creating IAM role and associate it with an instance.

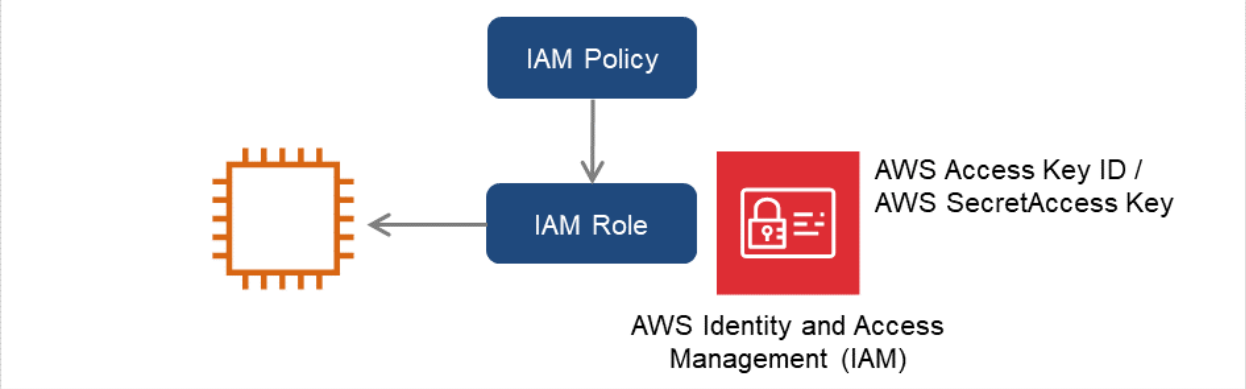


Fig. 6.2: Setting an instance by using IAM role

1) Create the IAM role and attach the IAM Policy to the role.
   You can create the IAM role from [Roles] - [Create New Role] in IAM Management Console
2) When creating an instance, specify the IAM role you created to **IAM Role**.
3) Log on to the instance.
4) Install Python.
   Install Python required by EXPRESSCLUSTER. First, confirm that Python has been installed on the machine. If not, download Python from the following URL and install it. After installation, add the file path of python.exe to the PATH environment variable from the Control Panel. Since the Python command is executed as the SYSTEM user, please make sure that the path to the Python command is set in the system environment variable PATH.

   https://www.python.org/downloads/
5) Install the AWS CLI.

   Download and install the AWS CLI.
   The installer automatically adds the path of the AWS CLI to the system environment variable PATH. If the automatic path addition fails, refer to "AWS Command Line Interface" of the AWS document to add the path.
   If Python or the AWS CLI has been installed in an environment with EXPRESSCLUSTER already installed, restart the OS before operating EXPRESSCLUSTER.
6) Launch the command prompt as the Admistrator and execyute the command as shown below.

```
> aws configure
```

Input the information required to execute AWS CLI in response to the prompt. Do not input AWS access key ID and AWS secret access key.

```
AWS Access Key ID [None]: (Just press Enter key)AWS Secret Access Key␣
↪[None]: (Just press Enter key)Default region name [None]: <default␣
↪region name>Default output format [None]: text
```

For "Default output format", other format than "text" may be specified.

When you input the wrong data, delete the files under `%SystemDrive%\Users\Administrator\.aws` and the directory itself and repeat the step described above.

Setting up an instance by using IAM user

In this method, you can execute execute AWS CLI after creating the IAM user and storing its access key ID and secret access key in the instance. You do not have to assign the IAM role to the instance when creating the instance.

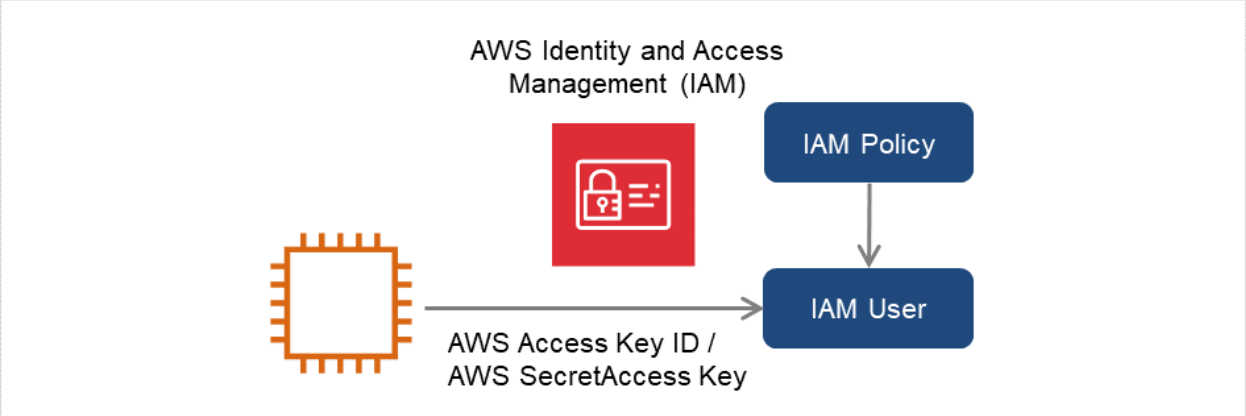


Fig. 6.3: Setting an instance by using IAM user

1) Create the IAM user and attach the IAM Policy to the role.
   You can create the IAM user in [Users] - [Create New Users] of IAM Management Console
2) Log on to the instance.
3) Install Python.
   Install Python required by EXPRESSCLUSTER. First, confirm that Python has been installed on the machine. If not, download Python from the following URL and install it. After installation, add the file path of python.exe to the PATH environment variable from the Control Panel. Since the Python command is executed as the SYSTEM user, please make sure that the path to the Python command is set in the system environment variable PATH.

   https://www.python.org/downloads/
4) Install the AWS CLI.

   Download and install the AWS CLI.
   The installer automatically adds the path of the AWS CLI to the system environment variable PATH. If the automatic path addition fails, refer to "AWS Command Line Interface" of the AWS document to add the path.
   If Python or the AWS CLI has been installed in an environment with EXPRESSCLUSTER already installed, restart the OS before operating EXPRESSCLUSTER.

5) Launch the command prompt as the Admistrator and execyute the command as shown below.

```
> aws configure
```

Input the information required to execute AWS CLI in response to the prompt. Obtain AWS access key ID and AWS secret access key from IAM user detail screen to input.

```
AWS Access Key ID [None]: <AWS access key>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.

When you input the wrong data, delete the files under `%SystemDrive%\Users\Administrator\.aws` and the directory itself and repeat the step described above.

6.2.19 Azure DNS resources

- For the procedures to install Azure CLI and create a service principal, refer to the "EXPRESSCLUSTER X HA Cluster Configuration Guide for Microsoft Azure (Windows)".
- The Azure CLI and Python must be installed because the Azure DNS resource uses them. When Azure CLI 2.0 is installed, Python is also installed. For details about the Azure CLI, refer to the following website:
  Microsoft Azure Documentation:
  https://docs.microsoft.com/en-us/azure/
- The Azure DNS service must be installed because the Azure DNS resource uses it. For details about Azure DNS, refer to the following website:
  Azure DNS:
  https://azure.microsoft.com/en-us/services/dns/
- To set up EXPRESSCLUSTER to work with Microsoft Azure, a Microsoft Azure organizational account is required. An account other than the organizational account cannot be used because an interactive login is required when executing the Azure CLI.
- It is necessary to create a service principal with Azure CLI.
  The Azure DNS resource logs in Microsoft Azure and performs the DNS zone registration. The Azure DNS resource uses Azure login based on service principal when logging in Microsoft Azure.
  For details about a service principal and procedure, refer to the following websites:

  Log in with Azure CLI 2.0:
  https://docs.microsoft.com/en-us/cli/azure/authenticate-azure-cli?view=azure-cli-latest

  Create an Azure service principal with Azure CLI 2.0:
  https://docs.microsoft.com/en-us/cli/azure/create-an-azure-service-principal-azure-cli?view=azure-cli-latest

  When changing the role of the created service principal from the default role "Contributor" to another role, select the role that can access all of the following operations as the Actions properties.
  If the role is changed to one that does not meet this condition, starting the Azure DNS resource fails due to an error.

  For Azure CLI 2.0:

Microsoft.Network/dnsZones/A/write
Microsoft.Network/dnsZones/A/delete
Microsoft.Network/dnsZones/NS/read

- Azure Private DNS is not supported.

6.2.20 Google Cloud virtual IP resources

- Using a Google Cloud virtual IP resource with Windows Server 2019 requires **Startup type** for the following services to be set at **Automatic (Delayed Start)**:
  - Google Compute Engine Agent
  - Google OSConfig Agent

6.2.21 Google Cloud DNS resources

- Google Cloud DNS resources use Cloud DNS by Google Cloud. For the details on Cloud DNS, refer to the following website.

Cloud DNS
https://cloud.google.com/dns/

- Cloud SDK needs to be installed to operate Cloud DNS. For the details on Cloud SDK, refer to the following website.

Cloud SDK
https://cloud.google.com/sdk/

- Cloud SDK needs to be authorized by the account with the permissions for the API methods below:

dns.changes.create
dns.changes.get
dns.managedZones.get
dns.resourceRecordSets.create
dns.resourceRecordSets.delete
dns.resourceRecordSets.list
dns.resourceRecordSets.update

As for authorizing Cloud SDK, refer to the following website.

Authorizing Cloud SDK tools
https://cloud.google.com/sdk/docs/authorizing

6.2.22 CLI settings in the OCI environtment

This section describes the settings of CLI in OCI environment.
Some of EXPRESSCLUSTER's functions internally run OCI CLI for their processes.
To run OCI CLI successfully, you need to set up in advance.

For OCI CLI settings, refer to the following website.

Oracle Cloud Infrastructure Documentation - Command Line Interface (CLI)
https://docs.oracle.com/en-us/iaas/Content/API/Concepts/cliconcepts.htm

6.2.23 Configuring OCI forced-stop resource

Using the OCI forced-stop resource requires changing parameter values in the following script, based on the directory where OCI CLI commands are installed and on the location where the OCI configuration file is stored:

```
<EXPRESSCLUSTER installation path>\cloud\oci\clpociforcestop.ps1

-   Parameter value to be changed according to the directory where OCI␣
↪CLI commands are installed
    $Env:Path += ";[directory where OCI CLI commands are installed]"
    Example: $Env:Path += ";C:\Users\opc\AppData\Local\Programs\Python\
↪Python36\Scripts\;C:\Users\opc\AppData\Local\Programs\Python\Python36\"

-   Parameter value to be changed according to the location where the OCI␣
↪configuration file is stored
    [string]$OCI_Path = "[path to the OCI configuration file]"
    Example: [string]$OCI_Path = "C:\Users\opc\.oci\config"
```

6.3 Notes when creating the cluster configuration data

Notes when creating a cluster configuration data and before configuring a cluster system is described in this section.

6.3.1 Folders and files in the location pointed to by the EXPRESSCLUSTER installation path

The folders and files in the location pointed to by the EXPRESSCLUSTER installation path must not be handled (edited, created, added, or deleted) by using any application or tool other than EXPRESSCLUSTER.
Any effect on the operation of a folder or file caused by using an application or tool other than EXPRESSCLUSTER will be outside the scope of NEC technical support.

6.3.2 Final action for group resource deactivation error

If select **No Operation** as the final action when a deactivation error is detected, the group does not stop but remains in the deactivation error status. Make sure not to set **No Operation** in the production environment.

6.3.3 Delay warning rate

If the delay warning rate is set to 0 or 100, the following can be achieved:

- When 0 is set to the delay monitoring rate
  An alert for the delay warning is issued at every monitoring.
  By using this feature, you can calculate the polling time for the monitor resource at the time the server is heavily loaded, which will allow you to determine the time for monitoring timeout of a monitor resource.
- When 100 is set to the delay monitoring rate
  The delay warning will not be issued.

Be sure not to set a low value, such as 0%, except for a test operation.

6.3.4 Monitoring method TUR for disk monitor resource and hybrid disk TUR monitor resource

- You cannot use the TUR methods on a disk or disk interface (HBA) that does not support the Test Unit Ready (TUR) command of SCSI. Even if your hardware supports these commands, consult the driver specifications because the driver may not support them.
- TUR methods burdens OS and disk load less compared to Read methods.
- In some cases, TUR methods may not be able to detect errors in I/O to the actual media.

6.3.5 Heartbeat resource settings

- For an interconnect with the highest priority, configure LAN heartbeat resources or kernel mode LAN heartbeat resources which can be exchanged between all servers.
- Configuring at least two kernel mode LAN heartbeat resources is recommended unless it is difficult to add a network to an environment such as the cloud or a remote cluster.
- It is recommended to register both an interconnect-dedicated LAN and a public LAN as LAN heartbeat resources.
- Time for heartbeat timeout needs to be shorter than the time required for restarting the OS. If the heartbeat timeout is not configured in this way, an error may occur after reboot in some servers in the cluster because other servers cannot detect the reboot.

6.3.6 Double-byte character set that can be used in script comments

- Scripts edited in Windows environment are dealt as Shift-JIS code, and scripts edited in Linux environment are dealt as EUC code. In case that other character codes are used, character corruption may occur depending on environment.

6.3.7 The number of server groups that can be set as servers to be started in a group

- The number of server groups that can be set as servers to be started in one group is 2.
  If three or more server groups are set, the ExpessCluster Disk Agent service (clpdiskagent.exe) may not operate properly.

6.3.8 Setting up JVM monitor resources

- When the monitoring target is WebLogic, the maximum values of the following JVM monitor resource settings may be limited due to the system environment (including the amount of installed memory):
  - **The number** under **Monitor the requests in Work Manager**
  - **Average** under **Monitor the requests in Work Manager**
  - **The number** of **Waiting Requests** under **Monitor the requests in Thread Pool**
  - **Average** of **Waiting Requests** under **Monitor the requests in Thread Pool**
  - **The number** of **Executing Requests** under **Monitor the requests in Thread Pool**
  - **Average** of **Executing Requests** under **Monitor the requests in Thread Pool**
- To use the Java Resource Agent, install the Java runtime environment (JRE) described in "Operation environment for JVM monitor" in "4. *Installation requirements for EXPRESSCLUSTER*" or a Java development kit (JDK). You can use either the same JRE or JDK as that used by the monitoring target (WebLogic Server or WebOTX) or a different one. If both JRE and JDK are installed on a server, you can use either one.
- The monitor resource name must not include a blank.

6.3.9 System monitor resource settings

- Pattern of detection by resource monitoring

  The System Resource Agent performs detection by using thresholds and monitoring duration time as parameters.

  The System Resource Agent collects the data (used size of memory, CPU usage rate, and used size of virtual memory) on individual system resources continuously, and detects errors when data keeps exceeding a threshold for a certain time (specified as the duration time).

6.3.10 Setting up PostgreSQL monitor resource

- The monitor resource name must not include a blank.

6.3.11 Setting up AWS Elastic IP resources

- IPv6 is not supported.
- In the AWS environment, floating IP resources, floating IP monitor resources, virtual IP resources, virtual IP monitor resources, virtual computer name resources, and virtual computer name monitor resources cannot be used.
- Only ASCII characters is supported. Check that the character besides ASCII character isn't included in an execution result of the following command.

  aws ec2 describe-addresses --allocation-ids *<EIP ALLOCATION ID>*
- AWS elastic IP resources associate an EIP with the primary private IP address of an ENI, but not with its secondary private IP address.

6.3.12 Setting up AWS Virtual IP resources

- IPv6 is not supported.
- In the AWS environment, floating IP resources, floating IP monitor resources, virtual IP resources, virtual IP monitor resources, virtual computer name resources, and virtual computer name monitor resources cannot be used.
- Only ASCII characters is supported. Check that the character besides ASCII character isn't included in an execution result of the following command.

  ```
  aws ec2 describe-vpcs --vpc-ids <VPC ID>
  aws ec2 describe-route-tables --filters Name=vpc-id,Values=<VPC ID>
  aws ec2 describe-network-interfaces --network-interface-ids <ENI ID>
  ```
- 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.
- When a AWS Virtual IP resource is set, Windows registers the physical host name and VIP record in the DNS (if the property of the corresponding network adapter for registering addresses to the DNS is set to ON). To convert the IP address linked by the physical host name resolution into a physical IP address, set the relevant data as follows.

  - Check the setting of the network adapter to which the corresponding VIP address is assigned, by choosing Properties - Internet Protocol Version 4 - Advanced - DNS tab - Register this connection's address in DNS. If this check box is selected, clear it.
  - Additionally, execute one of the following in order to apply this setting:
    * Reboot the DNS Client service.
    * Explicitly run the ipconfig/registerdns command.
  - Register the physical IP address of the network adapter to which the corresponding VIP address is assigned to the DNS server statically.

- An AWS virtual IP resource starts up normally, even if the route table to be used by instances does not include any route to an IP address to be used by the AWS virtual IP resource. This operation is as required. When activated, an AWS virtual IP resource updates the content of a route table that includes a specified IP address entry. Finding no route table, the resource considers the situation as nothing to be updated and therefore as normal. Which route table should have a specified entry, depending on the system configuration, is not the resource's criterion for judging the normality.
- An AWS virtual IP resource uses a Windows OS API to add a virtual IP address to a NIC--without setting the skipassource flag. Hence this flag is disabled after the AWS virtual IP resource is activated. However, the skipassource flag can be enabled by using PowerShell after the activation of the resource.

6.3.13 Setting up AWS Secondary IP resources

- IPv6 is not supported.
- In the AWS environment, floating IP resources, floating IP monitor resources, virtual IP resources, virtual IP monitor resources, virtual computer name resources, and virtual computer name monitor resources cannot be used.
- Only ASCII characters is supported. Check that the character besides ASCII character isn't included in an execution result of the following command.

```
aws ec2 describe-network-interfaces --network-interface-ids <ENI ID>
aws ec2 describe-subnets --subnet-ids <SUBNET_ID>
```

- No AWS secondary IP resources can be used in a configuration with a different subnet.
- The number of secondary IP addresses to be assigned for AWS secondary IP resources has an upper limit for each instance type.
  For more information, refer to the following:
  https://docs.aws.amazon.com/en_us/AWSEC2/latest/UserGuide/using-eni.html#AvailableIpPerENI
- Statically register the physical IP addresses of network adapters to which secondary IP addresses are to be assigned for AWS secondary IP resources.
  For more information, refer to Step 1 of the following:
  https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/config-windows-multiple-ip.html
- An AWS secondary IP resource adds a secondary IP address to a NIC with the help of the netsh command--with the skipassource flag not set. Hence this flag is disabled after the AWS secondary IP resource is activated. However, the skipassource flag can be enabled by using PowerShell after the activation of the resource.

6.3.14 Setting up AWS DNS resources

- IPv6 is not supported.
- In the AWS environment, floating IP resources, floating IP monitor resources, virtual IP resources, virtual IP monitor resources, virtual computer name resource, and virtual computer name monitor resource cannot be used.
- In the **Resource Record Set Name** field, enter a name without an escape code. If it is included in the **Resource Record Set Name**, a monitor error occurs.
- When activated, an AWS DNS resource does not await the completion of propagating changed DNS settings to all Amazon Route 53 DNS servers. This is due to the specification of Route 53: It takes time for the changes of a resource record set to be propagated throughout the network. Refer to "*Setting up AWS DNS monitor resources*".
- Associated with a single account, an AWS DNS resource cannot be used for different accounts, AWS access key IDs, or AWS secret access keys. If you want such usage, consider creating a script to execute the AWS CLI with a script resource and then setting the environment variables in the script for authenticating other accounts.

6.3.15 Setting up AWS DNS monitor resources

- The AWS DNS monitor resource runs the AWS CLI for monitoring. The AWS DNS monitor resource uses **AWS CLI Timeout** set to the AWS DNS resource as the timeout of the AWS CLI execution.
- Immediately after the AWS DNS resource is activated, monitoring by the AWS DNS monitor resource may fail due to the following events. If monitoring failed, set **Wait Time to Start Monitoring** of the AWS DNS monitor resource longer than the time to reflect the changed DNS setting of Amazon Route 53 (https://aws.amazon.com/route53/faqs/).
  - When the AWS DNS resource is activated, a resource record set is added or updated.
  - If the AWS DNS monitor resource starts monitoring before the changed DNS setting of Amazon Route 53 is applied, name resolution cannot be done and monitoring fails.
    The AWS DNS monitor resource will continue to fail monitoring while a DNS resolver cache is enabled.
  - The changed DNS setting of Amazon Route 53 is applied.
  - Name resolution succeeds after the **TTL** valid period of the AWS DNS resource elapses. Then, the AWS DNS monitor resource succeeds monitoring.

6.3.16 Setting up Azure probe port resources

- IPv6 is not supported.
- In the Microsoft Azure environment, floating IP resources, floating IP monitor resources, virtual IP resources, virtual IP monitor resources, virtual computer name resources, and virtual computer name monitor resources cannot be used.

6.3.17 Setting up Azure load balance monitor resources

- When a Azure load balance monitor resource error is detected, there is a possibility that switching of the active server and the stand-by server from Azure load balancer is not performed correctly. Therefore, in the **Final Action** of Azure load balance monitor resources and the recommended that you select **Stop the cluster service and shutdown OS**.

6.3.18 Setting up Azure DNS resources

- IPv6 is not supported.
- In the Microsoft Azure environment, floating IP resources, floating IP monitor resources, virtual IP resources, virtual IP monitor resources, virtual computer name resources, and virtual computer name monitor resources cannot be used.

6.3.19 Setting up Google Cloud virtual IP resources

- IPv6 is not supported.

6.3.20 Setting up Google Cloud load balance monitor resources

- For **Final Action** of Google Cloud load balance monitor resources, selecting **Stop the cluster service and shutdown OS** is recommended. When a Google Cloud load balance monitor resource detects an error, the load balancer may not correctly switch between the active server and the standby server.

6.3.21 Setting up Google Cloud DNS resources

- IPv6 is not supported.
- In the Google Cloud Platform environment, floating IP resources, floating IP monitor resources, virtual IP resources, and virtual IP monitor resources cannot be used.
- When using multiple Google Cloud DNS resources in the cluster, you need to configure them to prevent their simultaneous activation/deactivation for their dependence or a wait for a group start/stop. Their simultaneous activation/deactivation may cause an error.

6.3.22 Setting up Oracle Cloud virtual IP resources

- IPv6 is not supported.

6.3.23 Setting up Oracle Cloud load balance monitor resources

- For **Final Action** of Oracle Cloud load balance monitor resources, selecting **Stop the cluster service and shutdown OS** is recommended. When an Oracle Cloud load balance monitor resource detects an error, the load balancer may not correctly switch between the active server and the standby server.

6.3.24 Recovery operation on systems with Windows Server 2012 or later when a service fails

This applies to systems with Windows Server 2012 or later, with **Restart Computer** selected as the recovery option to be exercised when a service fails (abends): If the failure actually occurs, the OS is restarted not in the same way as on Windows Server 2008 or earlier but with a STOP error.

The EXPRESSCLUSTER services for which **Restart Computer** is set as the recovery operation by default are the following:

- EXPRESSCLUSTER Disk Agent service
- EXPRESSCLUSTER Node Manager service
- EXPRESSCLUSTER Server service
- EXPRESSCLUSTER Transaction service

6.3.25 Coexistence with the Network Load Balancing function of the OS

The IP address added to the NIC that is used by the Network Load Balancing (NLB) function of the OS is recognized as a virtual IP address of the NLB.

It is assumed that this virtual IP address is assigned to all servers within the NLB cluster.

If a floating IP address is assigned to the relevant NIC, the assigned floating IP address is also recognized as a virtual IP address.

When this floating IP address is accessed, the NLB function also balances the load of a network. However, since a floating IP address is not assigned to the NIC of the standby server, an error may occur in accessing to the floating IP address.

6.3.26 Note on applying the HBA configuration

When you create a new cluster by changing the access control settings under the **HBA** tab of the **Server Properties** dialog box and uploading the configuration data, you are possibly not prompted to restart the OS to apply the change. Even so, restart the OS after changing the access control settings under the **HBA** tab to apply the configuration data.

6.3.27 Coexistence of a mirror disk resource with a hybrid disk resource

A mirror disk resource and a hybrid disk resource cannot coexist in the same failover group.

6.4 After starting operating EXPRESSCLUSTER

Notes on situations you may encounter after start operating EXPRESSCLUSTER are described in this section.

6.4.1 Limitations during the recovery operation

Do not perform the following operations by the Cluster WebUI or from the command line while recovery processing is changing (reactivation -> failover -> last operation), if a group resource such as disk resource or application resource is specified as a recovery target and when a monitor resource detects an error.

- Stop and suspend of a cluster
- Start, stop, moving of a group

If these operations are controlled at the transition to recovering due to an error detected by a monitor resource, the other group resources in the group may not be stopped.
Even if a monitor resource detects an error, it is possible to control the operations above after the last operation is performed.

6.4.2 Executable format file and script file not described in the command reference

Executable format files and script files which are not described in "EXPRESSCLUSTER command reference" in the "Reference Guide" exist under the installation directory. Do not run these files on any system other than EXPRESSCLUSTER. The consequences of running these files will not be supported.

6.4.3 Cluster shutdown and cluster shutdown reboot

When using a mirror disk, do not execute cluster shutdown or cluster shutdown reboot from the clpstdn command or the Cluster WebUI while a group is being activated. A group cannot be deactivated while being activated. OS may shut down while mirror disk resource is not properly deactivated and mirror break may occur.

6.4.4 Shutdown and reboot of individual server

With a mirror disk used, a mirror break is caused by using a command or Cluster WebUI to stop a cluster service on a server, shut down a server, or run the shutdown reboot command.

6.4.5 Recovery from network partition status

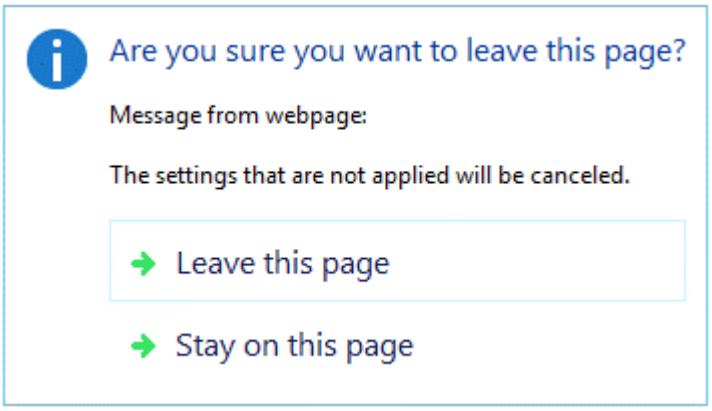
The servers that constitute a cluster cannot check the status of other servers if a network partition occurs. Therefore, if a group is operated (started/stopped/moved) or a server is restarted in this status, a recognition gap about the cluster status occurs among the servers. If a network is recovered in a state that servers with different recognitions about the cluster status are running like this, a group cannot be operated normally after that. For this reason, during the network partition status, shut down the server separated from the network (the one cannot communicate with the client) or stop the EXPRESSCLUSTER Server service. Then, start the server again and return to the cluster after the network is recovered. In case that a network is recovered in a state that multiple servers have been started, it becomes possible to return to the normal status, by restarting the servers with different recognitions about the cluster status.

When a network partition resolution resource is used, even though a network partition occurs, emergent shut-down of a server (or all the servers) is performed. This prevents two or more servers that cannot communicate with one another

from being started. When manually restarting the server that emergent shut down took place, or when setting the operations during the emergent shut down to restarting, the restarted server performs emergent shut down again. (In case of ping method or majority method, the EXPRESSCLUSTER Server service will stop.) However, if two or more disk heartbeat partitions are used by the disk method, and if a network partition occurs in the state that communication through the disk cannot be performed due to a disk failure, both of the servers may continue their operations with being suspended.

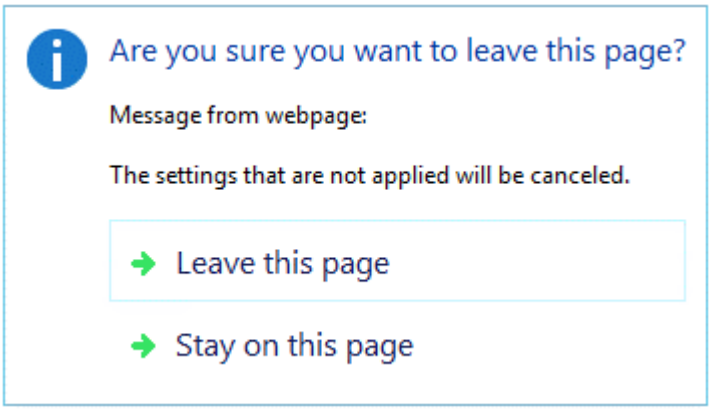
6.4.6 Notes on the Cluster WebUI

- If the Cluster WebUI is operated in the state that it cannot communicate with the connection destination, it may take a while until the control returns.
- When going through the proxy server, configure the settings for the proxy server be able to relay the port number of the Cluster WebUI.
- When going through the reverse proxy server, the Cluster WebUI will not operate properly.
- When updating EXPRESSCLUSTER, close all running browsers. Clear the browser cache and restart the browser.
- Cluster configuration data created using a later version of this product cannot be used with this product.
- When closing the Web browser, the dialog box to confirm to save may be displayed.



When you continue to edit, click the **Stay on this page** button.

- Reloading the Web browser (by selecting **Refresh from the menu** or tool bar) , the dialog box to confirm to save may be displayed.



When you continue to edit, click the **Stay on this page** button.

- For notes and restrictions of Cluster WebUI other than the above, see the online manual.

6.4.7 EXPRESSCLUSTER Disk Agent Service

Make sure not to stop the EXPRESSCLUSTER Disk Agent Service. This cannot be manually started once you stop. Restart the OS, and then restart the EXPRESSCLUSTER Disk Agent Service.

6.4.8 Changing the cluster configuration data during mirroring

Make sure not to change the cluster configuration data during the mirroring process including initial mirror configuration. The driver may malfunction if the cluster configuration is changed.

6.4.9 Returning the stand-by server to the cluster during mirror-disk activation

If the stand-by server is running while the cluster service (EXPRESSCLUSTER server service) is stopped and the mirror disk is activated, restart the stand-by server before starting the service and returning the stand-by server to the cluster. If the stand-by server is returned without being restarted, the information about mirror differences will be invalid and a mirror disk inconsistency will occur.

6.4.10 Changing the configuration between the mirror disk and hybrid disk

To change the configuration so that the disk mirrored using a mirror disk resource will be mirrored using a hybrid disk resource, first delete the existing mirror disk resource from the configuration data, and then upload the data. Next, add a hybrid disk resource to the configuration data, and then upload it again. You can change a hybrid disk to a mirror disk in a similar way.

If you upload configuration data in which the existing resource has been replaced with a new one without deleting the existing resource as described above, the disk mirroring setting might not be changed properly, potentially resulting in a malfunction.

6.4.11 chkdsk command and defragmentation

The chkdsk command or defragmentation to be executed on a switchable partition controlled by a disk resource or a data partition mirrored by a mirror disk resource must be executed on the server where the resource has already been started. Otherwise, the command or defragmentation cannot be executed due to access restriction.

When the chkdsk command is run in the restoration mode (/f option), stop the failover group and execute it while only the target disk resource/mirror disk resource is running. If not, and files or folders in the target partition are open, running the command. When there is a Disk RW monitor resource which monitors the target partition, it is necessary to suspend this monitor resource.

6.4.12 Index service

When you create a shared disk/mirror disk directory on the index service catalogue to make an index for the folders on the shared disk / mirror disk, it is necessary to configure the index service to be started manually and to be controlled from EXPRESSCLUSTER so that the index service starts after the shared disk / mirror disk is activated. If the index service is configured to start automatically, the index service opens the target volume, which leads to failure in mounting upon the following activation, resulting in failure in disk access from an application or explorer with the message telling the parameter is wrong.

6.4.13 Issues with User Account Control (UAC) in a Windows Server 2012 or later environment

In a Windows Server 2012 or later environment, User Account Control (UAC) is enabled by default. When UAC is enabled, there are following issues.

- Monitor Resource
  Following resource has issues with UAC.
  - Oracle Monitor Resource
    For the Oracle monitor resource, if you select **OS Authentication** for **Authentication Method** and then set any user other than those in the Administrators group as the monitor user, the Oracle monitoring processing will fail.
    When you set **OS Authentication** in **Authentication Method**, the user to be set in **Monitor User** must belong to the Administrators group.

6.4.14 Screen display of application resource / Script resource

Since the processes started from the application resource or Script resource of EXPRESSCLUSTER are executed in session 0, when you start a process having GUI, the **Interactive services dialog detection** pop-up menu is displayed. Unless you select **Show me the message**, GUI is not displayed.

6.4.15 Environment in which the network interface card (NIC) is duplicated

In an environment in which the NIC is duplicated, NIC initialization at OS startup may take some time. If the cluster starts before the NIC is initialized, the starting of the kernel mode LAN heartbeat resource (lankhb) may fail. In such cases, the kernel mode LAN heartbeat resource cannot be restored to its normal status even if NIC initialization is completed. To restore the kernel mode LAN heartbeat resource, you must first suspend the cluster and then resume it.

In that environment, we recommend to delay startup of the cluster by following setting.

- Network Initialization Complete Wait Time Setting
  You can configure this setting in the **Timeout** tab of **Cluster Properties**. This setting will be enabled on all cluster servers. If NIC initialization is completed within timeout, the cluster service starts up.

6.4.16 EXPRESSCLUSTER service login account

The EXPRESSCLUSTER service login account is set in **Local System Account**. If this account setting is changed, EXPRESSCLUSTER might not properly operate as a cluster.

6.4.17 Monitoring the EXPRESSCLUSTER resident process

The EXPRESSCLUSTER resident process can be monitored by using software monitoring processes. However, recovery actions such as restarting a process when the process abnormally terminated must not be executed.

6.4.18 Message receive monitor resource settings

- Error notification to message receive monitor resources can be done in any of three ways: using the clprexec command, or linkage with the server management infrastructure.
- To use the clprexec command, use the relevant file stored on the EXPRESSCLUSTER CD. Use this method according to the OS and architecture of the notification-source server. The notification-source server must be able to communicate with the notification-destination server.

6.4.19 JVM monitor resources

- When restarting the monitoring-target Java VM, you must first suspend JVM monitor resources or stop the cluster.
- When changing the JVM monitor resource settings, you must suspend and resume the cluster.
- JVM monitor resources do not support a delay warning for monitor resources.

6.4.20 System monitor resources, Process resource monitor resource

- To change a setting, the cluster must be suspended.
- System monitor resources do not support a delay warning for monitor resources.
- If the date and time of the OS is changed during operation, the timing of analysis processing being performed at 10-minute intervals will change only once immediately after the date and time is changed. This will cause the following to occur; suspend and resume the cluster as necessary.
  - An error is not detected even when the time to be detected as abnormal elapses.
  - An error is detected before the time to be detected as abnormal elapses.
- Up to 26 disks that can be monitored by the System monitor resources of disk resource monitor function at the same time.

6.4.21 Event log output relating to linkage between mirror statistical information collection function and OS standard function

- The following error may be output to an application event log in the environment where the internal version is updated from 11.16 or earlier.
- Event ID: 1008

  Source: Perflib

  Message: The Open Procedure for service clpdiskperf in DLL <EXPRESSCLUSTER installation path>binclpdiskperf.dll failed. Performance data for this service will not be available. The first four bytes (DWORD) of the Data section contains the error code.

  If the linkage function for the mirror statistical information collection function and OS standard function is used, execute the following command at the Command Prompt to suppress this message.

  ```
  >lodctr.exe <EXPRESSCLUSTER installation path>\perf\clpdiskperf.ini
  ```

  When the linkage function is not used, even if this message is output, there is no problem in EXPRESSCLUSTER and performance monitor operations. If this message is frequently output, execute the following two commands at the Command Prompt to suppress this message.

  ```
  > unlodctr.exe clpdiskperf
  > reg delete HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
  ↪clpdiskperf
  ```

- If the linkage function for the mirror statistical information collection function and OS standard function is enabled, the following error may be output in an application event log:
- Event ID: 4806

  Source: EXPRESSCLUSTER X

  Message: Cluster Disk Resource Performance Data can't be collected because a performance monitor is too numerous.

  When the linkage function is not used, even if this message is output, there is no problem in EXPRESSCLUSTER and performance monitor operations. If this message is frequently output, execute the following two commands at the Command Prompt to suppress this message.

  ```
  > unlodctr.exe clpdiskperf
  > reg delete HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
  ↪clpdiskperf
  ```

Refer to the following for the linkage function for the mirror statistical information collection function and OS standard function.

"Maintenance Guide"
The system maintenance information
Mirror statistics information collection function
Linkage between the mirror statistics information collection function and OS standard functions

6.4.22 Display of the Interactive services dialog detection pop-up menu

To allow the **Interactive services dialog detection** pop-up menu to be displayed by setting the **Allow to Interact with Desktop** of the application resource or Script resource, the "Interactive Services Detection" service must have been started.

The startup of the "Interactive Services Detection" service with its default settings is invalid. Follow the procedure below to validate the service.

See also:

Reference site : http://msdn.microsoft.com/en-us/library/windows/desktop/ms683502(v=vs.85).aspx
-> Using an Interactive Service

6.4.23 Restoration from an AMI in an AWS environment

If the ENI ID of a primary network interface is set to the **ENI ID** of the AWS virtual ip resource or AWS Elastic IP resource or AWS secondary ip resource, the AWS virtual ip resource or AWS Elastic IP resource or AWS secondary ip resource setting is required to change when restoring data from an AMI.

If the ENI ID of a secondary network interface is set to the **ENI ID** of the AWS virtual ip resource or AWS Elastic IP resource or AWS secondary ip resource, it is unnecessary to set the AWS virtual ip resource or AWS Elastic IP resource or AWS secondary ip resource again because the same ENI ID is inherited by a detach/attach processing when restoring data from an AMI.

6.5 Notes when changing the EXPRESSCLUSTER configuration

The section describes what happens when the configuration is changed after starting to use EXPRESSCLUSTER in the cluster configuration.

6.5.1 Exclusive rule of group common properties

When the exclusive attribute of the exclusive rule is changed, the change is applied by suspending and resuming the cluster.
When a group is added to the exclusive rule whose exclusive attribute is set to Absolute, multiple groups of **Absolute** may start on the same server depending on the group startup status before suspending the cluster.
Exclusive control will be performed at the next group startup.

6.5.2 Dependency between resource properties

When the dependency between resources has been changed, the change is applied by suspending and resuming the cluster.
If a change in the dependency between resources that requires the resources to be stopped during application is made, the startup status of the resources after the resume may not reflect the changed dependency.
Dependency control will be performed at the next group startup.

6.5.3 Setting cluster statistics information of message receive monitor resources

Once the settings of cluster statistics information of monitor resource has been changed, the settings of cluster statistics information are not applied to message receive monitor resources even if you execute the suspend and resume. Reboot the OS to apply the settings to the message receive monitor resources.

6.5.4 Changing a port number

If you have changed a port number with the server firewall enabled, the firewall configuration needs to be changed as well by using the clpfwctrl command. For more information, see "Reference Guide" -> "EXPRESSCLUSTER command reference" -> "Adding a firewall rule (clpfwctrl command)".

6.6 Notes on upgrading EXPRESSCLUSTER

This section describes the notes on upgrading EXPRESSCLUSTER after starting a cluster operation.

6.6.1 Changed functions

The following describes the functions changed for each of the versions.

Internal version 12.00

- Management tool
  The default management tool has been changed to Cluster WebUI. If you want to use the conventional WebManager as the management tool, specify "http://management IP address of management group or actual IP address:port number of the server in which EXPRESSCLUSTER Server is installed/main.htm" in the address bar of a web browser.
- Mirror/Hybrid disk resource
  Considering that the minimum size of a cluster partition has been increased to 1 GiB, prepare a sufficient size of it for upgrading EXPRESSCLUSTER..

Internal Version 12.10

- Configuration tool
  The default configuration tool has been changed to Cluster WebUI, which allows you to manage and configure clusters with Cluster WebUI.
- Cluster statistical information collection function
  By default, the cluster statistical information collection function saves statistics information files under the installation path. To avoid saving the files for such reasons as insufficient disk capacity, disable the cluster statistical information collection function. For more information on settings for this function, see "Parameter details" in the Reference Guide.
- System monitor resource
  The **System Resource Agent process settings** part of the system monitor resource has been separated to become a new monitor resource. Therefore, the conventional monitor settings of the **System Resource Agent process settings** are no longer valid. To continue the conventional monitoring, configure it by registering a new process resource monitor resource after upgrading EXPRESSCLUSTER. For more information on monitor settings for process resource monitor resources, see "Understanding process resource monitor resources" in "Monitor resource details" in the "Reference Guide".
- BMC linkage
  The ipmiutil parameters have been changed as follows.

  Before the change (12.01 or earlier)

  Forced Stop Action

Forced Stop Action	Parameters
BMC Power Off	ireset.cmd -d -J 0 -N *ip_address* -U *username* -P *password*
BMC Reset	ireset.cmd -r -J 0 -N *ip_address* -U *username* -P *password*
BMC Power Cycle	ireset.cmd -c -J 0 -N *ip_address* -U *username* -P *password*
BMC NMI	ireset.cmd -n -J 0 -N *ip_address* -U *username* -P *password*

  Chassis Identify

Chassis Identify	Parameters
Blinking	ialarms.cmd -i250 -J 0 -N *ip_address* -U *username* -P *password*
Off	ialarms.cmd -i0 -J 0 -N *ip_address* -U *username* -P *password*

After the change

Forced Stop Action

Forced Stop Action	Parameters
BMC Power Off	ireset.cmd -d -N *ip_address* -U *username* -P *password*
BMC Reset	ireset.cmd -r -N *ip_address* -U *username* -P *password*
BMC Power Cycle	ireset.cmd -c -N *ip_address* -U *username* -P *password*
BMC NMI	ireset.cmd -n -N *ip_address* -U *username* -P *password*

Chassis Identify

Chassis Identify	Parameters
	ialarms.cmd -i250 -N *ip_address* -U *username* -P *password*
	ialarms.cmd -i0 -N *ip_address* -U *username* -P *password*

Internal Version 12.20

- AWS AZ monitor resource

  The way of evaluating the AZ status grasped through the AWS CLI has been changed: available as normal, information or impaired as warning, and unavailable as warning. (Previously, any AZ status other than **available** was evaluated as abnormal.)

Internal Version 12.30

- Weblogic monitor resource

  REST API has been added as a new monitoring method. From this version, REST API is the default value for the monitoring method. At the version upgrade, reconfigure the monitoring method.

  The default value of the password has been changed. If you use weblogic that is the previous default value, reset the password default value.

Internal Version 13.00

- Forced stop function and scripts

  These have been redesigned as individual forced stop resources adapted to environment types.

  Since the forced stop function and scripts configured before the upgrade are no longer effective, set them up again as forced stop resources.

6.6.2 Removed Functions

The following describes the functions removed for each of the versions. **Internal Version 12.00**

- WebManager Mobile
- OfficeScan CL monitor resource
- OfficeScan SV monitor resource
- OracleAS monitor resource

Important:

Upgrading EXPRESSCLUSTER from its old version requires manually updating the cluster configuration data for functions with corresponding actions described in the table below.

For information on how to upgrade EXPRESSCLUSTER, see "Installation and Configuration Guide" -> "Installing EXPRESSCLUSTER" -> "Installing the EXPRESSCLUSTER Server" -> "Upgrading EXPRESSCLUSTER Server from the previous version". Then, at the timing described in the guide, follow each of the procedures described in the Action column.

Internal Version 13.00

Function	Action
WebManager/Builder	
COM network partition resolution resources	1. Open **Cluster Properties** -> **NP resolution tab**, then remove each NP resolution resource whose type is **unknown**.
NAS resources NAS monitor resources	1. If NAS resources are individually set in group resources' dependency, remove the dependency settings first. For the group resources, open **Resource Properties** -> the **Dependency** tab, select the NAS resources, and then click the **deleted** button to exclude them from the dependency. 2. Delete NAS resources, and NAS monitor resources will also be deleted.
Print spooler resources Print spooler monitor resources	1. If print spooler resources are individually set in group resources' dependency, remove the dependency settings first. For the group resources, open **Resource Properties** -> the **Dependency** tab, select the print spooler resources, and then click the **deleted** button to exclude them from the dependency. 2. Delete print spooler resources, and print spooler monitor resources will also be deleted.
Virtual machine groups Virtual machine resources Virtual machine monitor resources	You cannot move configuration data (for a host cluster) which involves virtual machine groups.
BMC linkage	1. Delete relevant message reception monitor resources.

Continued on next page

Table 6.18 – continued from previous page

Function	Action
Compatible commands	1. • Script resources • Custom monitor resources • Scripts before final action • Scripts before and after activation/deactivation • Recovery scripts • Pre-recovery action scripts • Forced-stop scripts • Other scripts configured with EXPRESSCLUSTER If any of these scripts includes a compatible command, modify the script by excluding the command. Example To start or stop services controlled with the armload command, use the sc command instead. To monitor services, use service monitor resources instead. 2. If you used armdelay to specify a delay time for starting EXPRESSCLUSTER services, open the **Cluster properties Timeout** tab, then specify the value in **Service Startup Delay Time** instead.
Controlling CPU frequency command (clpcpufreq command)	-
Estimating the amount of resource usage command (clpprer command)	-
Controlling chassis identify lamp command (clpledctrl command)	-
Processing inter-cluster linkage command (clptrnreq command)	-
Changing BMC information command (clpbmccnf command)	-

Continued on next page

Table 6.18 – continued from previous page

Function	Action
Broadcast for kernel mode LAN heartbeat resources	The **Broadcast** option (see **Heartbeat I/F -> Cast Method**) has been removed. If you use cluster configuration data created with an old version, **Unicast** is applied for the heartbeat transmission.
EXPRESSCLUSTER Task Manager	-
EXPRESSCLUSTER clients	-
Linking with the load balancer (JVM monitor resource)	-
The forced stop function using the System Center Virtual Machine Manager (SCVMM)	-
Mirror connect monitor resource (Integrated into mirror disk monitor resource)	Delete Mirror connect monitor resources.

6.6.3 Removed Parameters

The following tables show the parameters configurable with Cluster WebUI but removed for each of the versions.

Internal Version 12.00

Cluster

Parameters	default values
Cluster Properties	
WebManager Tab	
• Enable WebManager Mobile Connection	Off
WebManager Mobile Password	
• Password for Operation	-
• Password for Reference	-

JVM monitor resource

Parameters	default values
JVM Monitor Resource Properties	
Monitor (special) Tab	

Continued on next page

Table 6.20 – continued from previous page

Parameters	default values
Memory Tab (when Oracle Java is selected for JVM type)	
• Monitor Virtual Memory Usage	2048 MB
Memory Tab (when Oracle Java(usage monitoring) is selected for JVM Type)	
• Monitor Virtual Memory Usage	2048 MB

User mode monitor resource

Parameters	default values
User mode Monitor Resource Properties	
Monitor (special) Tab	
• Use Heartbeat Interval/Timeout	On

Internal Version 12.10

Cluster

Parameters	default values
Cluster Properties	
WebManager Tab	
WebManager Tuning Properties	
Behavior Tab	
• Max. Number of Alert Records on the Viewer	300
• Client Data Update Method	Real Time

Virtual Computer Name resource

Parameters	default values
Virtual Computer Name Resource Properties	
Details Tab	
Virtual Computer Name Resource Tuning Properties	
Parameter Tab	
• IP address to be associated[7]	FIP

Internal Version 13.00

Cluster

Parameters	default values
Cluster Properties	
Interconnect Tab	
Broadcast/Unicast	Unicast
Extension Tab	
• Virtual Machine Forced Stop Setting - Virtual Machine Management Tool	vCenter
• Virtual Machine Forced Stop Setting - Command	C:\Program Files (x86)\VMware\VMware vSphere CLI\Perl\apps\vm\vmcontrol.pl
• Execute Script for Forced Stop	Off
Server Properties	
Info Tab	
• Virtual Machine	Off
• Type	vSphere
BMC Tab	
• Forced Stop Command Line	-
• Chassis Identify - Flash / Turn off	-

6.6.4 Changed Default Values

The following tables show the parameters which are configurable with Cluster WebUI but whose defaults have been changed for each of the versions.

- To continue using a "Default value before update" after the upgrade, change the corresponding "Default value after update" to the desired one.
- Any setting other than a "Default value before update" is inherited to the upgraded version and therefore does not need to be restored.

Internal Version 12.00

[7]

From the IP address to be associated group box, the Public option has been removed.
When using configuration data with the Public option selected, you do not need to change it.
To change the IP address, select Any Address and specify the desired address.

Cluster

Parameters	Default value before update	Default value after update	Remarks
Cluster Properties			
JVM monitor Tab			
• Maximum Java Heap Size	7 MB	16 MB	
Extension Tab			
• Failover Count Method	Cluster	Server	

Group Resource (Common)

Parameters	Default value before update	Default value after update	Remarks
Resource Common Properties			
Recovery Operation Tab			
• Failover Threshold	Set as much as the number of the servers	1 time	This was also changed because the default value of Cluster Properties > Expand tab > Unit for Counting Failover Occurrences was changed.

Application resource

Parameters	Default value before update	Default value after update	Remarks
Application Resource Properties			
Dependency Tab			

Continued on next page

Table 6.27 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Follow the default dependence	On - CIFS resource - disk resource - Floating IP resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - Azure probe port resource	On - CIFS resource - Disk resource - Floating ip resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	

Registry synchronization resource

Parameters	Default value before update	Default value after update	Remarks
Registry Synchronization Resource Properties			
Dependency Tab			

Continued on next page

Table 6.28 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Follow the default dependence	On - CIFS resource - Disk resource - Floating IPresource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - Azure probe port resource	On - CIFS resource - Disk resource - Floating IPresource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	

Script resource

Parameters	Default value before update	Default value after update	Remarks
Script Resource Properties			
Dependency Tab			

Continued on next page

Table 6.29 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Follow the default dependence	On - CIFS resource - Disk resource - Floating IP resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - Azure probe port resource	On - CIFS resource - Disk resource - Floating ip resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	

Service resource

Parameters	Default value before update	Default value after update	Remarks
Service Resource Properties			
Dependency Tab			

Continued on next page

Table 6.30 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Follow the default dependence	On - CIFS resource - Disk resource - Floating IP resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - Azure probe port resource	On - CIFS resource - Disk resource - Floating IP resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IPresource - AWS virtual IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	

Monitor resource (common)

Parameters	Default value before update	Default value after update	Remarks
Monitor Resource Common Properties			
Recovery Operation Tab			

Continued on next page

Table 6.31 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Maximum Failover Count	Set as much as the number of the servers	1 time	This was also changed because the default value of Cluster Properties > Expand tab > Unit for Counting Failover Occurrences was changed.

Application monitor resource

Parameters	Default value before update	Default value after update	Remarks
Application Monitor Resource Properties			
Monitor (common) Tab			
• Wait Time to Start Monitoring	0 sec	3 sec	
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

Floating IP monitor resource

Parameters	Default value before update	Default value after update	Remarks
Floating IP Monitor Resource Properties			
Monitor (common) Tab			
• Timeout	60 sec	180 sec	

Continued on next page

Table 6.33 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

NIC Link Up/Down monitor resource

Parameters	Default value before update	Default value after update	Remarks
NIC Link Up/Down Monitor Resource Properties			
Monitor (common) Tab			
• Timeout	60 sec	180 sec	
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

Registry synchronous monitor resource

Parameters	Default value before update	Default value after update	Remarks
Registry Synchronization Monitor Resource Properties			
Monitor (common) Tab			

Continued on next page

Table 6.35 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

Service monitor resource

Parameters	Default value before update	Default value after update	Remarks
Service Monitor Resource Properties			
Monitor (common) Tab			
• Wait Time to Start Monitoring	0 sec	3 sec	
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

Print spooler monitor resource

Parameters	Default value before update	Default value after update	Remarks
Print Spooler Monitor Resource Properties			
Monitor (common) Tab			

Continued on next page

Table 6.37 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

Virtual computer name monitor resource

Parameters	Default value before update	Default value after update	Remarks
Virtual Computer Name Monitor Resource Properties			
Monitor (common) Tab			
• Timeout	60 sec	180 sec	
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

Virtual IP monitor resource

Parameters	Default value before update	Default value after update	Remarks
Virtual IP Monitor Resource Properties			
Monitor (common) Tab			
• Timeout	60 sec	180 sec	

Continued on next page

Table 6.39 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

Custom monitor resource

Parameters	Default value before update	Default value after update	Remarks
Custom Monitor Resource Properties			
Monitor (common) Tab			
• Wait Time to Start Monitoring	0 sec	3 sec	

Process name monitor resource

Parameters	Default value before update	Default value after update	Remarks
Process Name Monitor Properties			
Monitor (common) Tab			
• Wait Time to Start Monitoring	0 sec	3 sec	
• Do Not Retry at Timeout Occurrence	Off	On	

Continued on next page

Table 6.41 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

SQL Server monitor resource

Parameters	Default value before update	Default value after update	Remarks
SQL Server Monitor Resource Properties			
Monitor (special) Tab			
• ODBC Driver Name	SQL Native Client	ODBC Driver 13 for SQL Server	

Weblogic monitor resource

Parameters	Default value before update	Default value after update	Remarks
Weblogic Monitor Resource Properties			
Monitor (special) Tab			
• Install Path	`C:\bea\weblogic92`	`C:\Oracle\Middleware\Oracle_Home\wlserver`	

JVM monitor resource

Parameters	Default value before update	Default value after update	Remarks
JVM Monitor Resource Properties			
Monitor (common) Tab			
• Timeout	120 sec	180 sec	

Dynamic DNS monitor resource

Parameters	Default value before update	Default value after update	Remarks
Dynamic DNS Monitor Resource Properties			
Monitor (common) Tab			
• Timeout	120 sec	180 sec	
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

AWS Elastic IP monitor resource

Parameters	Default value before update	Default value after update	Remarks
AWS elastic ip Monitor Resource Properties			
Monitor (common) Tab			
• Timeout	100 sec	180 sec	
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

AWS Virtual IP monitor resource

Parameters	Default value before update	Default value after update	Remarks
AWS virtual ip Monitor Resource Properties			
Monitor (common) Tab			
• Timeout	100 sec	180 sec	
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

AWS AZ monitor resource

Parameters	Default value before update	Default value after update	Remarks
AWS AZ Monitor Resource Properties			
Monitor (common) Tab			
• Timeout	100 sec	180 sec	
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

Azure probe port monitor resource

Parameters	Default value before update	Default value after update	Remarks
Azure probe port Monitor Resource Properties			
Monitor (common) Tab			
• Timeout	100 sec	180 sec	
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

Azure load balance monitor resource

Parameters	Default value before update	Default value after update	Remarks
Azure load balance Monitor Resource Properties			
Monitor (common) Tab			
• Timeout	100 sec	180 sec	
• Do Not Retry at Timeout Occurrence	Off	On	
• Do not Execute Recovery Action at Timeout Occurrence	Off	On	

Internal Version 12.10

Script resource

Parameters	Default value before update	Default value after update	**Remarks**
Script Resource Properties			
Details Tab			
Script Resource Tuning Properties			
Parameter Tab			
• Allow to Interact with Desktop	On	Off	The settings cannot be changed for the internal version 12.00 or earlier. The settings can be changed for 12.10 or later.

Internal Version 12.20

Service resource

Parameters	Default value before update	Default value after update	Remarks
Service Resource Properties			
Recovery Operation Tab			
• Retry Count	0 times	1 time	

AWS Elastic IP monitor resource

Parameters	Default value before update	Default value after update	Remarks
AWS elastic ip Monitor Resource Properties			
Monitor(special) Tab			
• Action when AWS CLI command failed to receive response	Disable recovery action(Display warning)	Disable recovery action(Do nothing)	

AWS Virtual IP monitor resource

Parameters	Default value before update	Default value after update	Remarks
AWS virtual ip Monitor Resource Properties			
Monitor(special) Tab			
• Action when AWS CLI command failed to receive response	Disable recovery action(Display warning)	Disable recovery action(Do nothing)	

AWS AZ monitor resource

Parameters	Default value before update	Default value after update	Remarks
AWS AZ Monitor Resource Properties			
Monitor(special) Tab			
• Action when AWS CLI command failed to receive response	Disable recovery action(Display warning)	Disable recovery action(Do nothing)	

AWS DNS monitor resource

Parameters	Default value before update	Default value after update	Remarks
AWS DNS Monitor Resource Properties			
Monitor(special) Tab			
• Action when AWS CLI command failed to receive response	Disable recovery action(Display warning)	Disable recovery action(Do nothing)	

Internal Version 12.30

Cluster

Parameters	Default value before update	Default value after update	Remarks
Cluster Properties			
Extension Tab			
• Max Reboot Count	0 times	3 times	
• Max Reboot Count Reset Time	0 min	60 min	

Internal Version 13.00

Application resource

Parameters	Default value before update	Default value after update	Remarks
Application Resource Properties			
Dependency Tab			

Continued on next page

Table 6.58 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Follow the default dependence	On - CIFS resource - Disk resource - Floating ip resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	On - CIFS resource - Disk resource - Floating ip resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - AWS secondary IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	

Registry synchronization resource

Parameters	Default value before update	Default value after update	Remarks
Registry Synchronization Resource Properties			
Dependency Tab			

Continued on next page

Table 6.59 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Follow the default dependence	On - CIFS resource - Disk resource - Floating IPresource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	On - CIFS resource - Disk resource - Floating IPresource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - AWS secondary IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	

Script resource

Parameters	Default value before update	Default value after update	Remarks
Script Resource Properties			
Dependency Tab			

Continued on next page

Table 6.60 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Follow the default dependence	On - CIFS resource - Disk resource - Floating ip resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	On - CIFS resource - Disk resource - Floating ip resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - AWS secondary IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	

Service resource

Parameters	Default value before update	Default value after update	Remarks
Service Resource Properties			
Dependency Tab			

Continued on next page

Table 6.61 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Follow the default dependence	On - CIFS resource - Disk resource - Floating IP resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IPresource - AWS virtual IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	On - CIFS resource - Disk resource - Floating IP resource - Hybrid disk resource - Mirror disk resource - Print spooler resource - Registry synchronization resource - Virtual computer name resource - Virtual IP resource - AWS elastic IPresource - AWS virtual IP resource - AWS secondary IP resource - AWS DNS resource - Azure probe port resource - Azure DNS resource	

Virtual computer name resource

Parameters	Default value before update	Default value after update	Remarks
Virtual computer name resource Properties			
Dependency Tab			

Continued on next page

Table 6.62 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Follow the default dependence	On - Floating IP resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - Azure probe port resource	On - Floating IP resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - AWS secondary IP resource - Azure probe port resource	

CIFS resource

Parameters	Default value before update	Default value after update	Remarks
CIFS Resource Properties			
Details Tab			
• Errors in restoring file share setting are treated as activity failure	On	Off	

Dynamic DNS monitor resource

Parameters	Default value before update	Default value after update	Remarks
Dynamic DNS monitor resource Properties			
Dependency Tab			

Continued on next page

Table 6.64 – continued from previous page

Parameters	Default value before update	Default value after update	Remarks
• Follow the default dependence	On - Floating IP resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - Azure probe port resource	On - Floating IP resource - Virtual IP resource - AWS elastic IP resource - AWS virtual IP resource - AWS secondary IP resource - Azure probe port resource	

6.6.5 Moved Parameters

The following table shows the parameters which are configurable with Cluster WebUI but whose controls have been moved for each of the versions.

Internal Version 12.00

Parameter location Before the change	Parameter location After the change
[Cluster Properties]-[Recovery Tab]-[Max Reboot Count]	[Cluster Properties]-[Extension Tab]-[Max Reboot Count]
[Cluster Properties]-[Recovery Tab]-[Max Reboot Count Reset Time]	[Cluster Properties]-[Extension Tab]-[Max Reboot Count Reset Time]
[Cluster Properties]-[Recovery Tab]-[Use Forced Stop]	[Cluster Properties]-[Extension Tab]-[Use Forced Stop]
[Cluster Properties]-[Recovery Tab]-[Forced Stop Action]	[Cluster Properties]-[Extension Tab]-[Forced Stop Action]
[Cluster Properties]-[Recovery Tab]-[Forced Stop Timeout]	[Cluster Properties]-[Extension Tab]-[Forced Stop Timeout]
[Cluster Properties]-[Recovery Tab]-[Virtual Machine Forced Stop Setting]	[Cluster Properties]-[Extension Tab]-[Virtual Machine Forced Stop Setting]
[Cluster Properties]-[Recovery Tab]-[Execute Script for Forced Stop]	[Cluster Properties]-[Extension Tab]-[Execute Script for Forced Stop]
[Cluster Properties]-[Auto Recovery Tab]-[Auto Return]	[Cluster Properties]-[Extension Tab]-[Auto Return]
[Cluster Properties]-[Recovery Tab]-[Disable Recovery Action Caused by Monitor Resource Error]	[Cluster Properties]-[Extension Tab]-[Disable cluster operation]-[Recovery Action when Monitor Resource Failure Detected]
[Group Properties]-[Attribute Tab]-[Failover Exclusive Attribute]	[Group Common Properties]-[Exclusion Tab]

Internal Version 13.00

Parameter location Before the change	Parameter location After the change
[Cluster Properties]-[Extension Tab]-[Use Forced Stop]	[Cluster Properties]-[Fencing Tab]-[Forced Stop] - [Type]
[Cluster Properties]-[Extension Tab]-[Forced Stop Action]	[BMC Forced Stop Properties]-[Forced Stop Tab]-[Forced Stop Action]
[Cluster Properties]-[Extension Tab]-[Forced Stop Timeout]	[BMC Forced Stop Properties]-[Forced Stop Tab]-[Forced Stop Timeout]
[Cluster Properties]-[Extension Tab]-[Virtual Machine Forced Stop Setting] - [Action]	[vCenter Forced Stop Properties]-[Forced Stop Tab]-[Forced Stop Action]
[Cluster Properties]-[Extension Tab]-[Virtual Machine Forced Stop Setting] - [Timeout]	[vCenter Forced Stop Properties]-[Forced Stop Tab]-[Forced Stop Timeout]
[Cluster Properties]-[Extension Tab]-[Virtual Machine Forced Stop Setting] - [Host Name]	[vCenter Forced Stop Properties]-[vCenter Tab]-[Host Name]
[Cluster Properties]-[Extension Tab]-[Virtual Machine Forced Stop Setting] - [User Name]	[vCenter Forced Stop Properties]-[vCenter Tab]-[User Name]
[Cluster Properties]-[Extension Tab]-[Virtual Machine Forced Stop Setting] - [Password]	[vCenter Forced Stop Properties]-[vCenter Tab]-[Password]
[Cluster Properties]-[Extension Tab]-[Virtual Machine Forced Stop Setting] - [Perl Path]	[vCenter Forced Stop Properties]-[vCenter Tab]-[Perl Path]
[Server Properties]-[BMC Tab]-[IP Address]	[BMC Forced Stop Properties]-[Server List Tab]-[BMC Settings]-[IP Address]
[Server Properties]-[BMC Tab]-[User Name]	[BMC Forced Stop Properties]-[Server List Tab]-[BMC Settings]-[User Name]
[Server Properties]-[BMC Tab]-[Password]	[BMC Forced Stop Properties]-[Server List Tab]-[BMC Settings]-[Password]

6.7 Compatibility with old versions

6.7.1 Compatibility with EXPRESSCLUSTER X 1.0/2.0/2.1/3.0/3.1/3.2/3.3/4.0/4.1/4.2/4.3

The cluster configuration information created of X 1.0/2.0/2.1/3.0/3.1/3.2/3.3/4.0/4.1/4.2/4.3 can be used in X 5.0 or later. Since the type of failover destination server selection upon failure detection of group resource / monitor resource is the **stable server** which is the default, what is selected for failover destination in X 2.0 or later may differ from that of X 1.0 for the configuration of three nodes or more.

If the **stable server** is configured as failover destination and there are multiple failover destinations, a server with no error will be given a higher priority when a failover takes place. On the other hand, with X 1.0, since the server configured to have the highest priority among the movable servers is the failover destination, failback to the server where the error occurred in the first place takes place, which can result in failure to failing over to the third server.

For the reason described above, it is generally recommended to configure the **stable server** as failover destination . However if the same behavior as X 1.0 is required, change the failover destination select **Maximum Propriety Server** in the **Settings** tab of the properties in each resource.

6.7.2 Script files

When you port a script file used in EXPRESSCLUSTER Ver8.0 or earlier, change the first "ARMS_" of the environment variable name to "CLP_".

Example) IF "*%ARMS_EVENT%*" == "START" GOTO NORMAL

↓

IF "*%CLP_EVENT%*" == "START" GOTO NORMAL

CHAPTER

SEVEN

GLOSSARY

Active server

A server that is running for an application set.
(Related term: Standby server)

Cluster partition

A partition on a mirror disk. Used for managing mirror disks.
(Related term: Disk heartbeat partition)

Cluster shutdown To shut down an entire cluster system (all servers that configure a cluster system).

Cluster system Multiple computers are connected via a LAN (or other network) and behave as if it were a single system.

Data partition

A local disk that can be used as a shared disk for switchable partition. Data partition for mirror disks.
(Related term: Cluster partition)

Disk heartbeat partition A partition used for heartbeat communication in a shared disk type cluster.

Failover The process of a standby server taking over the group of resources that the active server previously was handling due to error detection.

Failback A process of returning an application back to an active server after an application fails over to another server.

Failover group A group of cluster resources and attributes required to execute an application.

Failover policy A priority list of servers that a group can fail over to.

Floating IP address

Clients can transparently switch one server from another when a failover occurs.
Any unassigned IP address that has the same network address that a cluster server belongs to can be used as a floating address.

Heartbeat

Signals that servers in a cluster send to each other to detect a failure in a cluster.
(Related terms: Interconnect, Network partition)

Interconnect

A dedicated communication path for server-to-server communication in a cluster.
(Related terms: Private LAN, Public LAN)

Management client Any machine that uses the Cluster WebUI to access and manage a cluster system.

Master server The server displayed at the top of Master Server in Server Common Properties of the Cluster WebUI.

Mirror connect LAN used for data mirroring in a data mirror type cluster. Mirror connect can be used with primary interconnect.

Mirror disk type cluster A cluster system that does not use a shared disk. Local disks of the servers are mirrored.

Moving failover group Moving an application from an active server to a standby server by a user.

Network partition

All heartbeat is lost and the network between servers is partitioned.
(Related terms: Interconnect, Heartbeat)

Node A server that is part of a cluster in a cluster system. In networking terminology, it refers to devices, including computers and routers, that can transmit, receive, or process signals.

Private LAN

LAN in which only servers configured in a clustered system are connected.
(Related terms: Interconnect, Public LAN)

Primary (server)

A server that is the main server for a failover group.
(Related term: Secondary server)

Public LAN

A communication channel between clients and servers.
(Related terms: Interconnect, Private LAN)

Startup attribute A failover group attribute that determines whether a failover group should be started up automatically or manually when a cluster is started.

Shared disk A disk that multiple servers can access.

Shared disk type cluster A cluster system that uses one or more shared disks.

Switchable partition

A disk partition connected to multiple computers and is switchable among computers.
(Related terms: Disk heartbeat partition)

Secondary server

A destination server where a failover group fails over to during normal operations.
(Related term: Primary server)

Server Group A group of servers connected to the same network or the shared disk device

Standby server

A server that is not an active server.
(Related term: Active server)

Virtual IP address IP address used to configure a remote cluster.

CHAPTER

EIGHT

LEGAL NOTICE

8.1 Disclaimer

- Information in this document is subject to change without notice. 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.
- Linux is a registered trademark of Linus Torvalds in the United States and other countries.
- Firefox is a trademark or registered trademark of Mozilla Foundation.
- Google Chrome is a trademark or registered trademark of Google, Inc.
- Google Cloud Platform (GCP) is a trademark or a registered trademark of Google LLC.
- 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.
- Apache Tomcat, Tomcat, and Apache are registered trademarks or trademarks of Apache Software Foundation.
- Python is a registered trademark of the Python Software Foundation.
- SVF is a registered trademark of WingArc Technologies, Inc.
- Oracle, Oracle Database, Solaris, MySQL, Tuxedo, WebLogic Server, Container, Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle Corporation and/or its affiliates.
- SAP, SAP NetWeaver, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries.
- IBM, DB2, and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.
- PostgreSQL is a registered trademark of the PostgreSQL Global Development Group.
- PowerGres is a registered trademark of SRA OSS, Inc.
- F5, F5 Networks, BIG-IP, and iControl are trademarks or registered trademarks of F5 Networks, Inc. in the United States and other countries.
- Equalizer is a registered trademark of Coyote Point Systems, Inc.
- WebOTX is a registered trademark of NEC Corporation.
- WebSAM is a registered trademark of NEC Corporation.
- 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, 2022	New manual
2nd	Apr 26, 2022	Corresponds to the internal version 13.01.
3rd	Jul 29, 2022	Updated Latest version information.
4th	Nov 04, 2022	Corresponds to the internal version 13.02.