



EXPRESSCLUSTER X 5.0
HA Cluster Configuration Guide for Microsoft Azure
(Windows)
Release 3

NEC Corporation

Feb 17, 2023

TABLE OF CONTENTS:

1	Preface	1
1.1	Who Should Use This Guide	1
1.2	Scope of application	2
1.3	How This Guide is Organized	3
1.4	EXPRESSCLUSTER X Documentation Set	4
1.5	Conventions	5
1.6	Contacting NEC	6
2	Overview	7
2.1	Functional overview	7
2.2	Basic configuration	9
2.3	Network partition resolution	16
2.4	Differences between on-premises and Microsoft Azure	18
3	Operating Environments	25
3.1	HA cluster using Azure DNS	25
3.2	HA cluster using a load balancer	27
4	Cluster Creation Procedure (for an HA Cluster Using Azure DNS)	29
4.1	Creation example	29
4.2	Configuring Microsoft Azure	34
4.3	Configuring the EXPRESSCLUSTER settings	58
4.4	Verifying the created environment	76
5	Cluster Creation Procedure (for an HA Cluster Using a Public Load Balancer)	77
5.1	Creation example	77
5.2	Configuring Microsoft Azure	82
5.3	Configuring the EXPRESSCLUSTER settings	113
5.4	Verifying the created environment	132
6	Cluster Creation Procedure (for an HA Cluster Using an Internal Load Balancer)	133
6.1	Creation example	133
6.2	Configuring Microsoft Azure	137
6.3	Configuring the EXPRESSCLUSTER settings	165
6.4	Verifying the created environment	173
7	Error Messages	175
8	Notes and Restrictions	177
8.1	HA cluster using Azure DNS	177
8.2	HA cluster using a load balancer	179

9	Legal Notice	181
9.1	Disclaimer	181
9.2	Trademark Information	182
10	Revision History	183

PREFACE

1.1 Who Should Use This Guide

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

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

1.2 Scope of application

This guide covers the following product versions.

- EXPRESSCLUSTER X 4.2 for Windows (Internal version: 12.20)
- Windows Server 2016 Datacenter
- Microsoft Azure portal: Environment as of December 19, 2019
- Azure CLI 2.0

If the product versions that you use differ from the above, some display and configuration contents may differ from those described in this guide.

The display and configuration contents may also change in the future. Therefore, for the latest information, see the website or manual of each product and service.

1.3 How This Guide is Organized

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

1.4 EXPRESSCLUSTER X Documentation Set

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

EXPRESSCLUSTER X Getting Started Guide

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

EXPRESSCLUSTER X Installation and Configuration Guide

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

EXPRESSCLUSTER X Reference Guide

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

EXPRESSCLUSTER X Maintenance Guide

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

1.5 Conventions

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

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

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

See also:

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

The following conventions are used in this guide.

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



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

1.6 Contacting NEC

For the latest product information, visit our website below:

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

OVERVIEW

2.1 Functional overview

This guide describes how to configure an HA cluster based on EXPRESSCLUSTER X (hereinafter referred to as "EXPRESSCLUSTER") using Azure Resource Manager on a Microsoft Azure cloud service.

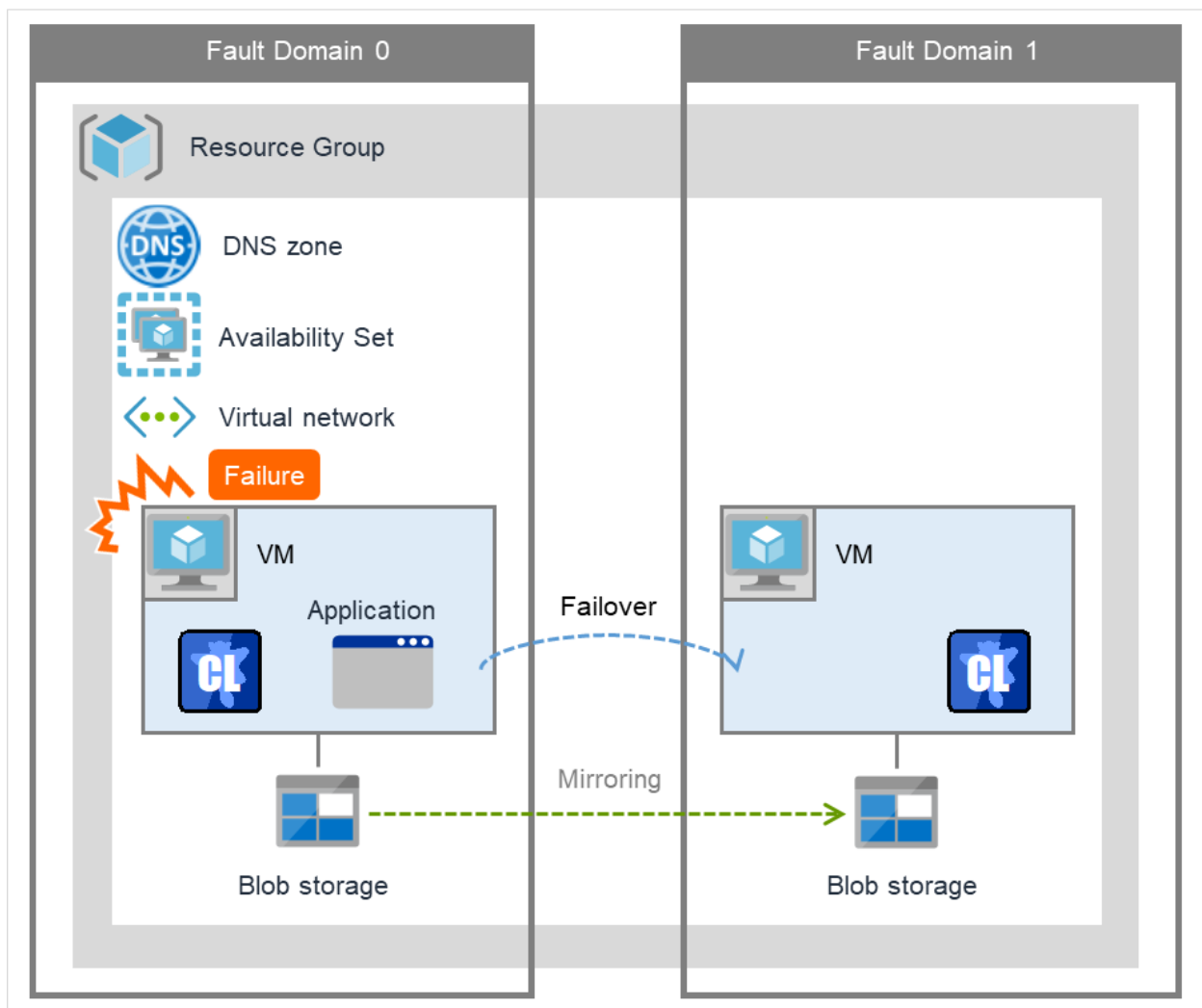


Fig. 2.1: HA Cluster on a Cloud Service (Using Azure DNS)

Operational availability can be increased by clustering virtual machines (VMs in [Figure 2.1 HA Cluster on a Cloud Service \(Using Azure DNS\)](#)) using a Microsoft Azure region and availability set in a Microsoft Azure environment.

- Microsoft Azure region

Physical and logical units called a Microsoft Azure region are provided.

It is possible to build all nodes in a single region (such as Japan East or Japan West). However, if all nodes are built in a single region, there is a possibility for nodes to go down due to a network failure or natural disaster, causing interruption to the flow of business. Distributing nodes into multiple regions can improve the operational availability.

- Availability set

Microsoft Azure allows each node to be deployed in a logical group called an *availability set*.

Locating each node in an availability set minimizes the impact of planned maintenance or unplanned maintenance due to a physical hardware failure of the Microsoft Azure platform. This guide describes the configuration using an availability set.

For details about an availability set, see the following website:

Manage the availability of Windows virtual machines in Azure:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/manage-availability>

2.2 Basic configuration

This guide assumes two types of HA clusters. One is an HA cluster using Azure DNS of the Resource Manager deployment model. The other is an HA cluster using a load balancer of the Resource Manager deployment model. (Both HA clusters are configured as a unidirectional standby cluster.) The following table describes the EXPRESSCLUSTER resources to be selected depending on the Microsoft Azure deployment model in use.

Purpose	EXPRESSCLUSTER resource to use
Accessing the cluster by using a DNS name (Use Azure DNS recordset)	Azure DNS resource
Accessing the cluster by using a virtual IP address(global IP address) (Use public load balancer)	Azure probe port resource
Accessing the cluster by using a virtual (private) IP address (Use internal load balancer)	Azure probe port resource

HA cluster using Azure DNS

In this configuration, two virtual machines are deployed the same resource group so that the cluster can be accessed by using the same DNS name. The EXPRESSCLUSTER Azure DNS resource uses Azure DNS to enable access with a DNS name. For details about Azure DNS, see the following website:

Azure DNS: <https://azure.microsoft.com/en-us/services/dns/>

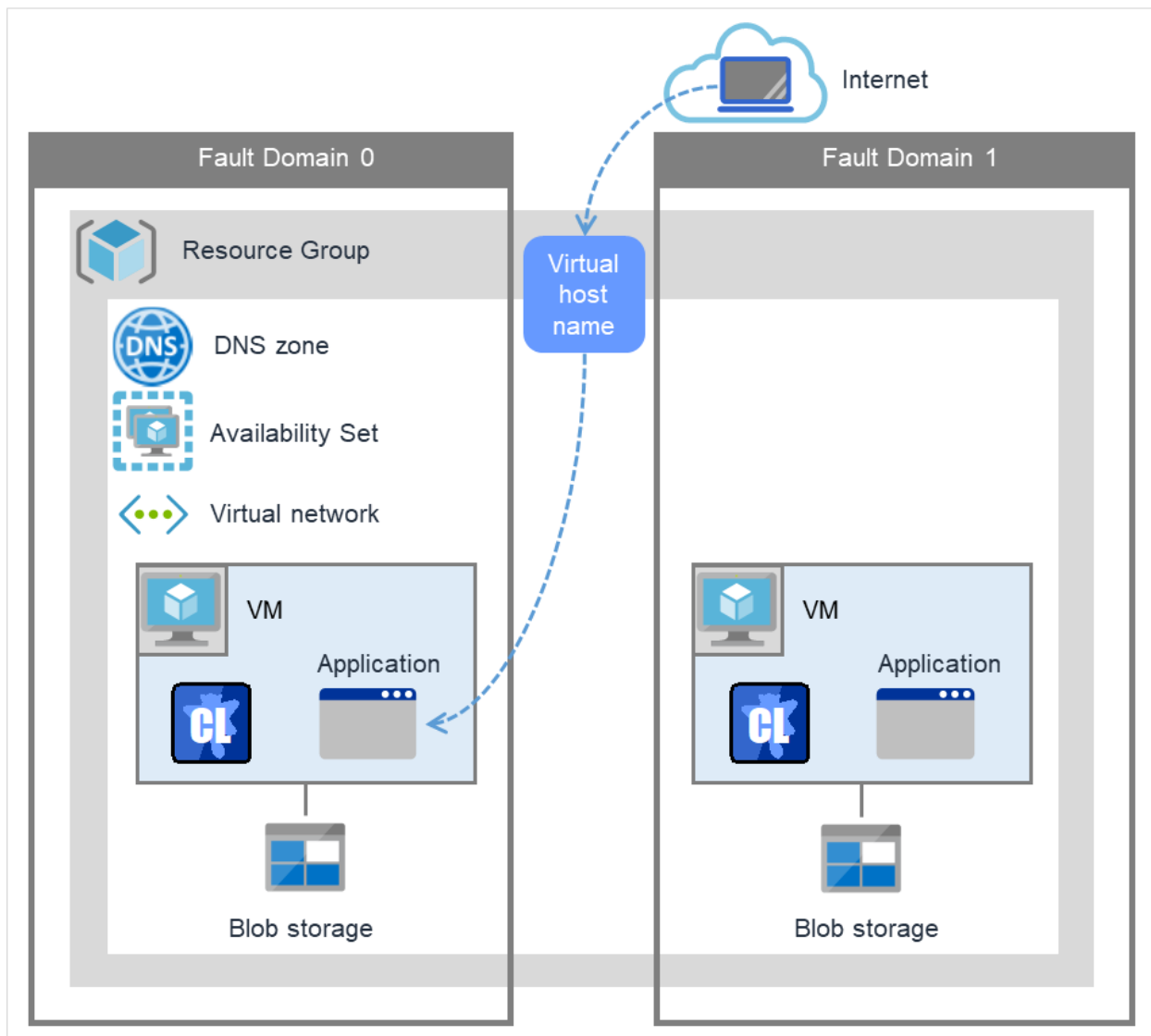


Fig. 2.2: HA Cluster Using Azure DNS

These two virtual machines use the same availability set to minimize the impact of planned maintenance or unplanned maintenance due to a physical hardware failure of the Microsoft Azure platform.

The cluster in [Figure 2.2 HA Cluster Using Azure DNS](#) is accessed by using the DNS name of the Azure DNS zone. EXPRESSCLUSTER manages record sets and DNS A records of the Azure DNS zone to find an IP address according to the DNS name. A client need not be conscious about the switching of virtual machines upon failover occurrence or group migration.

The following table describes the EXPRESSCLUSTER resources and monitor resources required for a HA cluster configuration using Azure DNS.

Resource or monitor resource type	Description	Setting
Azure DNS resource	Manages the record sets (A records) of the Azure DNS zone to find an IP address according to the DNS name.	Required
Azure DNS monitor resource	Monitors that the results of name resolution are normal in relation to the Azure DNS record set.	Required
IP monitor resource	Monitors whether communication with the Microsoft Azure Service Management API is possible, and also monitors health of communication with an external network.	When an public load balancer is used, required to monitor communication between clusters that are configured with virtual machines, and also to monitor health of communication with an internal network.
Custom monitor resource	Monitors communication between clusters that are configured with virtual machines, and also monitors health of communication with an internal network.	When an public load balancer is used, required to monitor whether communication with the Microsoft Azure Service Management API is possible, and also to monitor health of communication with an external network.
Multi target monitor resource	Monitors the statuses of both the IP monitor resource and custom monitor resource. If the statuses of both monitor resources are abnormal, a script in which a process for network partition resolution (NP resolution) is described is executed.	When an public load balancer is used, required to monitor health of communication between an internal network and external network.
Other resources and monitor resources	Depends on the configuration of application, such as a mirror disk, that is used in an HA cluster.	Optional

HA cluster using a load balancer

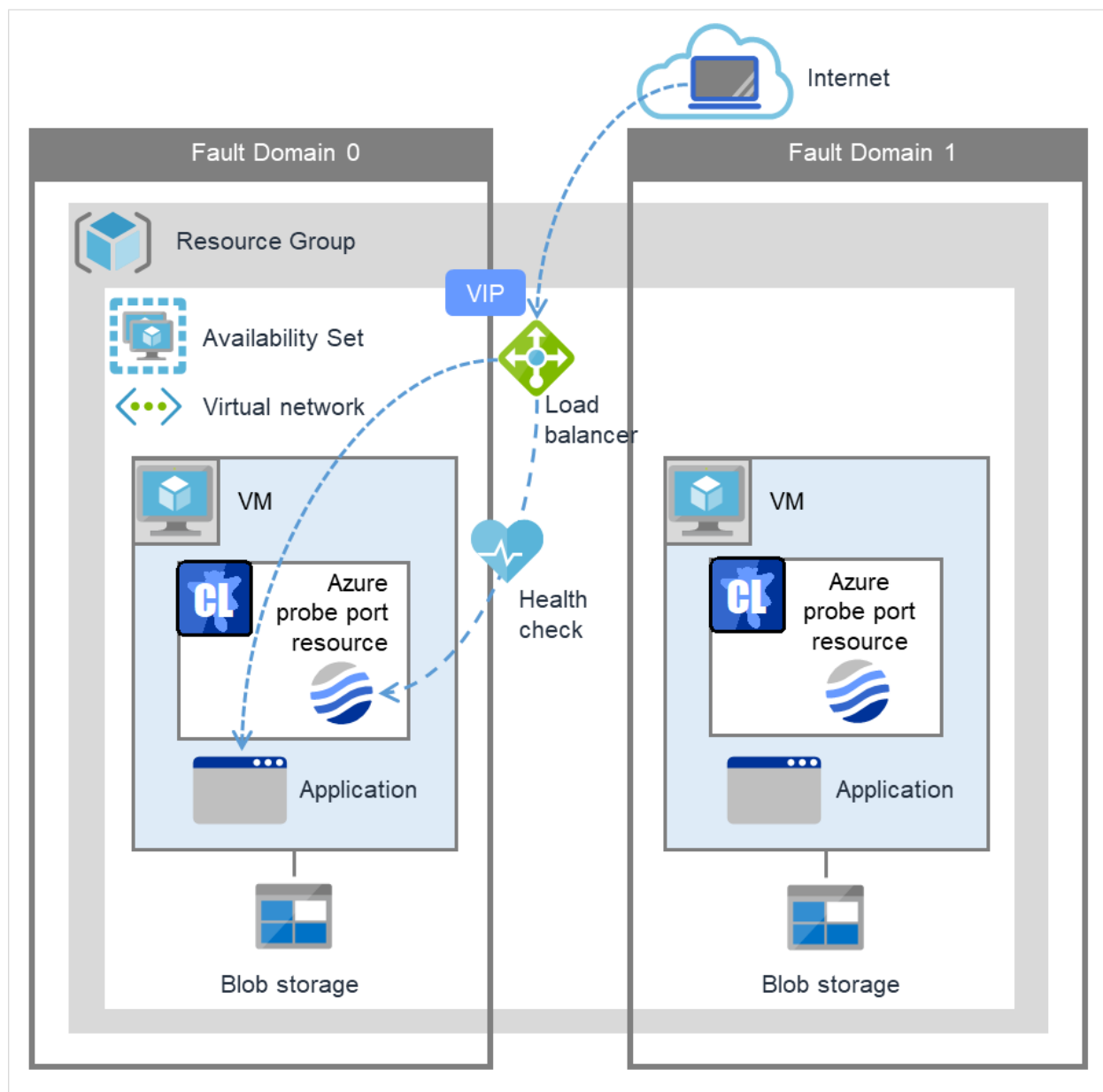


Fig. 2.3: HA Cluster Using an Public Load Balancer

A client application can connect a virtual machine on an availability set in a Microsoft Azure environment to a cluster node by using a frontend IP address. By using a VIP (Virtual IP), a client need not be conscious about the switching of virtual machines upon failover occurrence or group migration.

A cluster built in a Microsoft Azure environment in [Figure 2.3 HA Cluster Using an Public Load Balancer](#) is accessed by specifying a global IP address of the Microsoft Azure Load Balancer (Load Balancer in [Figure 2.3 HA Cluster Using an Public Load Balancer](#)).

Active and standby nodes of a cluster are switched by using probes of Microsoft Azure Load Balancer. To use Microsoft Azure Load Balancer probes, use a probe port provided by the EXPRESSCLUSTER Azure probe port resource.

Activating the Azure probe port resource starts a probe port control process in standby for alive monitoring (access to a probe port) from Microsoft Azure Load Balancer.

Deactivating the Azure probe port resource stops a probe port control process in standby for alive monitoring (access to a probe port) from Microsoft Azure Load Balancer.

The Azure probe port resource also supports the Microsoft Azure internal load balancer (Internal Load Balancing: ILB). For the internal load balancer, a Microsoft Azure private IP address is used as a VIP.

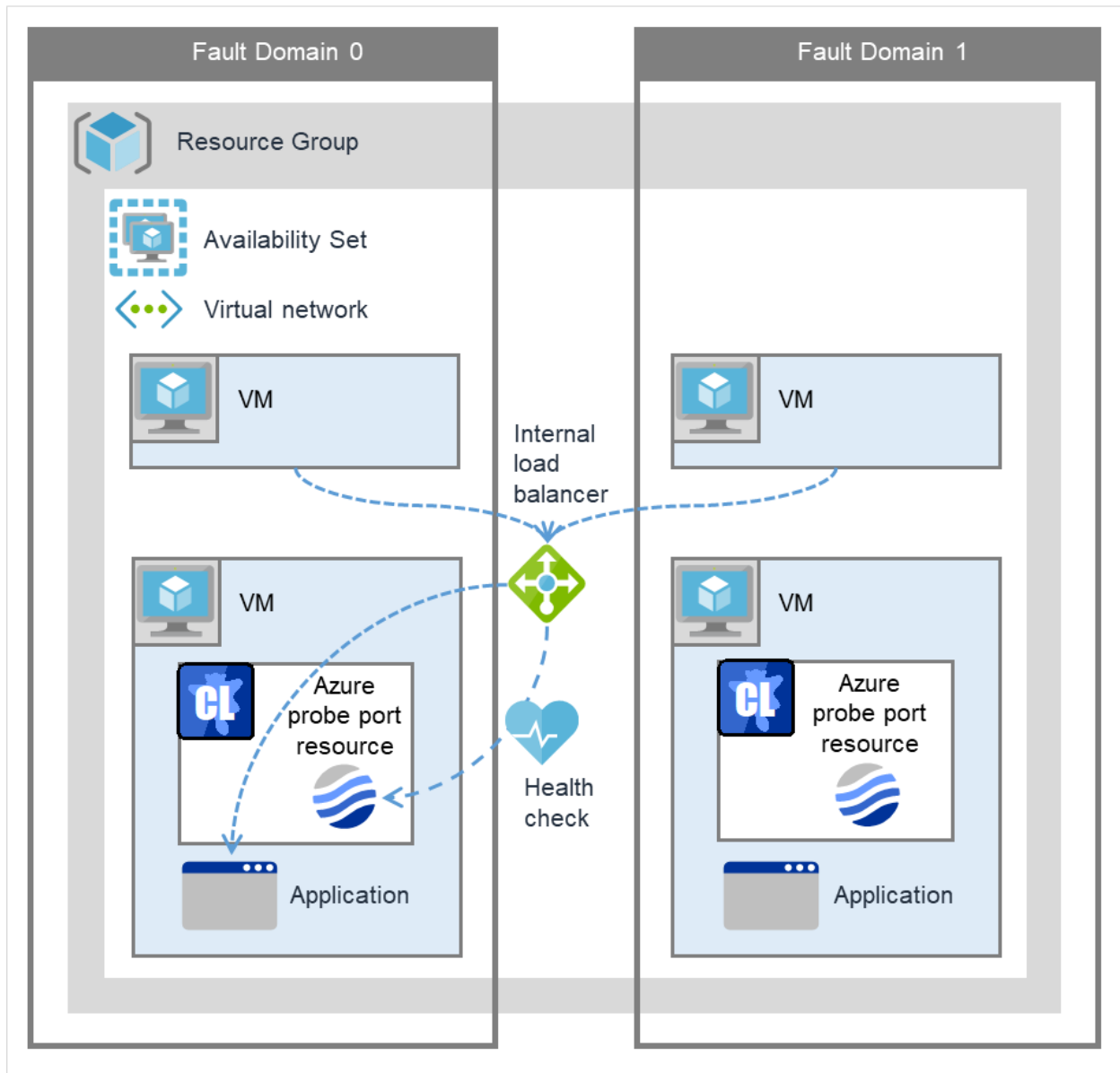


Fig. 2.4: HA Cluster Using the Internal Load Balancer

The following are examples of two HA cluster configurations using a load balancer. Select a load balancer to use depending on your purpose.

Purpose	Load balancer to use	Creating procedure
Disclosing operations outside the Microsoft Azure network	Public load balancer	See "5. Cluster Creation Procedure (for an HA Cluster Using a Public Load Balancer)" in this guide.
Publishing operations within the Microsoft Azure network	Internal load balancer (ILB)	See "6. Cluster Creation Procedure (for an HA Cluster Using an Internal Load Balancer)" in this guide.

The following table describes the EXPRESSCLUSTER resources and monitor resources required for a HA cluster using a load balancer.

Resource or monitor resource type	Description	Setting
Azure probe port resource	Provides a mechanism to wait for alive monitoring from a load balancer on a specific port of a node in which operations are running.	Required
Azure probe port monitor resource	Performs alive monitoring of a probe port control process, which starts upon activation of the Azure probe port resource, for a node in which the Azure probe port resource is running.	Required
Azure load balance monitor resource	Monitors whether a port with the same number as a probe port is open for a node in which the Azure probe port resource is not running.	Required
IP monitor resource	Monitors whether communication with the Microsoft Azure Service Management API is possible, and also monitors health of communication with an external network.	When an public load balancer is used, required to monitor communication between clusters that are configured with virtual machines, and also to monitor health of communication with an external network.
Custom monitor resource	Monitors communication between clusters that are configured with virtual machines, and also monitors health of communication with an internal network.	When an public load balancer is used, required to monitor whether communication with the Microsoft Azure Service Management API is possible, and also to monitor health of communication with an external network.

Continued on next page

Table 2.4 – continued from previous page

Resource or monitor resource type	Description	Setting
Multi target monitor resource	Monitors the statuses of both the IP monitor resource and custom monitor resource. If the statuses of both monitor resources are abnormal, a script in which a process for network partition resolution (NP resolution) is described is executed.	When an public load balancer is used, required to monitor health of communication between an internal network and external network.
PING network partition resolution resource	When an internal load balancer (ILB) is used, monitors health of communication between subnets by checking whether to communicate with a device that is always on and can return a response to ping (ping device).	When an internal load balancer (ILB) is used, required to monitor health of communication between subnets.
Other resources and monitor resources	Depends on the configuration of application, such as a mirror disk, that is used in an HA cluster.	Optional

2.3 Network partition resolution

Virtual machines configuring an HA cluster mutually performs alive monitoring through a heartbeat communication. If the virtual machines exist in different subnets, an undesirable event, such as an application starting more than once, occurs if a heartbeat ceases. To prevent a service from starting more than once, it is necessary to identify whether other virtual machines went down or whether the applicable virtual machine was isolated from a network (network partitioning: NP).

The network partition resolution feature (NP resolution) sends ping to or checks a LISTEN port of a device that is always on and can return a response to ping etc. (access destination). If there is no reply, this feature judges that the device entered the NP status and executes the specified action (such as a warning, recovery action, and server shutdown).

The access destination used on Microsoft Azure described in the following table.

(*) A private IP address of an internal load balancer (ILB) cannot be used because it does not reply to ping.

Scope of disclosure	access destination	Procedure	EXPRESSCLUSTER resources, monitor resources, and commands to be used for NP resolution
Outside the Microsoft Azure Virtual network	Microsoft Azure Service Management API (management.core.windows.net)	Checking a LISTEN port	- Custom monitor resource - clpazure_port_checker command
	each cluster server	Ping	IP monitor resource
Inside the Microsoft Azure Virtual network	Servers, excluding a cluster server, that exist within the Microsoft Azure network(*)	Ping	PING network partition resolution resource
	Web servers that exist within the Microsoft Azure network	HTTP	HTTP network partition resolution resource

For details about NP resolution, see the following:

- "Details on network partition resolution resources" in the Reference Guide.

Setting the NP resolution destination

You need to examine the NP resolution destination and method depending on the location of clients accessing a cluster system and the condition for connecting to an on-premise environment (for example, using a dedicated line). There is no NP resolution destination nor method to recommend.

How to judge the network partition status

EXPRESSCLUSTER provides the clpazure_port_checker command to check the TCP port listening status. Use this command as **Script created with this product** of the custom monitor resource or multi target monitor resource.

For details about the `clpazure_port_checker` command, see the following subsections.

Checking the TCP port listening status (`clpazure_port_checker` command)

`clpazure_port_checker`

Checks whether a LISTEN port exists among TCP ports of the specified server.

Command line `clpazure_port_checker -h hostname -p port`

Description

This command checks whether a LISTEN port exists among TCP ports of the server specified for an argument.

If there is no response five seconds (fixed) after the command execution, it is judged that an error (timeout) has occurred.

In case of an error, an error message is output to the standard output.

Executing this command from the custom monitor resource makes it possible to judge the network partition status.

For the configuration example of network partition resolution using this command, see "[4.3. Configuring the EXPRESSCLUSTER settings](#)" and "[6.3. Configuring the EXPRESSCLUSTER settings](#)"

Options

-h *hostname* Specify the determining server as *hostname* (by using an FQDN name or IP address). This option cannot be omitted.

-p *port* Specify the determining *port number* as *port* (by using a *port number* or *service name*). This option cannot be omitted.

Return values

- 0** Normal
- 1** Error (communication error)
- 2** Error (timeout)
- 3** Error (invalid argument or internal error)

2.4 Differences between on-premises and Microsoft Azure

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

Function	On-premise	Microsoft Azure Resource Manager deployment model
Creating a shared disk type cluster	✓	✓
Creating a mirror disk type cluster	✓	✓
Creating a hybrid disk type cluster	✓	✓
Using the floating IP resource	✓	n/a
Using the virtual IP resource	✓	n/a
Using the Azure probe port resource	n/a	✓
Using the Azure DNS resource	n/a	✓

For the procedure to create a 2-node cluster using a mirror disk on an on-premise or Microsoft Azure environment, see the following subsections.

The difference of the procedure to create a cluster between an on-premise environment and Microsoft Azure environment is whether or not configuring the Microsoft Azure settings in advance is required.

HA cluster using Azure DNS

For Microsoft Azure, execute steps 1 to 6 in the following table after logging in to the Microsoft Azure portal (<https://portal.azure.com/>).

For Microsoft Azure, execute steps 7 to 17 after logging in to each virtual machine.

- Before installing EXPRESSCLUSTER

Step No.	Procedure	On-premise	Microsoft Azure
1	Creating a resource group	Not required	See "4.2. <i>Configuring Microsoft Azure</i> " in this guide.
2	Creating a virtual network	Not required	See "4.2. <i>Configuring Microsoft Azure</i> " in this guide.
3	Creating a virtual machine	Not required	See "4.2. <i>Configuring Microsoft Azure</i> " in this guide.
4	Setting a private IP address	Not required	See "4.2. <i>Configuring Microsoft Azure</i> " in this guide.
5	Adding a disk	Not required	See "4.2. <i>Configuring Microsoft Azure</i> " in this guide.
6	Creating a DNS zone	Not required	See "4.2. <i>Configuring Microsoft Azure</i> " in this guide.
7	Setting up the DNS server	See the manual provided with the OS or DNS server.	Not required

Continued on next page

Table 2.7 – continued from previous page

Step No.	Procedure	On-premise	Microsoft Azure
8	Setting a partition for the mirror disk resource	See the following: - "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide. - "Understanding mirror disk resources" in the Reference Guide.	See "4.2. <i>Configuring Microsoft Azure</i> " in this guide.
9	Adjusting the OS startup time	See "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.	Same as "On-premise"
10	Checking the network setting	See "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.	Same as "On-premise"
11	Checking the firewall setting	See "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.	Same as "On-premise"
12	Synchronizing the server time	See "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.	Same as "On-premise"
13	Disabling the power saving function	See "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.	Same as "On-premise"
14	Installing the Azure CLI	Not required	See "4.2. <i>Configuring Microsoft Azure</i> " in this guide.
15	Registering the service principal	Not required	See "4.2. <i>Configuring Microsoft Azure</i> " in this guide.

Continued on next page

Table 2.7 – continued from previous page

Step No.	Procedure	On-premise	Microsoft Azure
16	Installing EXPRESS-CLUSTER	See "Installing EXPRESSCLUSTER" in the Installation and Configuration Guide.	Same as "On-premise"

- After installing EXPRESSCLUSTER

Step No.	Procedure	On-premise	Microsoft Azure
17	Registering the EXPRESSCLUSTER license	See "Registering the license." in the Installation and Configuration Guide.	Same as "On-premise"
18	Creating a cluster: Setting the heartbeat method	See "Creating the configuration data of a node cluster" in "Creating the cluster configuration data" in the Installation and Configuration Guide.	The COM heartbeat, BMC heartbeat, and disk heartbeat cannot be used.
19	Creating a cluster: Setting the NP resolution processing	The network partition resolution resource is used. See the following: - "Creating the configuration data of a node cluster" in "Creating the cluster configuration data".in the Installation and Configuration Guide. - "Network partition resolution resources details" in the Reference Guide.	See "6.3. <i>Configuring the EXPRESSCLUSTER settings</i> " in this guide.
20	Creating a cluster: Creating a failover group and monitor resource	See "Creating the configuration data of a node cluster" in "Creating the cluster configuration data".in the Installation and Configuration Guide.	In addition to the references for on-premises, see the following: - "Understanding Azure DNS resources" in the Reference Guide. - "Understanding Azure DNS monitor resources" in the Reference Guide. - "4.3. <i>Configuring the EXPRESSCLUSTER settings</i> " in this guide.

HA cluster using a load balancer

For Microsoft Azure, execute steps 1 to 5, and 7 to 8 in the following table after logging in to the Microsoft Azure portal (<https://portal.azure.com/>).

For Microsoft Azure, execute steps 6, and 9 to 15 after logging in to each virtual machine.

- Before installing EXPRESSCLUSTER

Step No.	Procedure	On-premise	Microsoft Azure
1	Creating a resource group	Not required	See either of the following depending on the load balancer to use: - "5.2. <i>Configuring Microsoft Azure</i> " in this guide - "6.2. <i>Configuring Microsoft Azure</i> " in this guide
2	Creating a virtual network	Not required	See either of the following depending on the load balancer to use: - "5.2. <i>Configuring Microsoft Azure</i> " in this guide - "6.2. <i>Configuring Microsoft Azure</i> " in this guide
3	Creating a virtual machine	Not required	See either of the following depending on the load balancer to use: - "5.2. <i>Configuring Microsoft Azure</i> " in this guide - "6.2. <i>Configuring Microsoft Azure</i> " in this guide

Continued on next page

Table 2.9 – continued from previous page

Step No.	Procedure	On-premise	Microsoft Azure
4	Setting a private IP address	Not required	See either of the following depending on the load balancer to use: - "5.2. <i>Configuring Microsoft Azure</i> " in this guide - "6.2. <i>Configuring Microsoft Azure</i> " in this guide
5	Adding a disk	Not required	See either of the following depending on the load balancer to use: - "5.2. <i>Configuring Microsoft Azure</i> " in this guide - "6.2. <i>Configuring Microsoft Azure</i> " in this guide
6	Setting a partition for the mirror disk resource	See the following: - "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide - "Understanding mirror disk resources" in the Reference Guide.	See either of the following depending on the load balancer to use: - "5.2. <i>Configuring Microsoft Azure</i> " in this guide - "6.2. <i>Configuring Microsoft Azure</i> " in this guide
7	Creating and configuring a load balancer	Not required	See either of the following depending on the load balancer to use: - "5.2. <i>Configuring Microsoft Azure</i> " in this guide - "6.2. <i>Configuring Microsoft Azure</i> " in this guide
8	Setting the inbound security rules	Not required	- "5.2. <i>Configuring Microsoft Azure</i> " in this guide

Continued on next page

Table 2.9 – continued from previous page

Step No.	Procedure	On-premise	Microsoft Azure
9	Adjusting the OS startup time	See "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.	Same as "On-premise"
10	Checking the network setting	See "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.	Same as "On-premise"
11	Checking the firewall setting	See "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.	Same as "On-premise"
12	Synchronizing the server time	See "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.	Same as "On-premise"
13	Disabling the power saving function	See "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.	Same as "On-premise"
14	Installing EXPRESS-CLUSTER	See "Installing EXPRESSCLUSTER" in the Installation and Configuration Guide.	Same as "On-premise"

- After installing EXPRESSCLUSTER

Step No.	Procedure	On-premise	Microsoft Azure
15	Registering the EXPRESSCLUSTER license	See "Registering the license" in the Installation and Configuration Guide.	Same as "On-premise"
16	Creating a cluster: Setting the heartbeat method	See "Creating the configuration data of a node cluster" in "Creating the cluster configuration data" in the Installation and Configuration Guide.	The COM heartbeat, BMC heartbeat, and DISK heartbeat cannot be used.

Continued on next page

Table 2.10 – continued from previous page

Step No.	Procedure	On-premise	Microsoft Azure
17	Creating a cluster: Setting the NP resolution processing	The network partition resolution resource is used. See the following: - "Creating the configuration data of a node cluster" in "Creating the cluster configuration data". in the Installation and Configuration Guide - "Network partition resolution resources details" in the Reference Guide.	See either of the following depending on the load balancer to use: - See "5.3. <i>Configuring the EXPRESSCLUSTER settings</i> " in this guide. - See "6.3. <i>Configuring the EXPRESSCLUSTER settings</i> " in this guide.
18	Creating a cluster: Creating a failover group and monitor resource	See "Creating the configuration data of a node cluster" in "Creating the cluster configuration data" in the Installation and Configuration Guide.	See the following in addition to the description of "On-premise." - "Understanding Azure probe port resources" in the Reference Guide. - "Understanding Azure load balance monitor resources" in the Reference Guide. - "Understanding Azure load balance monitor resources" in the Reference Guide. See either of the following depending on the load balancer to use: - See "5.3. <i>Configuring the EXPRESSCLUSTER settings</i> " in this guide. - See "6.3. <i>Configuring the EXPRESSCLUSTER settings</i> " in this guide.

OPERATING ENVIRONMENTS

3.1 HA cluster using Azure DNS

Supports the OS versions listed in the following manuals:

- "Getting Started Guide" > "Installation requirements for EXPRESSCLUSTER" > "Operation environment for Azure DNS resource and Azure DNS monitor resource"

Its operation has been verified in the following environments.

If the OS version is supported by Azure in EXPRESSCLUSTER X 4.2, you can use it by the same procedure.

If the procedure differs depending on the OS version, replace it.

x86_64

OS	Windows Server 2016 DataCenter
EXPRESSCLUSTER	EXPRESSCLUSTER X 4.2 for Windows(Internal version: 12.20)
Microsoft Azure deployment model	Resource Manager
Region (otherwise region or location according to parameter)	(Asia Pacific) Japan East
Mirror disk size	Disk size: 20 GB (1 GB for a cluster partition and 19 GB for a data partition)
Azure CLI	2

The Azure CLI and Python must be installed because Azure DNS resource use them.

Python is installed together with the Azure CLI 2.0.

For details about the Azure CLI, see the following website:

Get started with Azure CLI:

<https://docs.microsoft.com/en-us/cli/azure/get-started-with-azure-cli?view=azure-cli-latest>

Azure DNS must be installed because Azure DNS resource use it. For details about Azure DNS, see the following website:

Azure DNS: <https://azure.microsoft.com/en-us/services/dns/>

3.2 HA cluster using a load balancer

Supports the OS versions listed in the following manuals:

- "Operation environment for Azure probe port resource, Azure probe port monitor resource and Azure load balance monitor resource" in "Installation requirements for EXPRESSCLUSTER" in the Getting Started Guide.

Its operation has been verified in the following environments.

If the OS version is supported by Azure in EXPRESSCLUSTER X 4.2, you can use it by the same procedure.

If the procedure differs depending on the OS version, replace it.

x86_64

OS	Windows Server 2016 DataCenter
EXPRESSCLUSTER	EXPRESSCLUSTER X 4.2 for Windows(Internal version: 12.20)
Microsoft Azure deployment model	Resource Manager
Region (otherwise region or location according to parameter)	(Asia Pacific) Japan East
Mirror disk size	Disk size: 20 GB (1 GB for a cluster partition and 19 GB for a data partition)

CLUSTER CREATION PROCEDURE (FOR AN HA CLUSTER USING AZURE DNS)

4.1 Creation example

This guide introduces the procedure for creating a 2-node unidirectional standby cluster using EXPRESSCLUSTER. This procedure is intended to create a mirror disk type configuration in which node-1 is used as an active server.

The following tables describe the parameters that do not have a default value and the parameters whose values are to be changed from the default values.

- Microsoft Azure settings (common to node-1 and node-2)

Setting item	Setting value
Resource group setting	
– Resource group	TestGroup1
– Region	(Asia Pacific) Japan East
Virtual network setting	
– Name	Vnet1
– Address space	10.5.0.0/24
– Subnet Name	Vnet1-1
– Subnet Address range	10.5.0.0/24
– Resource group	TestGroup1
– Location	(Asia Pacific) Japan East
DNS zone setting	
– Name	cluster1.zone
– Resource group	TestGroup1
– Resource group location	(Asia Pacific) Japan East
– Record set	test-record1

- Microsoft Azure settings (specific to each of node-1 and node-2)

Setting item	Setting value	
	node-1	node-2
Virtual machine setting		
– Disk type	Standard HDD	
– User name	testlogin	
– Password	PassWord_123	
– Resource group	TestGroup1	
– Region	(Asia Pacific) Japan East	
Network security group setting		
Name	node-1-nsg	node-2-nsg
Availability set setting		
– Name	AvailabilitySet-1	
– Update domains	5	
– Fault domains	2	
Diagnostics storage account setting		
– Name	Automatically generated	
– Performance	Standard	
– Replication	Locally-redundant storage (LRS)	
IP configuration setting		
– IP address	10.5.0.120	10.5.0.121
Disk setting		
– Name	node-1_DataDisk_0	node-2_DataDisk_0
– Source type	None (empty disk)	
– Account type	Standard HDD	
– Size	20	

- EXPRESSCLUSTER settings (cluster properties)

Setting item	Setting value	
	node-1	node-2
– Cluster Name	Cluster1	
– Server Name	node-1	node-2
– Timeout Tab: Heartbeat Timeout	210	

- EXPRESSCLUSTER settings (failover group)

Resource name	Setting item	Setting value
Mirror disk resource	Name	md
	Details Tab: Data Partition Drive Letter	G:
	Details Tab: Cluster Partition Drive Letter	F:
Azure DNS resource	Name	azuredns1
	Record Set Name	test-record1
	Zone Name	cluster1.zone
	IP Address	(node-1) 10.5.0.120 (node-2) 10.5.0.121
	Resource Group Name	TestGroup1
	User URI	http://azure-test
	Tenant ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
	File Path of Service Principal	C:\Users\testlogin\ examplecert.pem
	Azure CLI File path	C:\Program Files(x86)\ Microsoft SDKs\Azure\ CLI2\wbin\az.cmd

- EXPRESSCLUSTER settings (monitor resource)

Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	Name	mdw1
Azure DNS monitor resource	Name	azurednsw1
Custom monitor resource	Name	genw1
	Script created with this product	On
	Monitor Type	Synchronous
	Normal Return Value	0
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
IP monitor resource	Name	ipw1
	Server to monitor	node-1

Continued on next page

Table 4.2 – continued from previous page

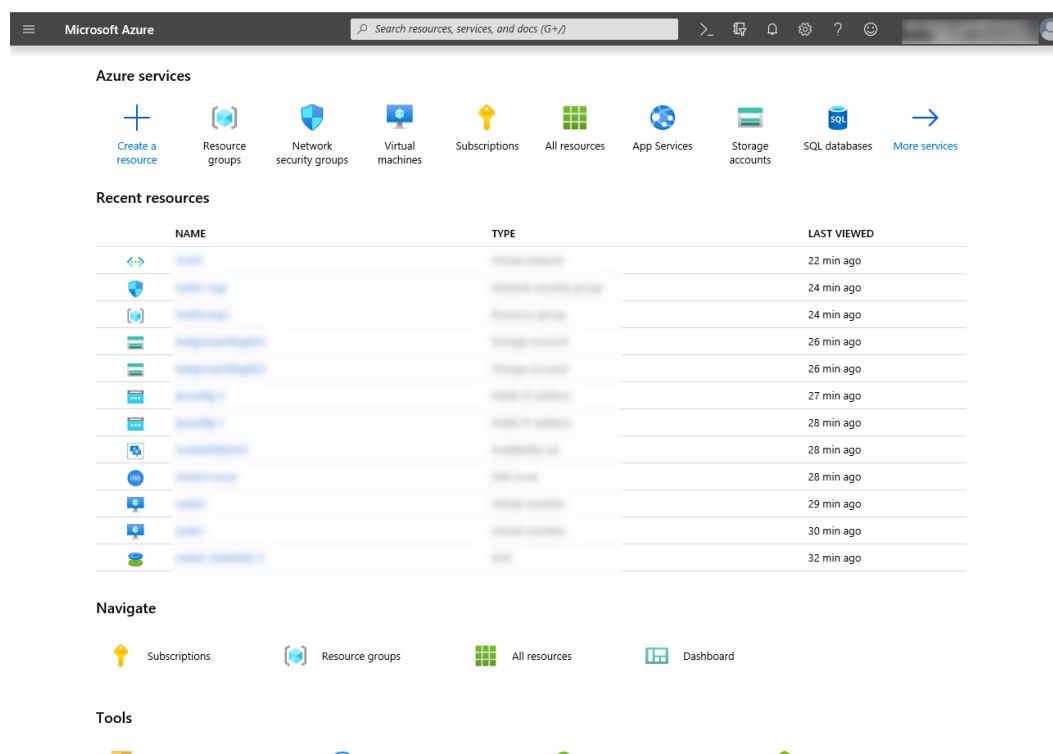
Monitor resource name	Setting item	Setting value
	IP address	10.5.0.121
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
IP monitor resource	Name	ipw2
	Server to monitor	node-2
	IP address	10.5.0.120
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
Multi target monitor resource	Name	mtw1
	Monitor resource list	genw1 ipw1 ipw2
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer

4.2 Configuring Microsoft Azure

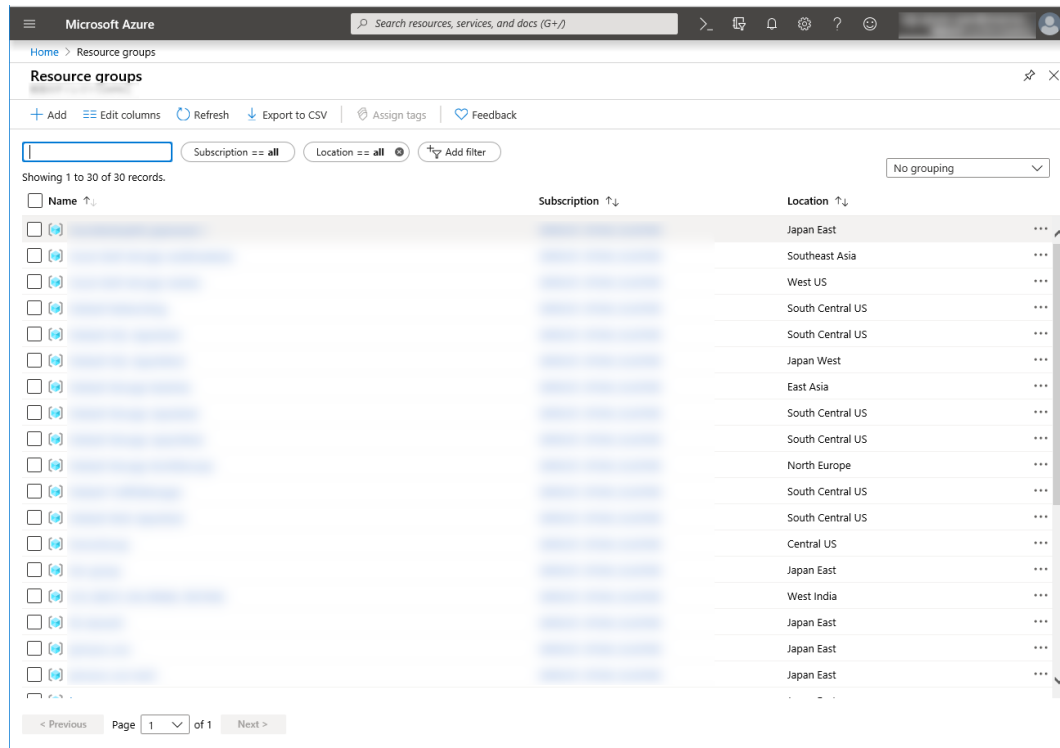
1) Creating a resource group

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create a resource group following the steps below.

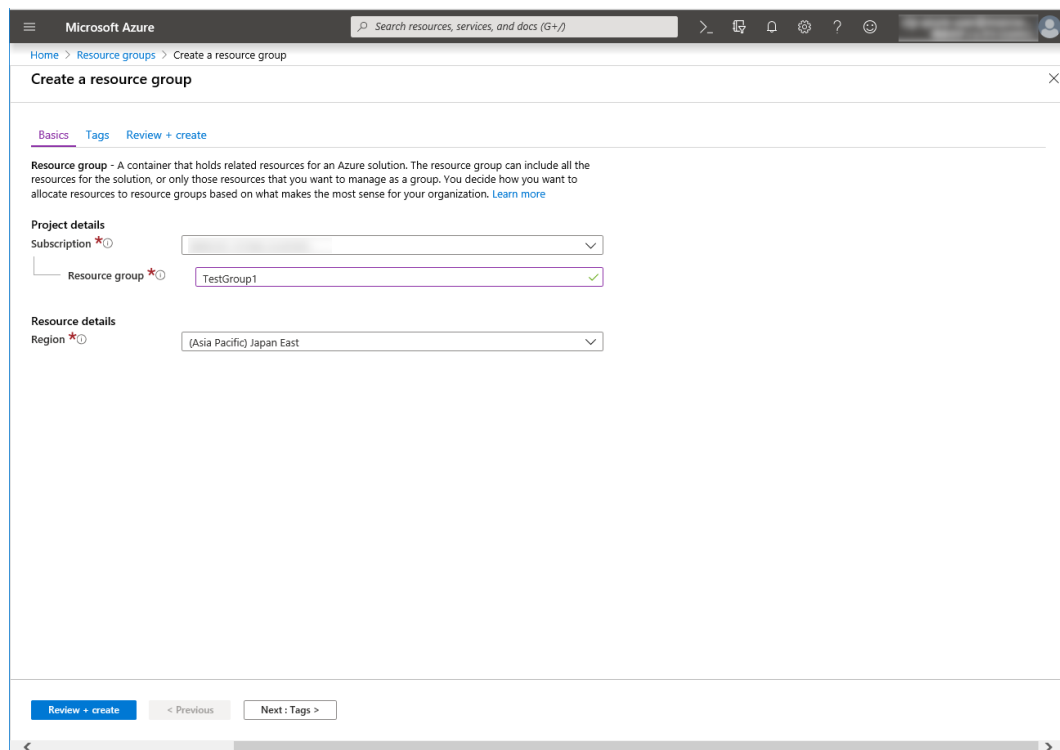
1. Select **Resource groups** on the upper part of the window. If there are existing resource groups, they are displayed in a list.



2. Select **+Add** on the upper part of the window.



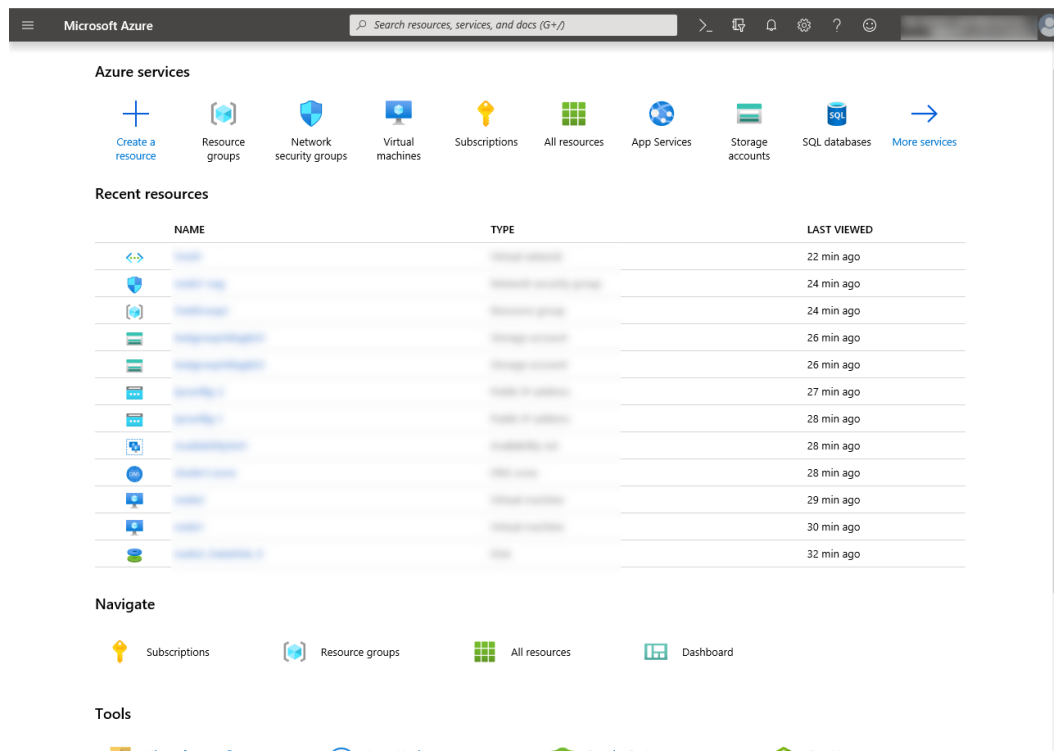
3. Specify **Subscription**, **Resource group**, and **Region**, and click **Review+Create**.



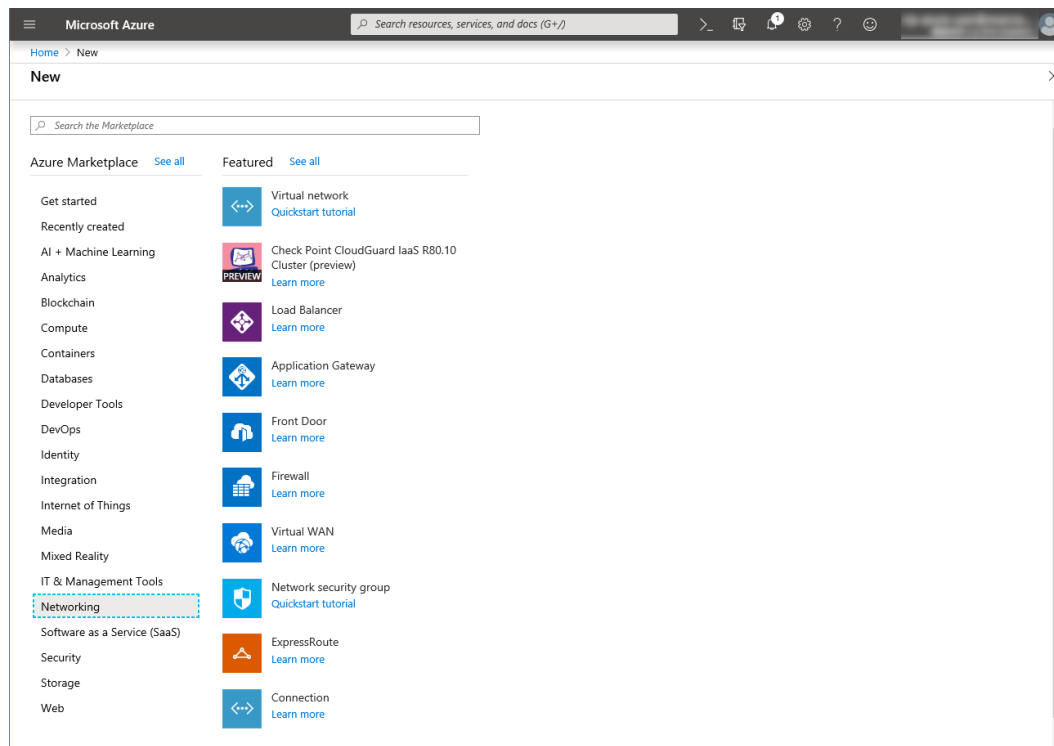
2) Creating a virtual network

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create a virtual network following the steps below.

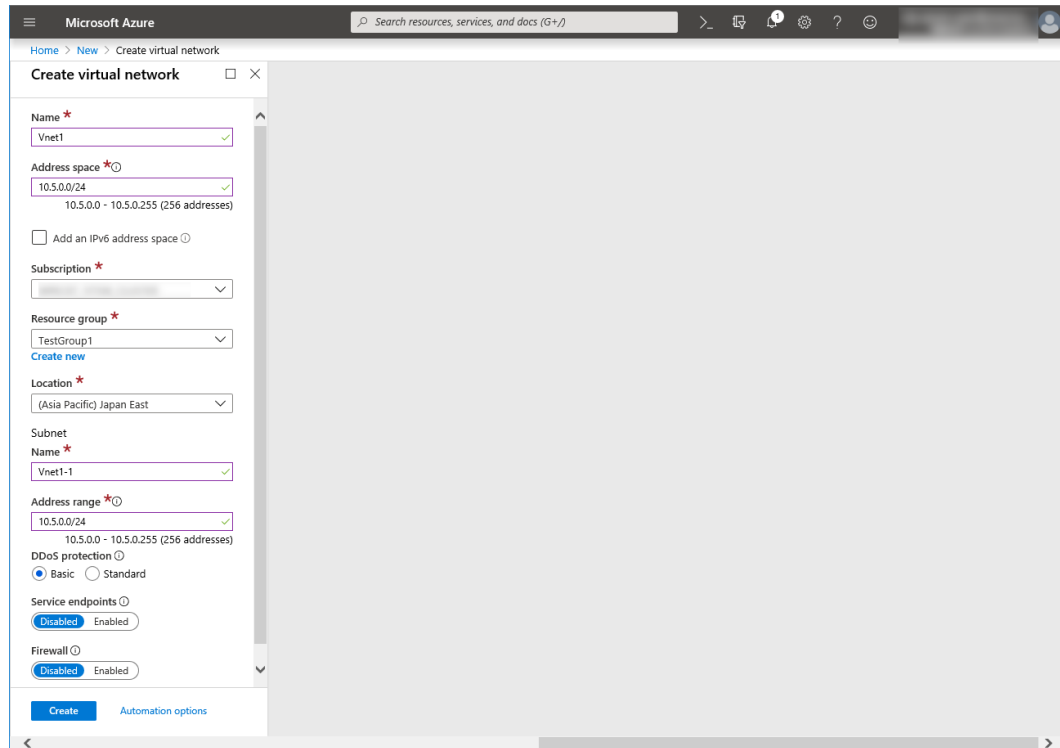
1. Select **Create a resource** on the upper part of the window.



2. Select **Networking** and then **Virtual network**.



3. Specify **Name**, **Address space**, **Subscription**, **Resource group**, **Location**, **Name of Subnet**, and **Address range**, and click **Create**.

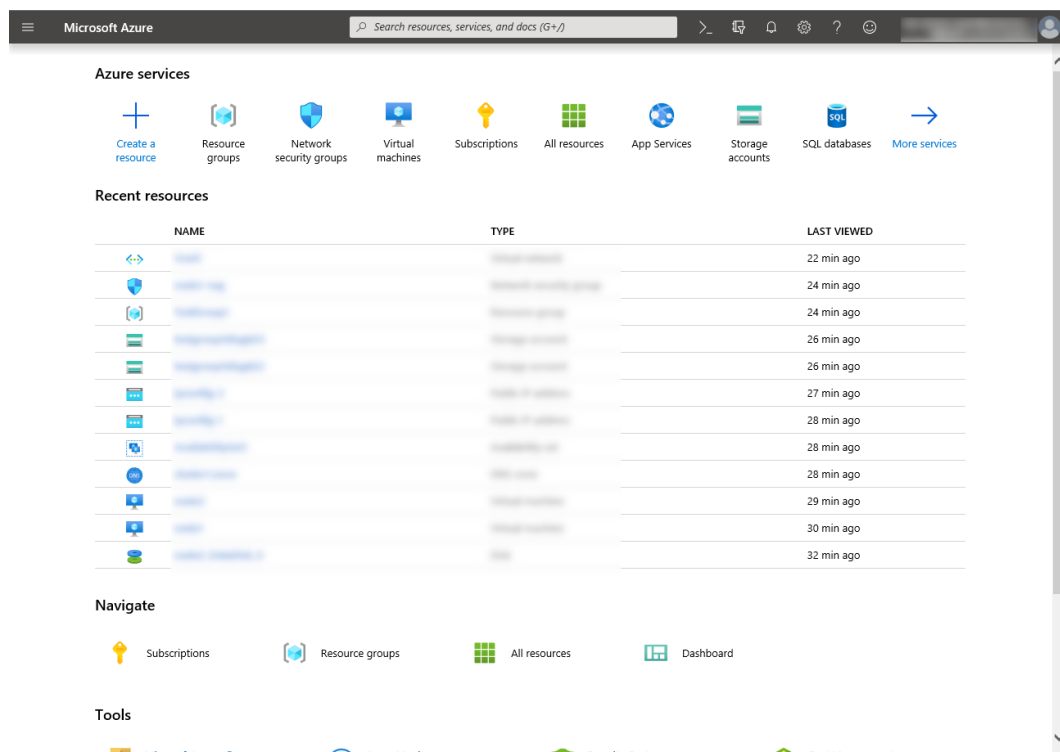


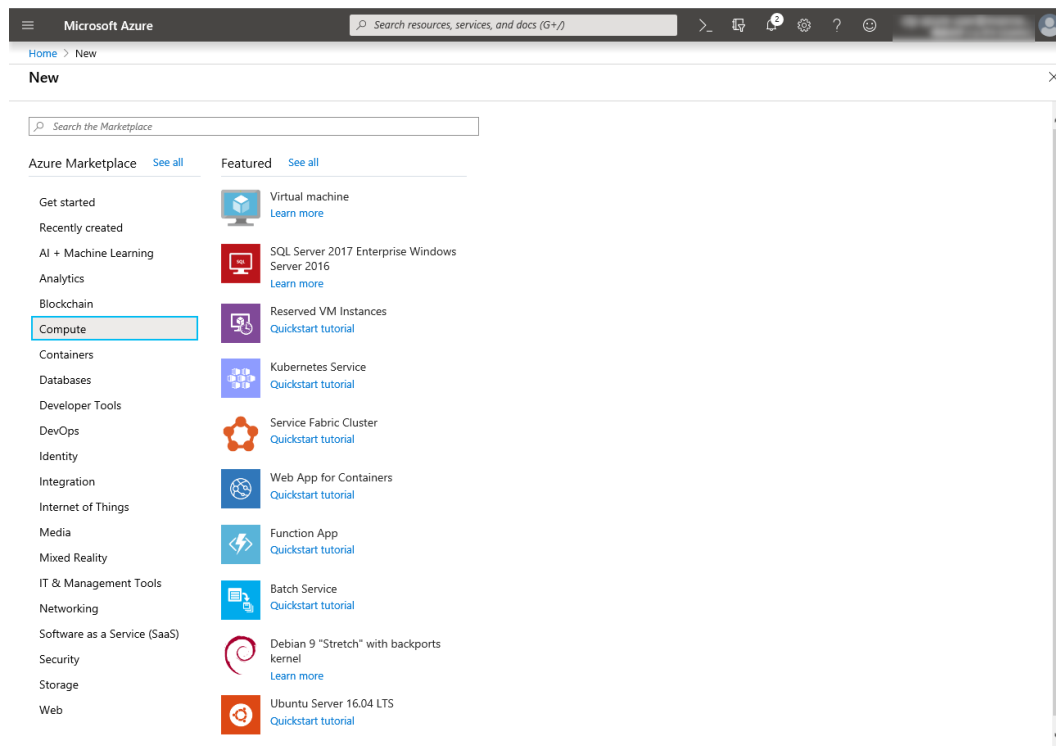
3) Creating a virtual machine

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create virtual machines and disks following the steps below.

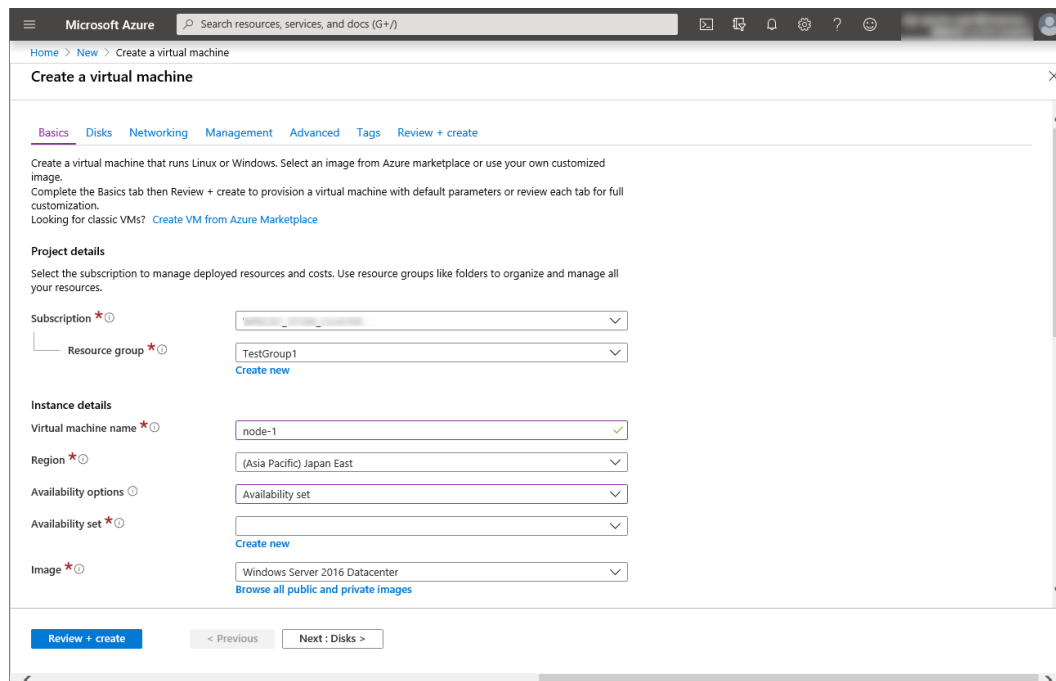
Create as many virtual machines as required to create a cluster. Create node-1 and then node-2.

1. Select **Create a resource** on the upper part of the window.



2. Select **Compute** and then **See all**.3. Select **Windows Server 2016 Datacenter**.

4. When the **Basics** tab appears, specify the settings of **Subscription**, **Resource group**, **Virtual machine name**, **Region**, **Image**, **Size**, **Username**, **Password**, and **Confirm password**. Select **Availability set** from **Availability options**, and click **Create new** under the **Availability set** field. When the **Create new** blade appears, specify the settings of **Name**, **Fault domains**, and **Update domains**. Then click **OK**.



Click **Change size** to display the **Select a VM size** blade.

From the list, choose a size (**A1 - Standard** in this guide) suitable for your virtual machine and click **Select**.

Regarding the **Virtual machine name**, node-1 is for node-1, and node-2 is for node-2.

Click **Next: Disks >**

- When the **Disks** tab appears, go through the following steps to add a disk to be used for a mirror disk (cluster partition or data partition).

From the **DATA DISKS** list, click **Create and attach a new disk**.

Microsoft Azure Search resources, services, and docs (G+/I)

Home > New > Create a virtual machine

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type *

Enable Ultra Disk compatibility ☐ Yes ☒ No

Ultra Disk compatibility is not available for this VM size and location.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
Create and attach a new disk Attach an existing disk				

Advanced

[Review + create](#) [< Previous](#) [Next: Networking >](#)

6. The **Create a new disk** blade appears.
- Specify **Name**, **Source type**, and **Size**. Then click **OK**.
- Click **Next: Networking >**.

Microsoft Azure Search resources, services, and docs (G+/I)

Home > New > Create a virtual machine > Create a new disk

Create a new disk

Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions. [Learn more about Azure Managed Disks](#)

Name *

Source type *

Size *

Standard HDD

[Change size](#)

[OK](#)

7. The **Networking** tab appears.
- Specify the settings of **Virtual network**, **Subnet**, **Network security group**, and **Configure network security group**.
- Click **Create new** under the **Configure network security group** field to display the **Create network security group** blade. Specify the setting of **Name** and then click **OK**.
- Click **Next: Management >**.

The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal, specifically the 'Networking' tab. The page title is 'Create a virtual machine'. Below the title are tabs for 'Basics', 'Disks', 'Networking' (selected), 'Management', 'Advanced', 'Tags', and 'Review + create'. The main content area is titled 'Network interface' and contains the following settings:

- Virtual network ***: A dropdown menu showing 'Vnet1' with a 'Create new' link below it.
- Subnet ***: A dropdown menu showing 'Vnet1-1 (10.5.0.0/24)' with a 'Manage subnet configuration' link below it.
- Public IP**: A dropdown menu showing 'None' with a 'Create new' link below it.
- NIC network security group**: Three radio buttons: 'None', 'Basic', and 'Advanced' (selected).
- Configure network security group ***: A dropdown menu showing '(new) node-1-nsg' with a 'Create new' link below it.
- Accelerated networking**: Two radio buttons: 'On' and 'Off' (selected). A note below states: 'The selected VM size does not support accelerated networking.'

At the bottom, there is a 'Load balancing' section with a note: 'You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)'. At the very bottom are three buttons: 'Review + create' (in blue), '< Previous', and 'Next : Management >'.

8. The **Management** tab appears.

Click **Create new** under the **Diagnostics storage account** field to display the **Create storage account** blade.

Specify the settings of **Name**, **Account kind**, and **Replication**. Then click **OK**.

In the **Diagnostics storage account** field, the default value is automatically generated and entered.

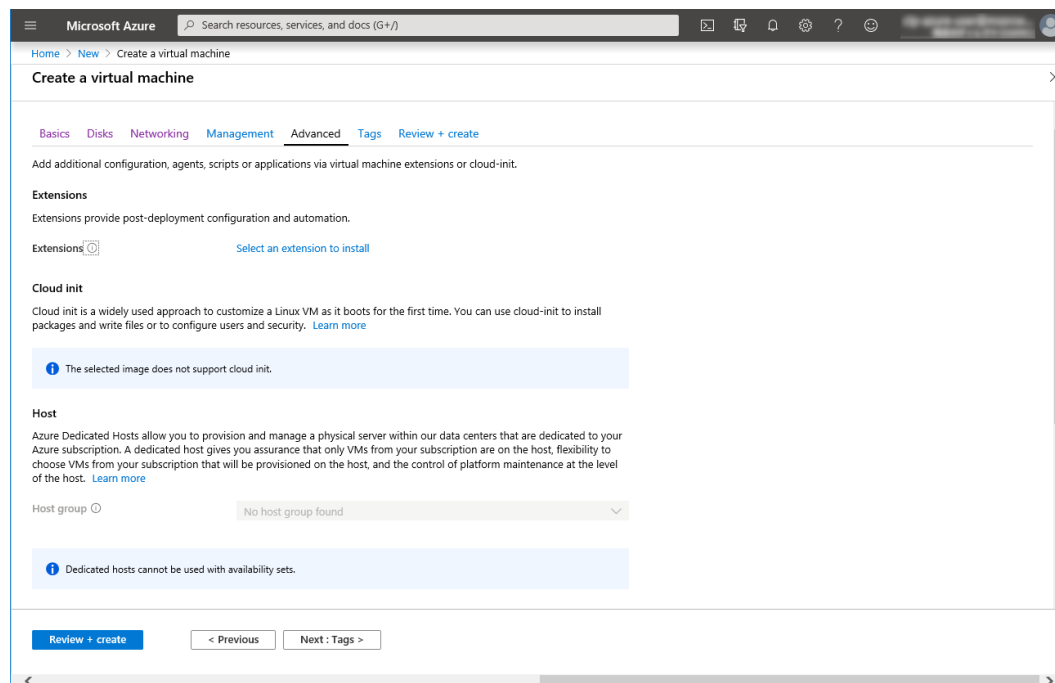
Click **Next: Advanced >**.

The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal, specifically the 'Management' tab. The page title is 'Create a virtual machine'. Below the title are tabs for 'Basics', 'Disks', 'Networking', 'Management' (selected), 'Advanced', 'Tags', and 'Review + create'. The main content area is titled 'Configure monitoring and management options for your VM.' and contains the following settings:

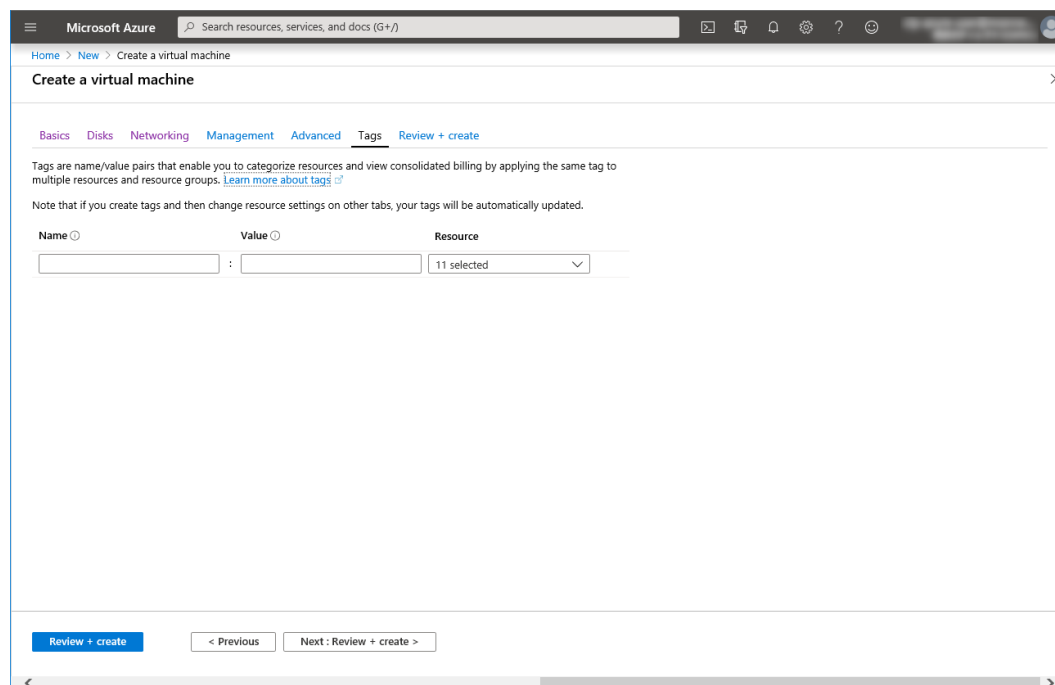
- Azure Security Center**: A green checkmark icon and the text 'Your subscription is protected by Azure Security Center basic plan.' with a 'Learn more' link.
- Monitoring**:
 - Boot diagnostics**: Two radio buttons: 'On' (selected) and 'Off'.
 - OS guest diagnostics**: Two radio buttons: 'On' and 'Off' (selected).
 - Diagnostics storage account ***: A dropdown menu showing 'testgroup1diag600' with a 'Create new' link below it.
- Identity**:
 - System assigned managed identity**: Two radio buttons: 'On' and 'Off' (selected).
- Azure Active Directory**:
 - Login with AAD credentials (Preview)**: Three radio buttons: 'On', 'Off', and 'Off' (selected).

At the bottom are three buttons: 'Review + create' (in blue), '< Previous', and 'Next : Advanced >'.

9. Click **Next: Tags >**.



10. Click **Next: Review + create >**.

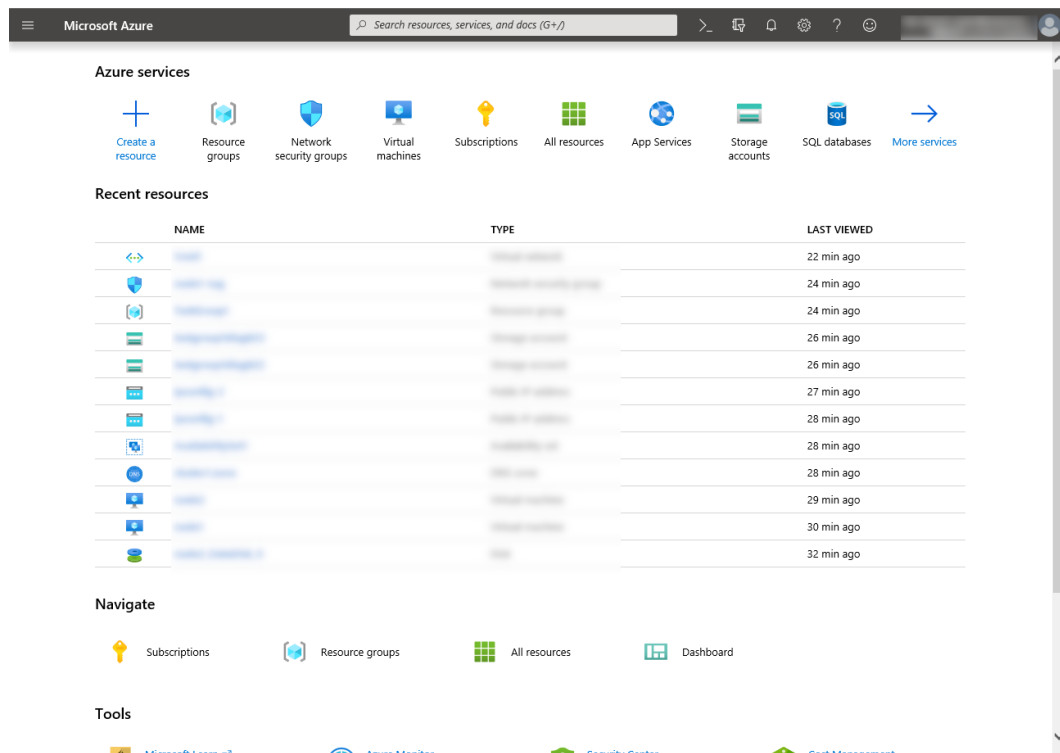


11. The **Review + create** tab appears. Check the contents. If there is no problem, click **Create**. The deployment starts and takes several minutes.

4) Setting a private IP address

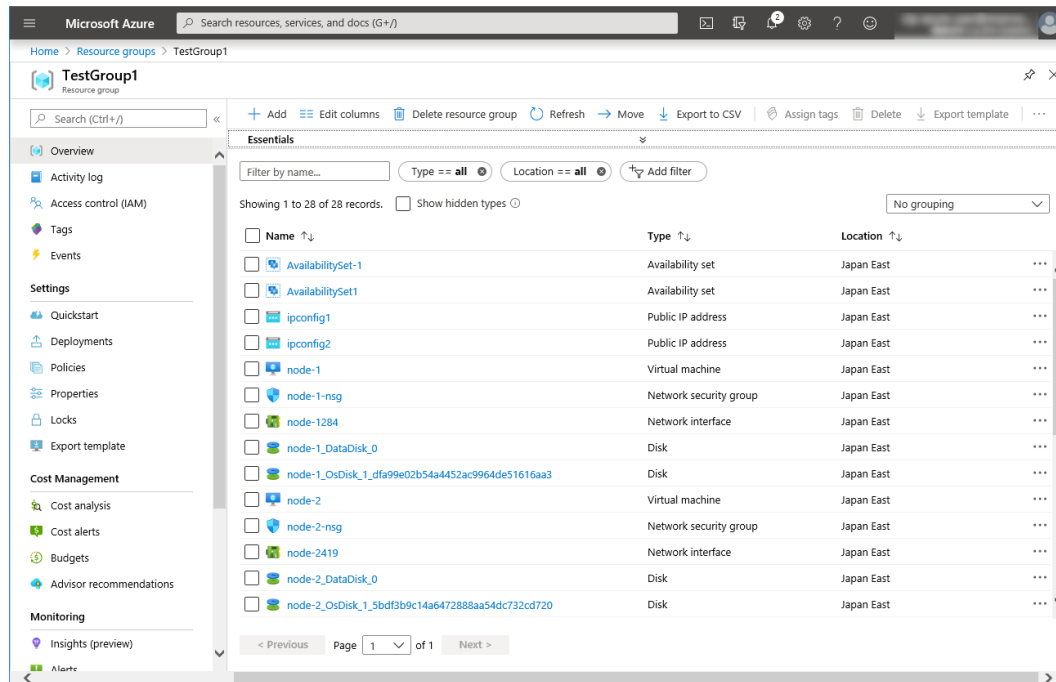
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and change the private IP address setting following the steps below. Since an IP address is initially set to be assigned dynamically, change the setting so that an IP address is assigned statically. Change the settings of node-1 and then node-2.

1. Select **Resource groups** on the upper part of the window.

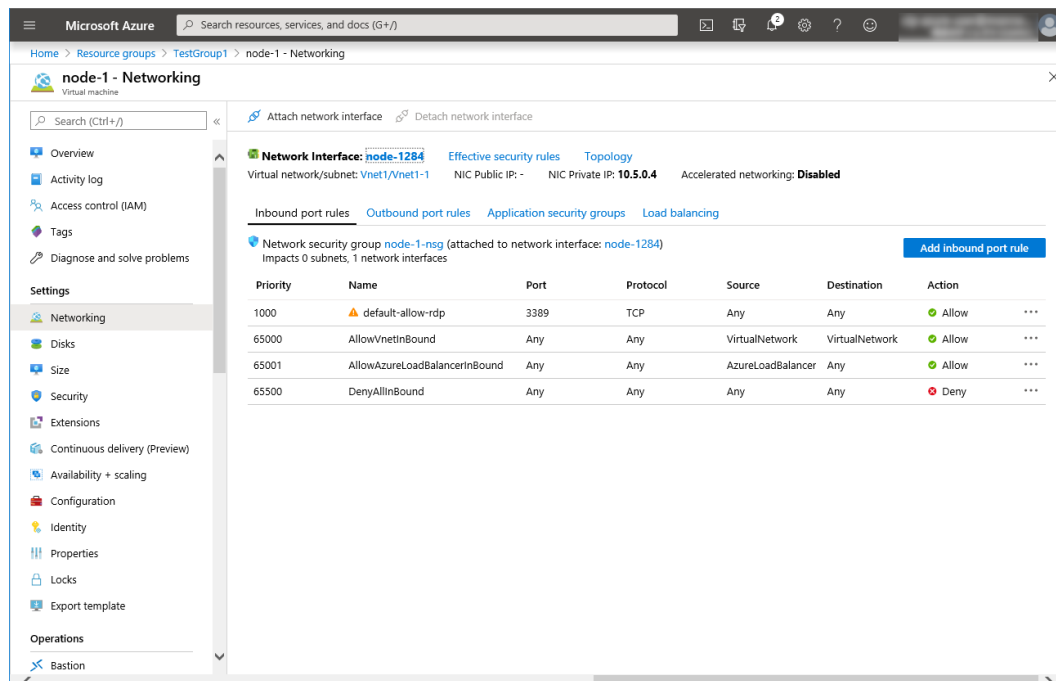


2. Select TestGroup1 from the resource group list.

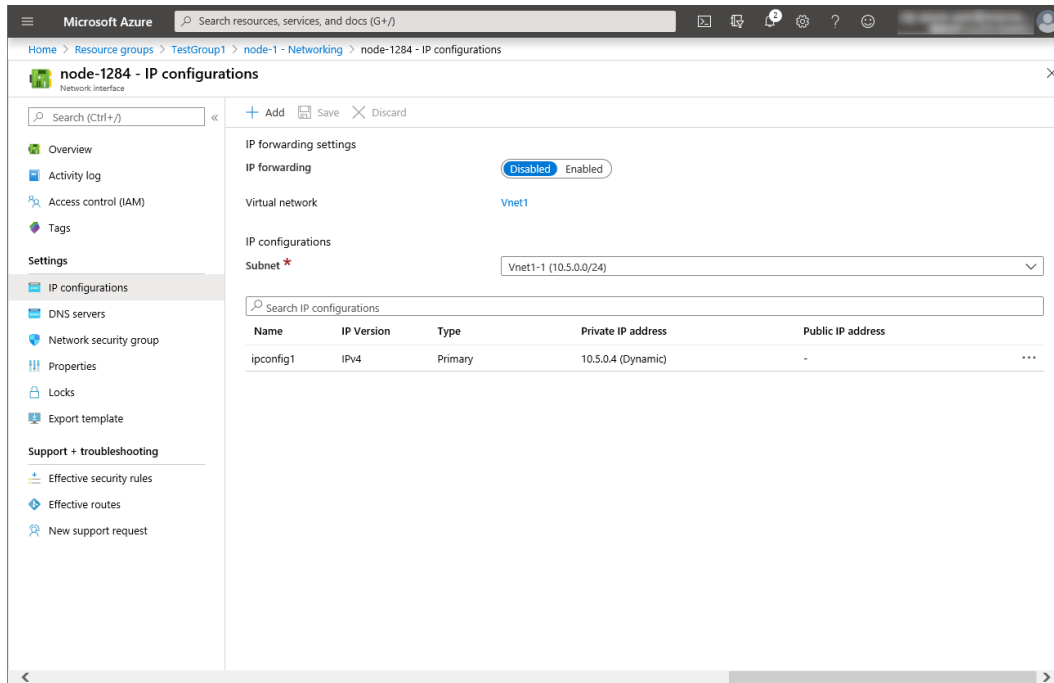
3. The summary of TestGroup1 is displayed. Select virtual machine node-1 or node-2 from the item list.



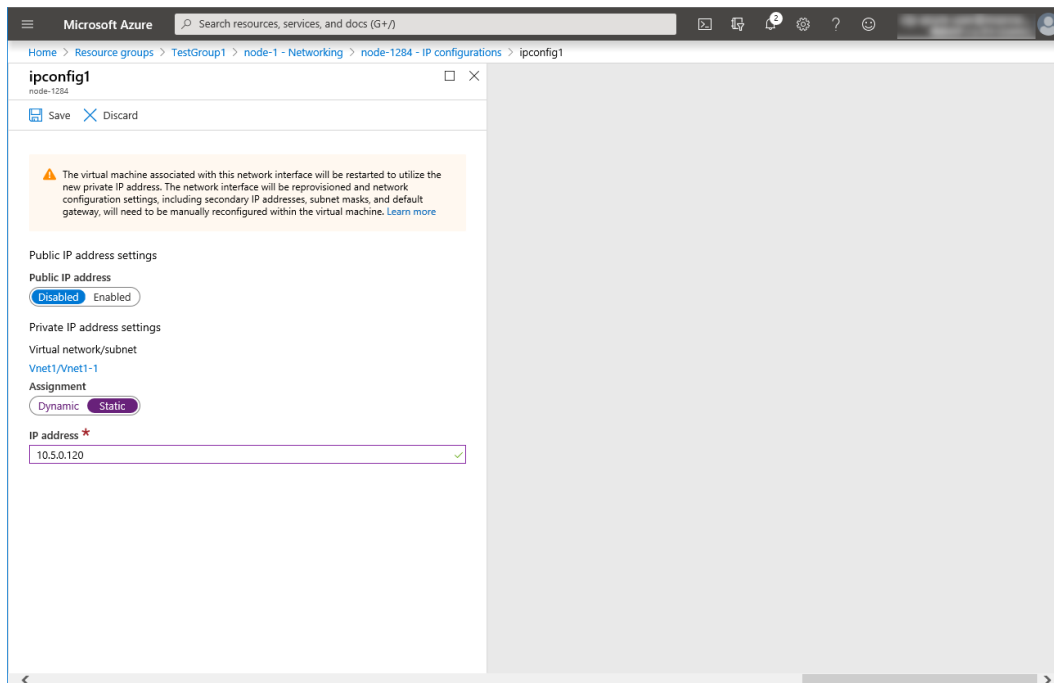
4. Select **Networking**.



5. Select a network interface displayed in the list. The network interface name is generated automatically.
6. Select **IP configurations**.



7. Only ipconfig1 is displayed in the list. Select it.
8. Select **Static** for **Assignment** under **Private IP address settings**. Enter the IP address to be assigned statically in the **IP address** text box and click **Save** at the top of the window. The IP address of node-1 is 10.5.0.120. The IP address of node-2 is 10.5.0.121.

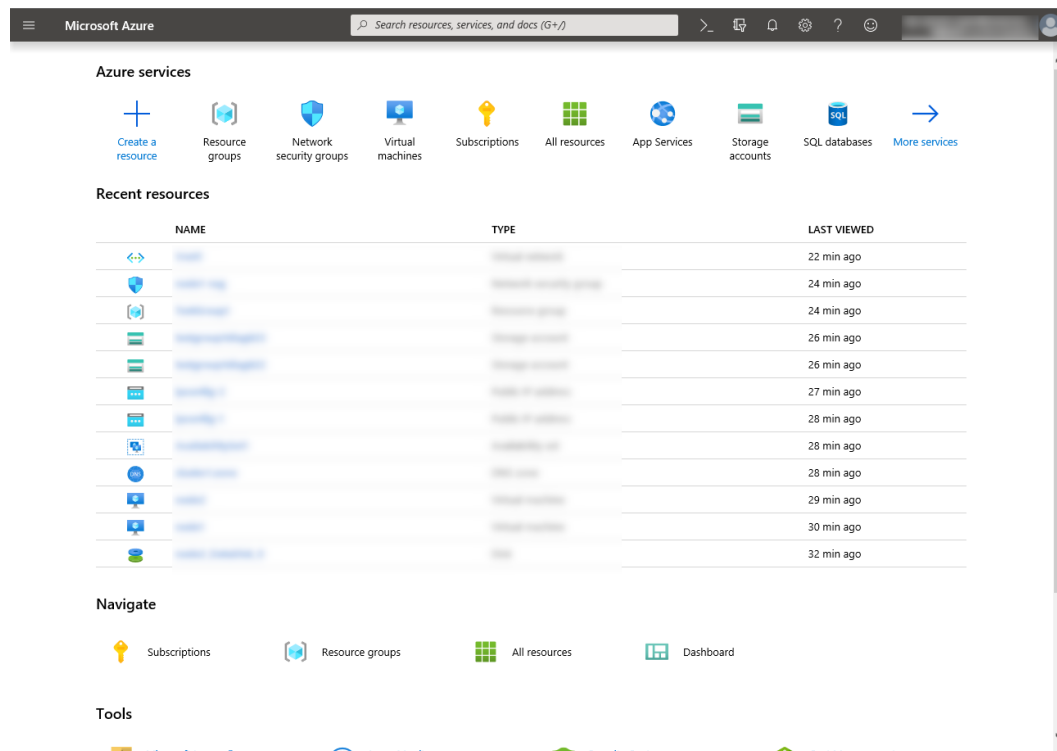


9. The virtual machines restart automatically so that new private IP addresses can be used.

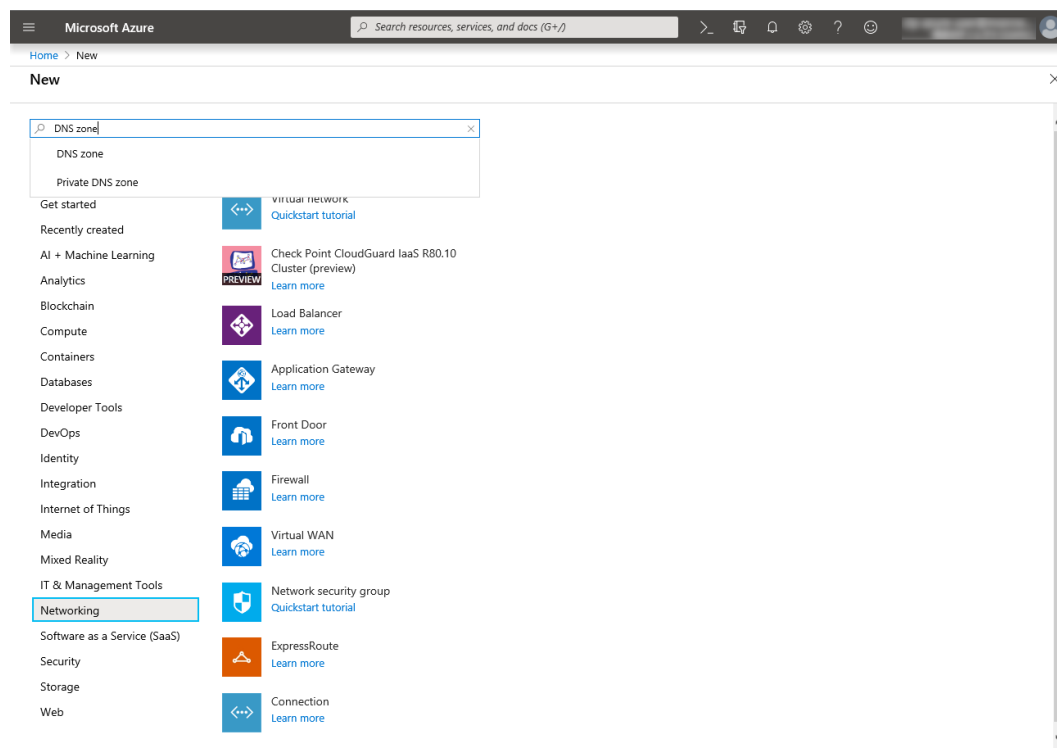
5) Creating a DNS zone

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and configure the DNS zone following the steps below.

1. Select **Create a resource** on the upper part of the window.



2. Select **Networking > See all**, and search for DNS zone.



3. **Create DNS zone** is displayed. Specify **Subscription**, **Resource group**, and **Name**, and click **Review+create**. Then click **Create**.

The screenshot shows the 'Create DNS zone' page in the Microsoft Azure portal. The breadcrumb navigation at the top indicates the path: Home > New > DNS zone > Create DNS zone. The page has a title bar 'Create DNS zone' with a close button. Below the title bar, there are tabs for 'Basics', 'Tags', and 'Review + create'. The 'Basics' tab is active. A descriptive paragraph explains that a DNS zone is used to host DNS records for a particular domain. Below this, the 'Project details' section contains a 'Subscription' dropdown and a 'Resource group' dropdown set to 'TestGroup1' with a 'Create new' link. The 'Instance details' section contains a 'Name' field with 'cluster1.zone' and a green checkmark, and a 'Resource group location' dropdown set to '(Asia Pacific) Japan East'. At the bottom, there are three buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next: Tags >', along with a link 'Download a template for automation'.

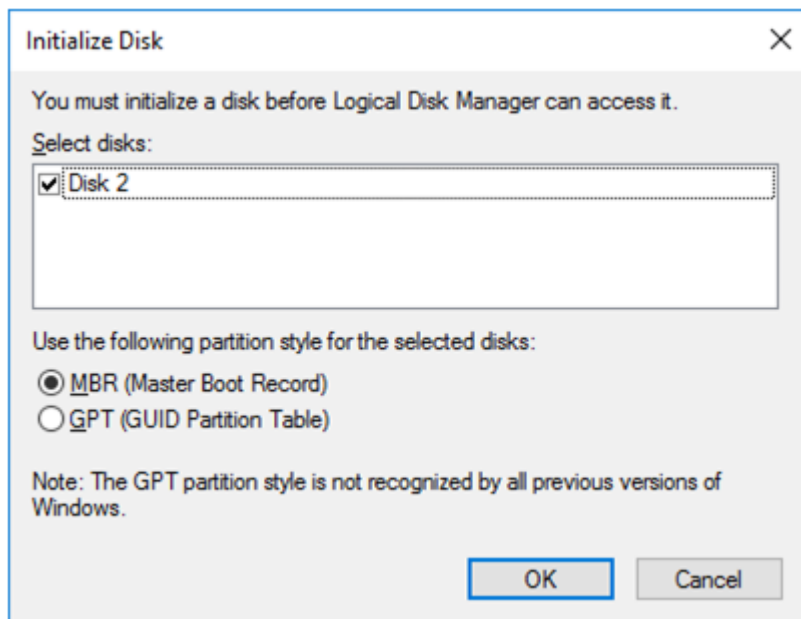
6) Configuring virtual machines

Log in to the created node-1 and node-2 and specify the settings following the procedure below.

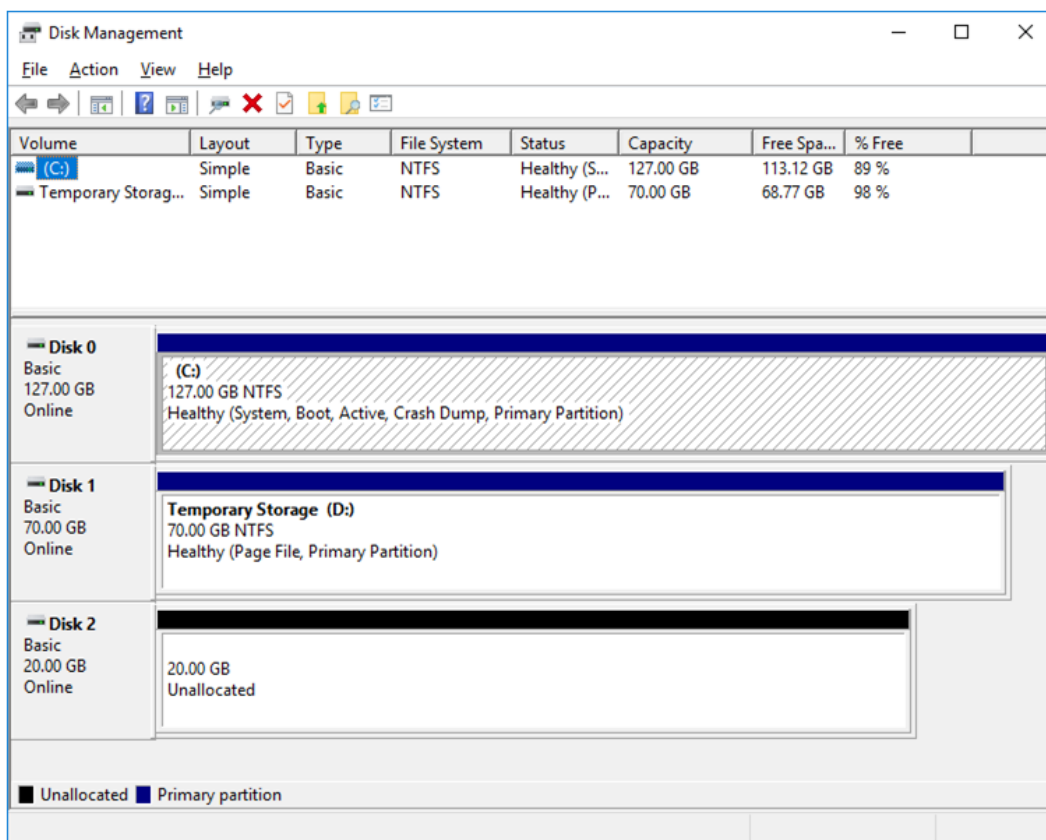
Set a partition for the mirror disk resource. Create a file system in the added disk.

For details about the partition for the mirror disk resource, see "Partition settings for mirror disk resource (when using Replicator)" in "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.

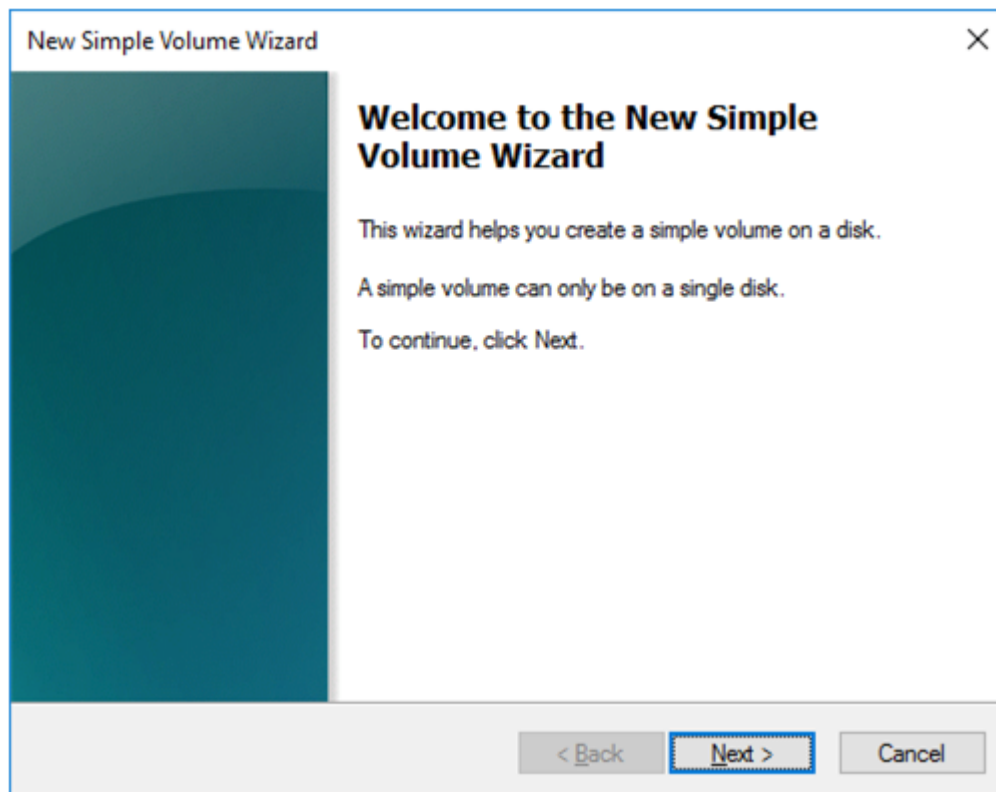
1. Open the **Disk Management** window. The **Initialize Disk** dialog box is displayed.



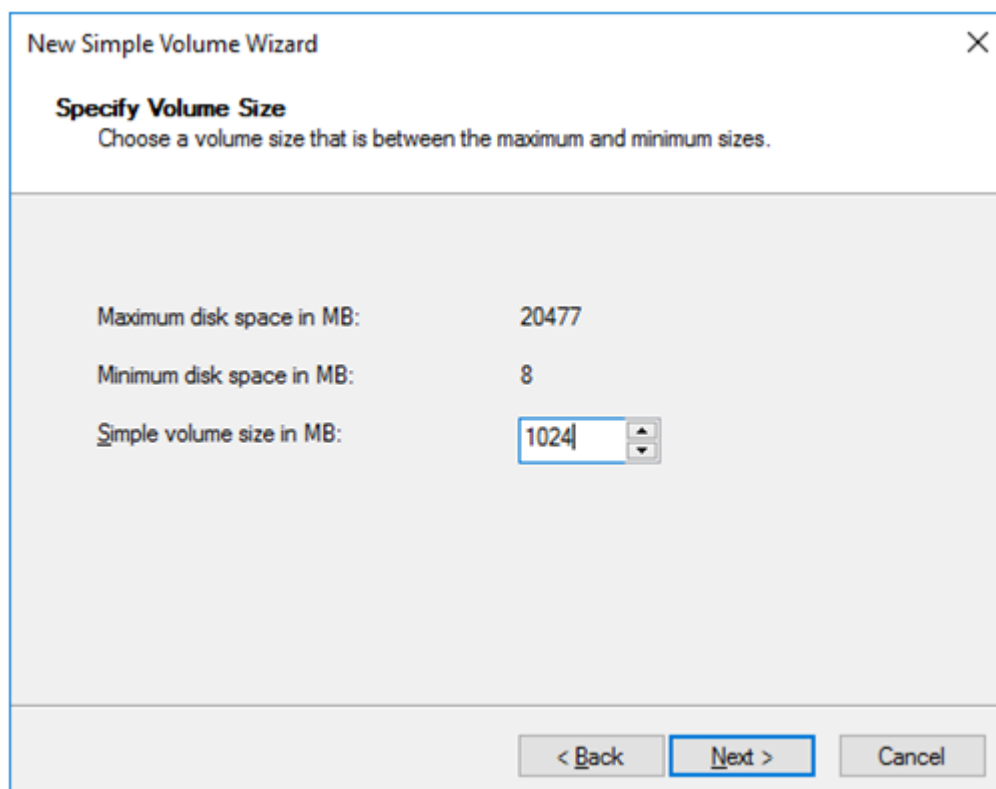
2. Confirm that the added disk is displayed as "Disk 2" in unassigned state under the existing C drive and D drive.



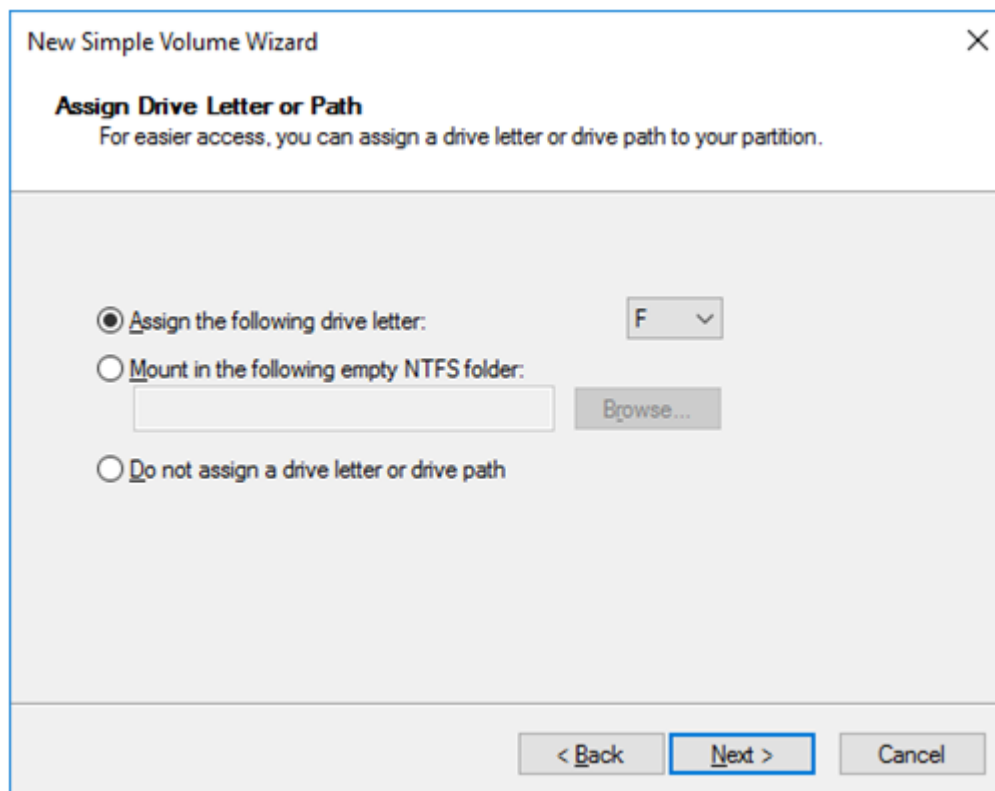
3. Create a cluster partition. Right-click "Disk 2" and select **New Simple Volume**.
4. The **Welcome to the New Simple Volume Wizard** is displayed. Click **Next**.



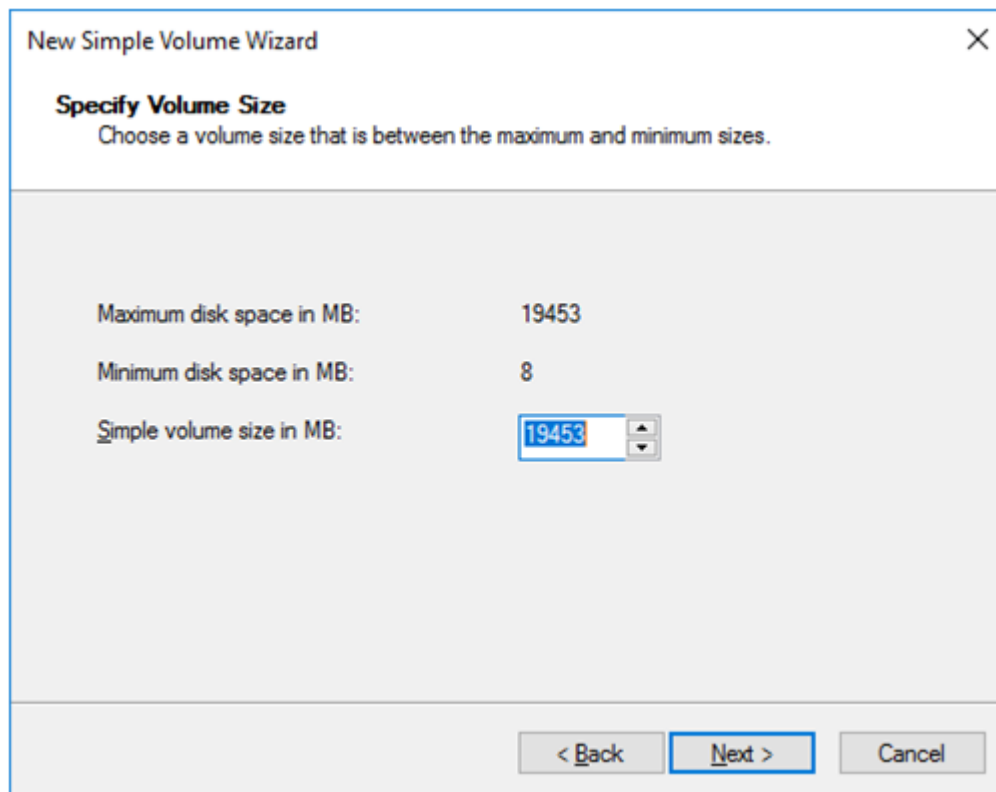
5. The **Specify Volume Size** window is displayed. Allocate 1024 MB (1,073,741,824 bytes) or more to a cluster partition. Click **Next**.



6. The **Assign Drive Letter or Path** window is displayed. Select the F drive for **Assign the following drive letter:.** Use the disk as a raw partition without formatting.

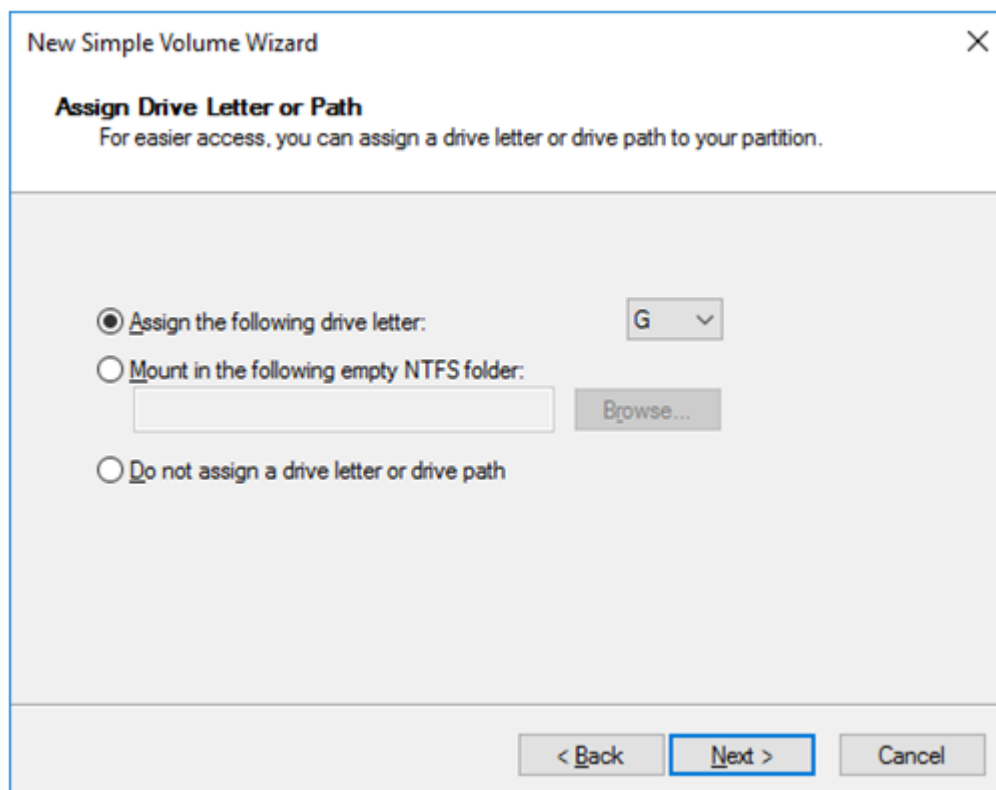


7. Next, create a data partition. Right-click "Disk 2" and select **New Simple Volume**.
8. The **Welcome to the New Simple Volume Wizard** is displayed. Click **Next**.
9. The **Specify Volume Size** window is displayed. Click **Next**.



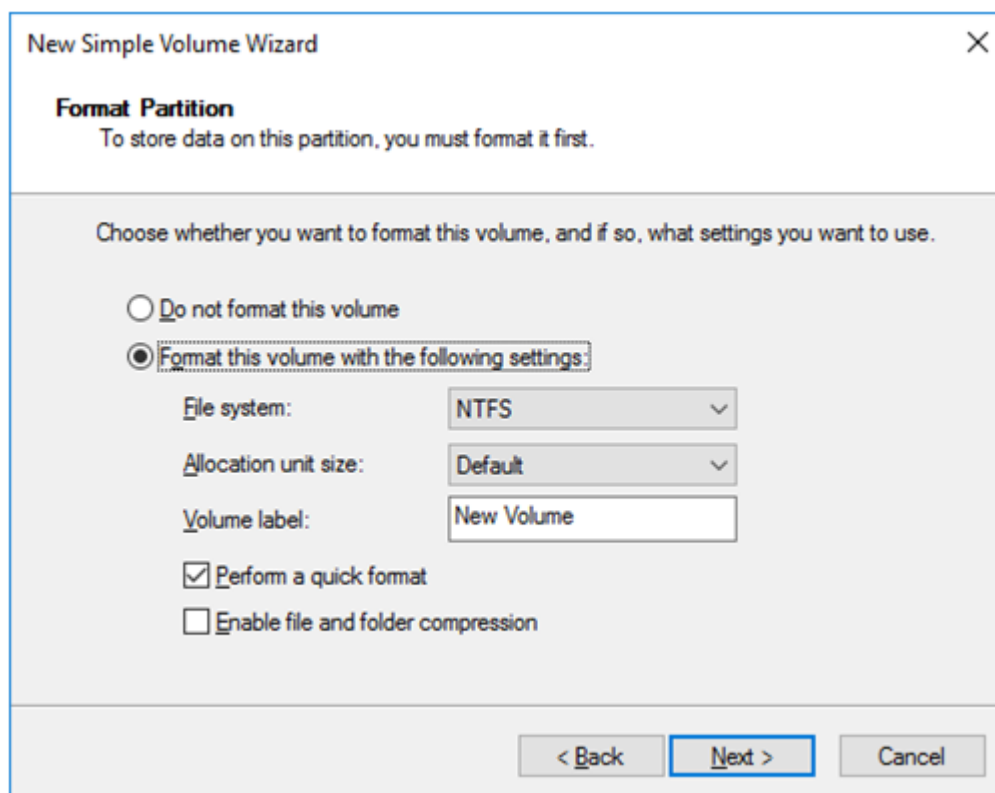
The screenshot shows the 'New Simple Volume Wizard' window, specifically the 'Specify Volume Size' step. The window title is 'New Simple Volume Wizard' with a close button (X) in the top right corner. Below the title bar, the section header is 'Specify Volume Size' followed by the instruction 'Choose a volume size that is between the maximum and minimum sizes.' The main area contains three rows of information: 'Maximum disk space in MB:' with the value '19453', 'Minimum disk space in MB:' with the value '8', and 'Simple volume size in MB:' with a text box containing '19453' and a spinner control to its right. At the bottom of the window, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

10. The **Assign Drive Letter or Path** window is displayed. Select the G drive for **Assign the following drive letter:** and click **Next**.

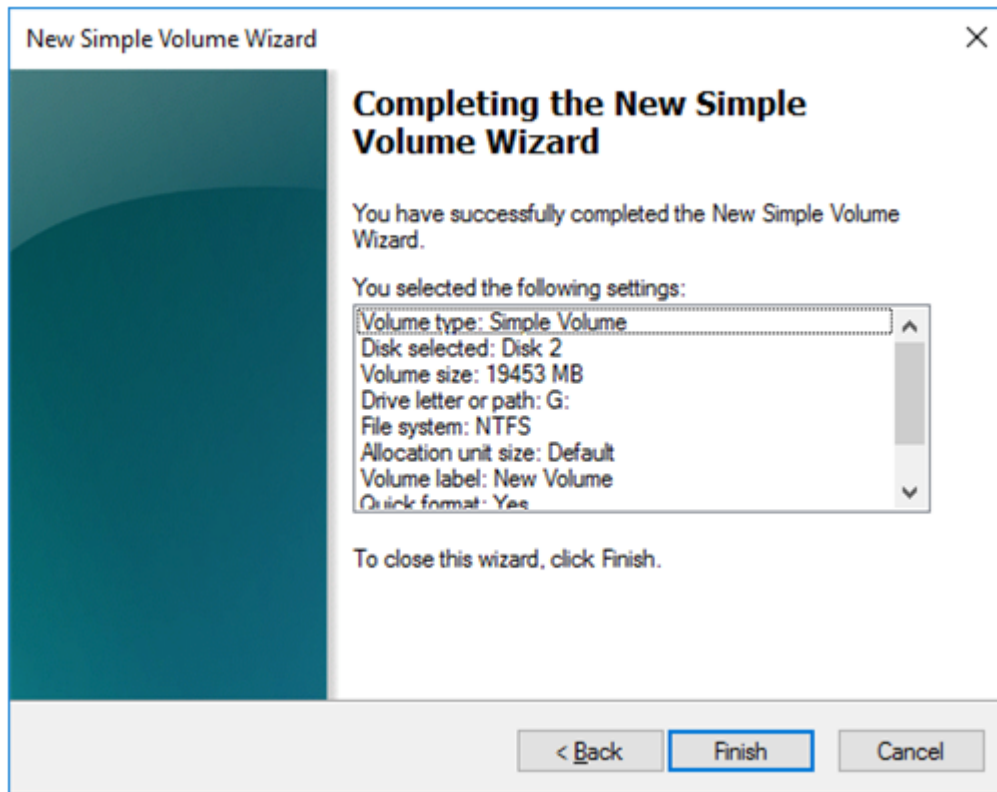


The screenshot shows the 'New Simple Volume Wizard' window, specifically the 'Assign Drive Letter or Path' step. The window title is 'New Simple Volume Wizard' with a close button (X) in the top right corner. Below the title bar, the section header is 'Assign Drive Letter or Path' followed by the instruction 'For easier access, you can assign a drive letter or drive path to your partition.' The main area contains three radio button options: the first is 'Assign the following drive letter:' with a dropdown menu showing 'G'; the second is 'Mount in the following empty NTFS folder:' with a text box and a 'Browse...' button; and the third is 'Do not assign a drive letter or drive path'. At the bottom of the window, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

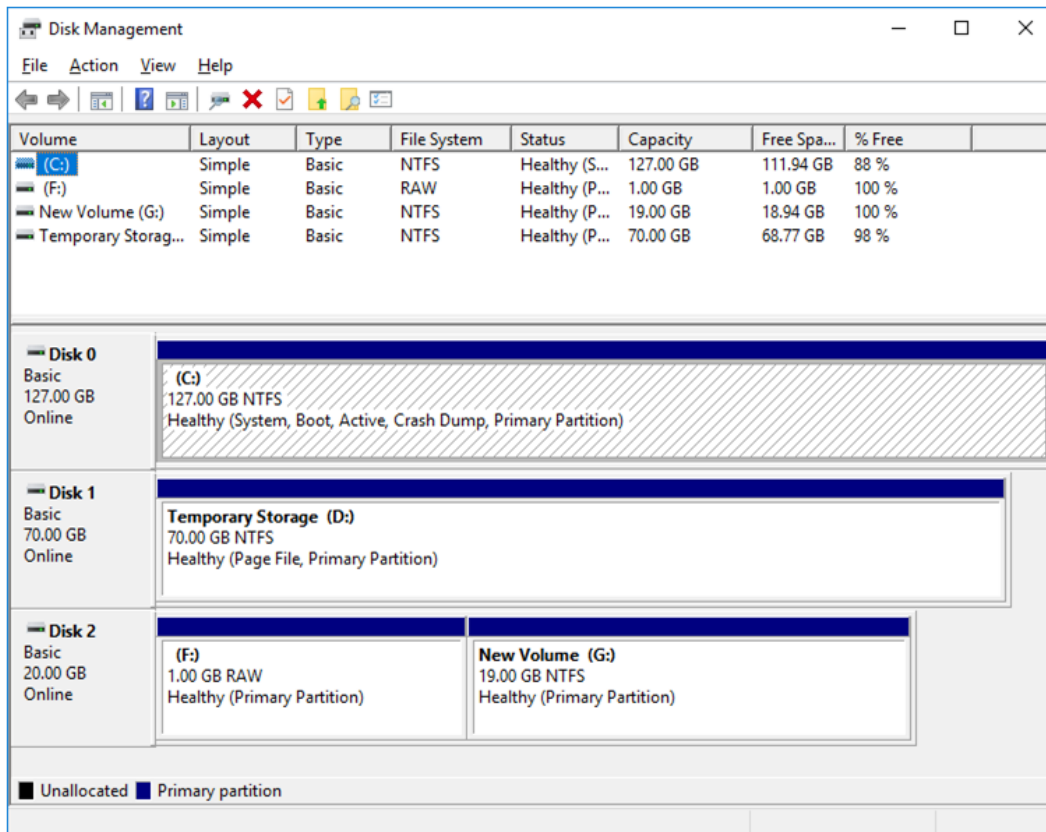
11. The **Format Partition** window is displayed. Confirm that **File System** is **NTFS**.



12. Click **Next**.
13. The **Completing the New Simple Volume Wizard** window is displayed. Check the displayed contents and click **Finish**.



14. Confirm that the added disks are assigned as the F drive and G drive.



- 7) **Adjusting the OS startup time, checking the network setting, checking the firewall setting, synchronizing the server time, and disabling the power saving function.**

For each procedure, see "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.

8) **Installing the Azure CLI**

Install the Azure CLI.

The procedure to install the Azure CLI from the installer is described.

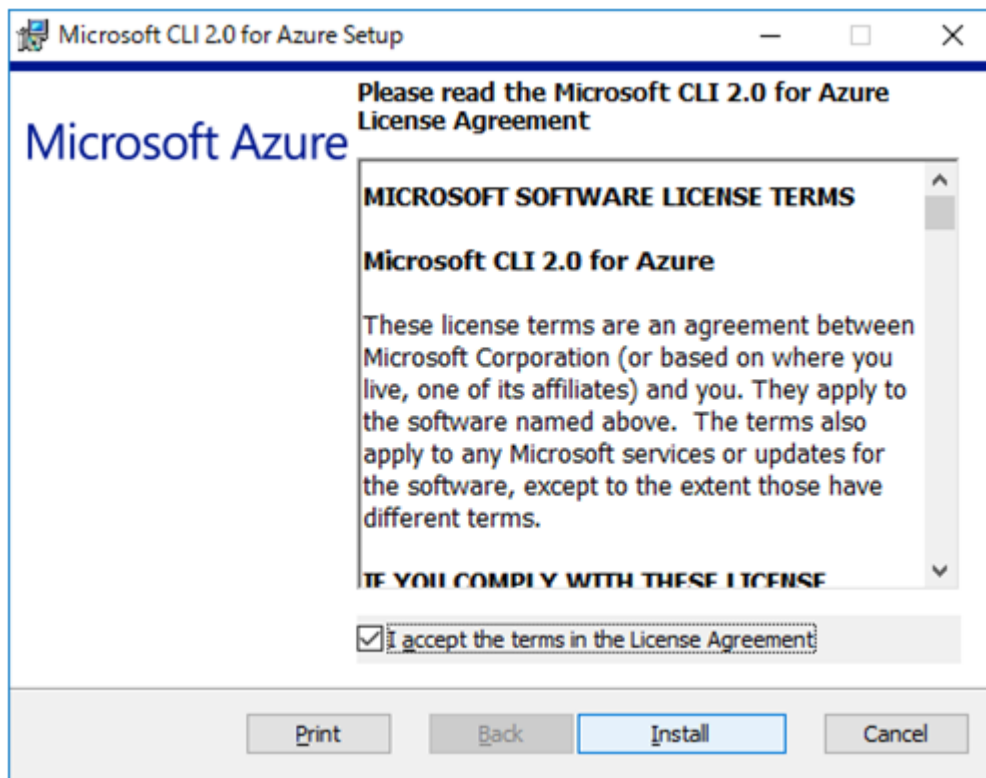
For details about this procedure and other procedures, see the following website:

Install the Azure CLI:

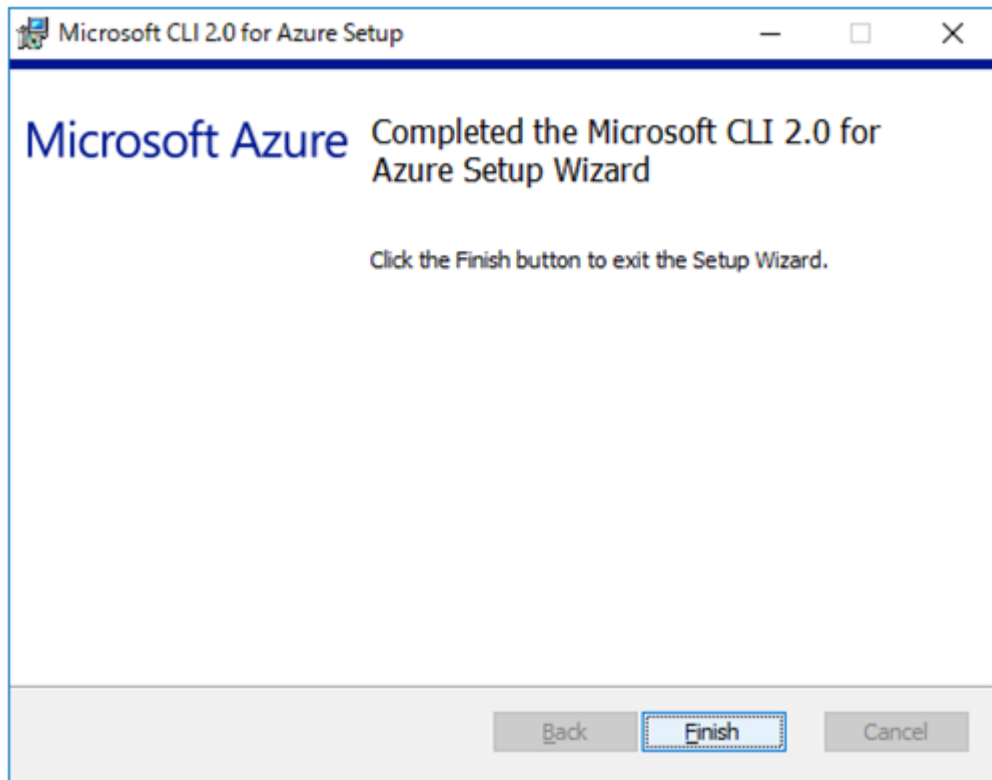
<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest>

Log in to the created node-1 and node-2 and install the Azure CLI following the procedure below.

1. Download the MSI installer from the above website.
2. Double-click the MSI installer file and click **Run**.
3. Agree with the license terms and click **Install**.



4. When the installation complete window is displayed, click **Finish**.



9) Creating a service principal

Create a service principal using the Azure CLI.

A script for Azure DNS performs login to Microsoft Azure and DNS zone registration and monitoring. When logging in to Microsoft Azure, Azure login with a service principal is used.

Please note that certificates have an expiration date.

For more details, see the --years option of `az ad sp create-for-rbac`.

<https://docs.microsoft.com/en-us/cli/azure/ad/sp?view=azure-cli-latest#az-ad-sp-create-for-rbac>

For details about a service principal and procedure, see the following websites:

Sign in with Azure CLI:

<https://docs.microsoft.com/en-us/cli/azure/authenticate-azure-cli?view=azure-cli-latest>

Create an Azure service principal with Azure CLI:

<https://docs.microsoft.com/en-us/cli/azure/create-an-azure-service-principal-azure-cli?view=azure-cli-latest>

1. Log in with an organizational account.

```
az login -u <account-name> -p <password>
```

2. Create and register a service principal. Write down the displayed name and tenant because they need to be entered for configuring Azure DNS resource by Cluster WebUI. In the following example, a service principal is created in C:\Users\testlogin\examplecert.pem.

```
az ad sp create-for-rbac --create-cert --scope
{
  "appId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "displayName": "azure-test",
  "fileWithCertAndPrivateKey": "C:\\Users\\testlogin\\examplecert.
pem",
  "name": "http://azure-test",
  "password": null,
  "tenant": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

3. Log out.

```
az logout --u <account-name>
```

4. Check whether login to Microsoft Azure using the created service principal is possible.

```
az login --service-principal -u <name-value-in-step-2> --tenant
↪<tenant-value-in-step-2> -p <fileWithCertAndPrivateKey-value-in-step-2>
↪
```

The following is displayed upon successful sign-in.

```
[
  {
    "cloudName": "AzureCloud",
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "isDefault": true,
    "name": "xxxxxxxx",
    "state": "Enabled",
    "tenantId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "user": {
      "name": "http://azure-test",
      "type": "servicePrincipal"
    }
  }
]
```

5. Log out.

```
az logout --username <name-value-in-step-4>
```

When changing the role of the created service principal from the default "Contributor" to another role, select a role that has access permissions to all of the following operations as the Actions properties. If the role is changed to a role that does not satisfy this condition, monitoring by the Azure DNS monitor resource, which are set up later, fails due to an error.

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

10) Installing EXPRESSCLUSTER

For the installation procedure, see the Installation and Configuration Guide.

After installation is complete, restart the OS.

11) Registering the EXPRESSCLUSTER license

For the license registration procedure, see the Installation and Configuration Guide.

4.3 Configuring the EXPRESSCLUSTER settings

For the Cluster WebUI setup and connection procedures, see "Creating the cluster configuration data" in the Installation and Configuration Guide.

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

- Mirror disk resource
- Azure DNS resource
- Azure DNS monitor resource
- Custom monitor resource (for NP resolution)
- IP monitor resource (for NP resolution)
- Multi target monitor resource (for NP resolution)

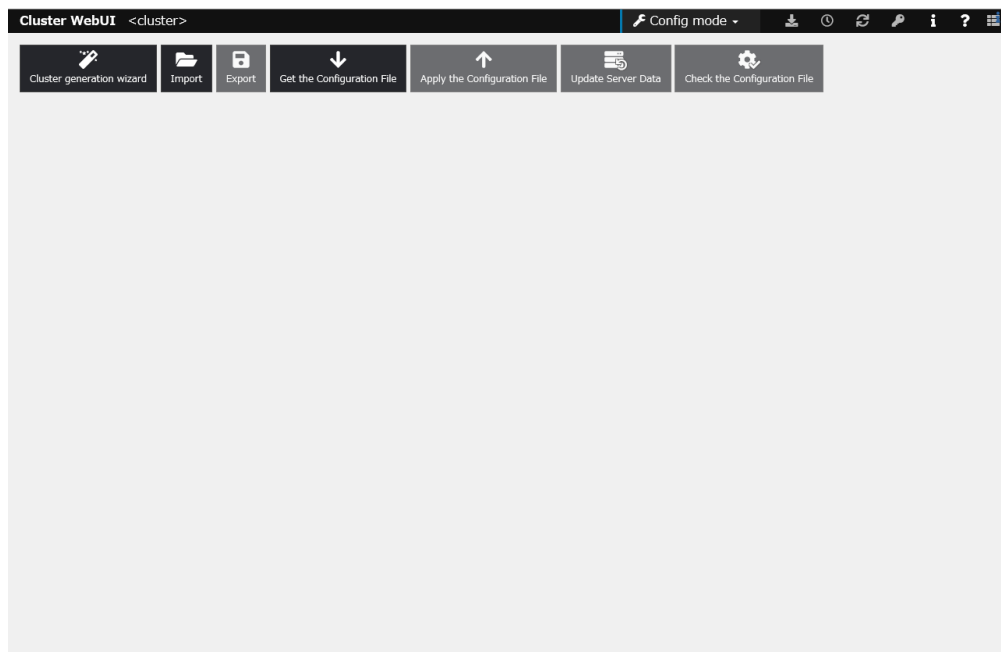
or the settings of other resources and monitor resources, see the Installation and Configuration Guide and the Reference Guide.

1) Creating a cluster

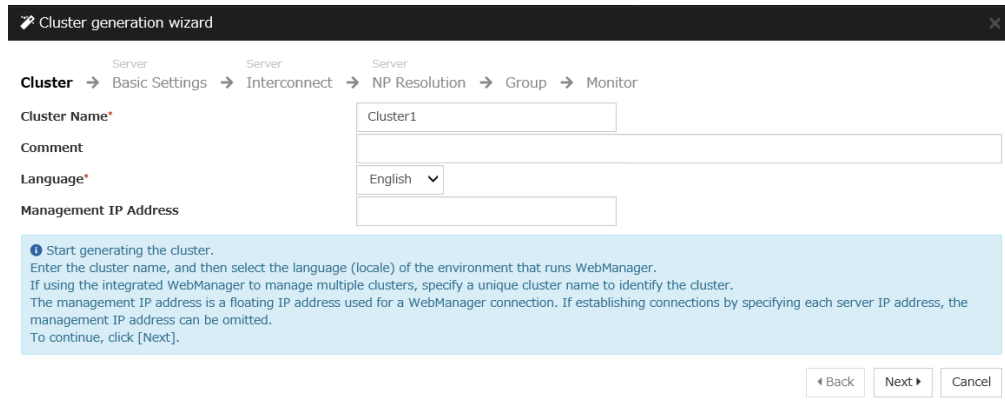
Start the Cluster generation wizard to create a cluster.

- Creating a cluster

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



2. The **Cluster** window on the **Cluster generation wizard** is displayed.
Enter a desired name in **Cluster Name**.
Select an appropriate language in **Language**. Click **Next**.



Cluster generation wizard

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

Cluster Name*

Comment

Language* English ▾

Management IP Address

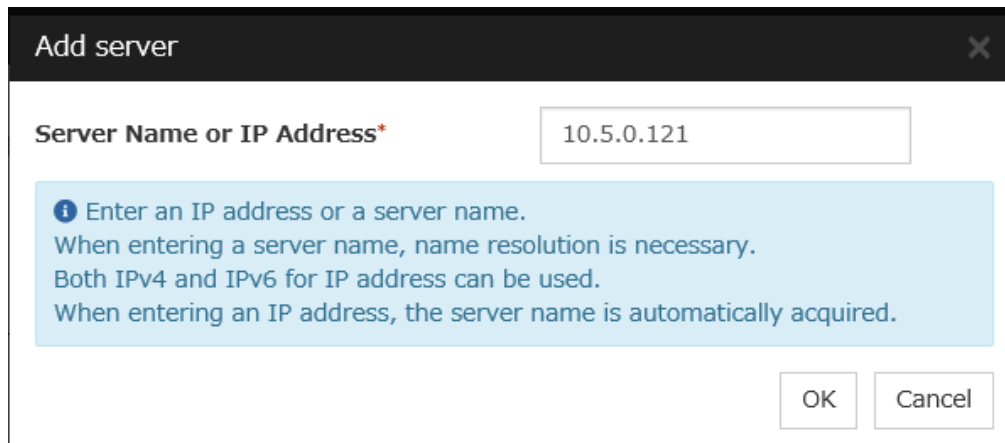
Start generating the cluster.
 Enter the cluster name, and then select the language (locale) of the environment that runs WebManager.
 If using the integrated WebManager to manage multiple clusters, specify a unique cluster name to identify the cluster.
 The management IP address is a floating IP address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

◀ Back Next ▶ Cancel

3. The **Basic Settings** window is displayed.

The instance connected to Cluster WebUI is displayed as a registered master server.

Click **Add** to add the remaining instances (by specifying the private IP address of each instance). Click **Next**.

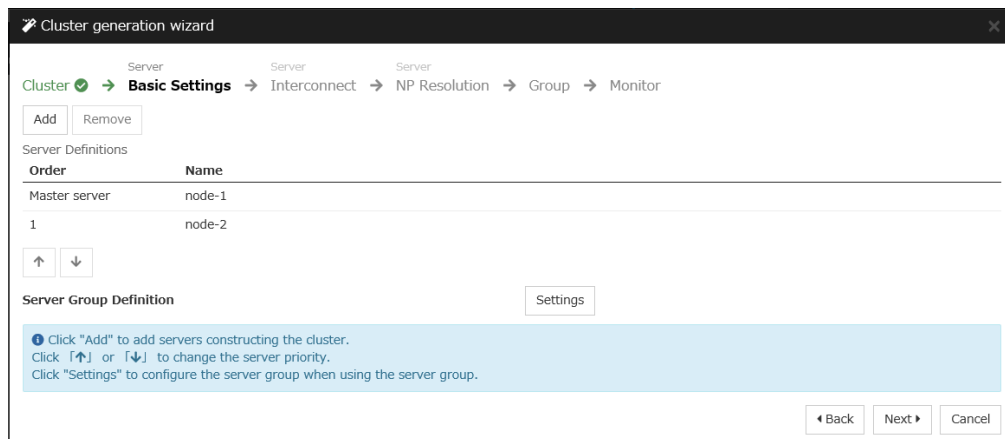


Add server

Server Name or IP Address*

Enter an IP address or a server name.
 When entering a server name, name resolution is necessary.
 Both IPv4 and IPv6 for IP address can be used.
 When entering an IP address, the server name is automatically acquired.

OK Cancel



Cluster generation wizard

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

Add Remove

Server Definitions

Order	Name
Master server	node-1
1	node-2

↑ ↓

Server Group Definition Settings

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

◀ Back Next ▶ Cancel

4. The **Interconnect** window is displayed.

Specify the IP addresses (IP address of each instance) to be used for interconnect. In addition, select mdc1 for **MDC** as a communication path of a mirror disk resource to be created later.

Click **Next**.

Cluster generation wizard

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

Properties Add Remove

Interconnect List

Priority	Type	MDC	node-1	node-2
1	Kernel Mode	mdc1	10.5.0.120	10.5.0.121

↑ ↓

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

Back Next Cancel

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

Note that NP resolution is not configured on this window. The equivalent feature is achieved by adding the IP monitor resource, custom monitor resource, and multi target monitor resource. Configure NP resolution in "3) **Adding a monitor resource**"

You need to examine the NP resolution destination and method depending on the location of clients accessing a cluster system and the condition for connecting to an on-premise environment (for example, using a dedicated line). There is no NP resolution destination nor method to recommend. Additionally, you can use network partition resolution resources for NP resolution.

Click **Next**.

Cluster generation wizard

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

Properties Add Remove

NP Resolution List

Type	Target	node-1	node-2
No NP resolutions			

Tuning

Configure network partition (NP) resolution function.
 Click "Add" to add NP resolution resource and select the type.
 For "COM" setting, click each server column cell to configure COM port.
 For "DISK" setting, click each server column cell to configure driver letter of the partition for disk heartbeat.
 For "Ping" setting, click Target column cell to configure IP address of Ping destination, and then click each server column cell to configure "Use" or "Do not use".
 For "HTTP" setting, click Target column cell to configure HTTP packet destination, and then click each server column cell to configure "Use" or "Do not use".
 For "Majority" setting, click each server column cell to configure "Use" or "Do not use".
 For "DISK", "Ping", and "HTTP" settings, the detailed settings can be verified and changed by clicking "Properties".
 Click "Tuning" to configure the actions at NP occurrence.

Back Next Cancel

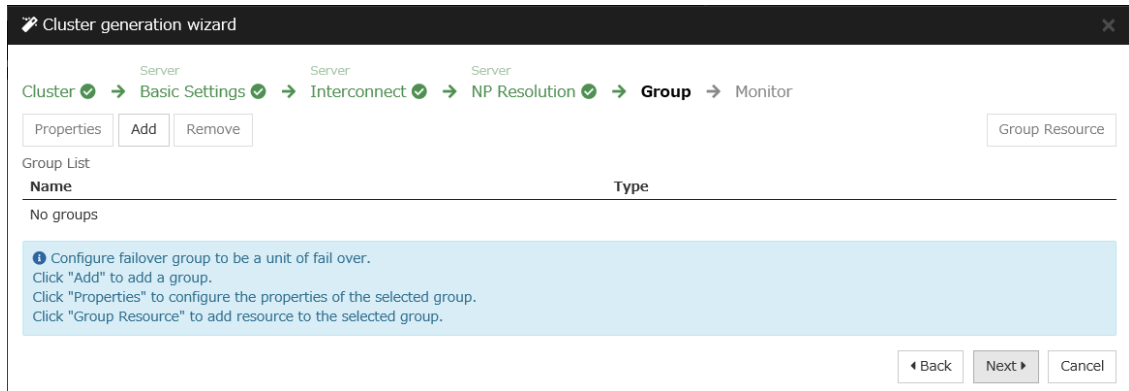
2) **Adding a group resource**

- Defining a group

Create a failover group.

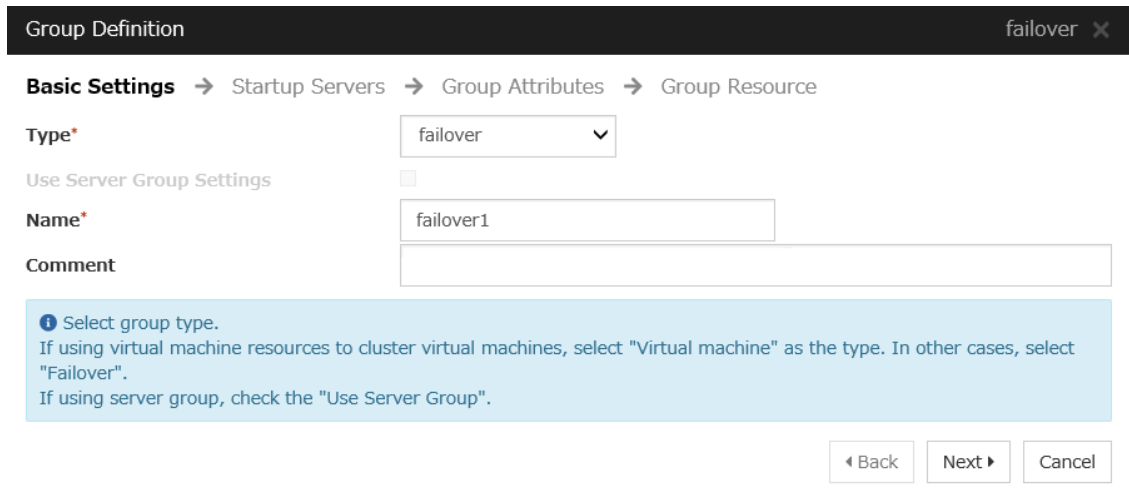
1. The **Group List** window is displayed.

Click **Add**.



2. The **Group Definition** window is displayed.

Specify a failover group name (failover1) for **Name**. Click **Next**.



3. The **Startup Servers** window is displayed.

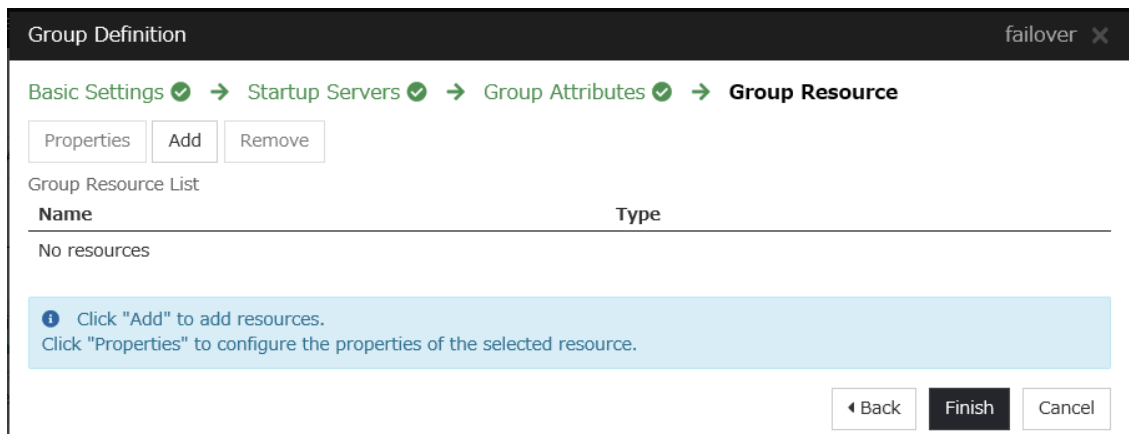
Click **Next** without specifying anything.

4. The **Group Attributes** window is displayed.

Click **Next** without specifying anything.

5. The **Group Resource** window is displayed.

On this page, add a group resource following the procedure below.



- Mirror disk resource

Create a mirror disk resource.

For details, see "Understanding mirror disk resources" in the Reference Guide.

1. Click **Add** on the **Group Resource List** page.
2. The **Resource Definition of Group | failover1** window is displayed.
Select the group resource type (Mirror disk resource) from the **Type** box and enter the group name (md) in the **Name** box. Click **Next**.

Resource Definition of Group | failover1 md ✕

Info → Dependency → Recovery Operation → Details

Type*

Name*

Comment

Select the type of group resource and enter its name.

3. The **Dependency** window is displayed.
Click **Next** without specifying anything.
4. The **Recovery Operation** window is displayed.
Click **Next**.
5. The **Details** window is displayed.
Select a server name in the **Name** column of **Servers that can run the group** and click **Add**.

Resource Definition of Group | failover1 md ✕

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

Mirror Disk No.* 1 ▼

Data Partition Drive Letter*

Cluster Partition Drive Letter*

Cluster Partition Offset Index* 0 ▼

Mirror Disk Connect Select

Servers that can run the group

Name	Data Partition	Cluster Partition

←
Add

→
Remove

Edit

Add Servers that can run the group

Tuning

Name
node-1
node-2

◀ Back
Finish
Cancel

6. The **Selection of partition** dialog box is displayed. Click **Connect**, select the data partition and cluster partition created in "6)Configuring virtual machines", and click **OK**.

Selection of partition

Obtain information

Connect

Data Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	10238MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

Cluster Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	10238MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

OK Cancel

7. Perform steps 5 and 6 for node-1 and then node-2 and click **Finish**.

Resource Definition of Group | failover1 md x

Info ✓ → Dependency ✓ → Recovery Operation ✓ → Details

Mirror Disk No.* 1 ▼

Data Partition Drive Letter* G:

Cluster Partition Drive Letter* F:

Cluster Partition Offset Index* 0 ▼

Mirror Disk Connect Select

Servers that can run the group

Name	Data Partition	Cluster Partition
node-1		
node-2		

Add

Remove

Edit

Tuning

◀ Back Finish Cancel

- Azure DNS resource

Provides a mechanism to register or unregister a record to or from Azure DNS.

For details about the Azure DNS resource, see "Understanding Azure DNS resources" in the Reference Guide.

1. Click **Add** on the **Group Resource List** page.
2. The **Resource Definition of Group | failover1** window is displayed. Select the group resource type (Azure DNS resource) from the **Type** box and enter the group name (azuredns1) in the **Name** box. Click **Next**.

3. The **Dependency** window is displayed. Click **Next** without specifying anything.
4. The **Recovery Operation** window is displayed. Click **Next**.
5. Enter the values for each of the following: **Record Set Name**, **Zone Name**, **IP Address**, **Resource Group Name**, **User URI**, **Tenant ID**, **File Path of Service Principal**, **Azure CLI File Path**. When using the IP address of each server, enter the IP address in the tab for each server. When setting up the servers separately, enter any IP address of the servers in the **Common** tab and then make settings for other servers. For **User URI** and **Tenant ID**, specify respectively the name and tenant you wrote down in "9)Creating a service principal".

Resource Definition of Group | failover1 azuredns X

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

Common node-1 node-2

Record Set Name*	test-record1
Zone Name*	cluster1.zone
IP Address*	10.5.0.120
TTL*	3600 sec
Resource Group Name*	TestGroup1

Account

User URI*	http://azure-test
Tenant ID*	xxxxxxxx-xxxx-xxxx-xxxx-xx
File Path of Service Principal*	C:\Users\testlogin\temp.
Azure CLI File Path*	C:\Program Files (x86)\Micr

Delete a record set at deactivation ☒

Tuning

◀ Back
Finish
Cancel

6. Click **Finish**.

3) Adding a monitor resource

- Azure DNS monitor resource

The mechanism to check the record sets registered to the Azure DNS and whether the name resolution is available is provided.

For details about Azure DNS monitor resources, see "Reference Guide" > "Understanding Azure DNS monitor resources."

Adding one Azure DNS resource creates one Azure DNS monitor resource automatically.

- Custom monitor resource

Sets a script to monitor whether communication with Microsoft Azure Service Management API is possible, and also monitors health of communication with an external network.

For details about the custom monitor resource, see "Understanding custom monitor resources" in the Reference Guide.

1. Click **Add** on the **Monitor Resource List** page.
2. Select the monitor resource type (Custom monitor) from the **Type** box and enter the monitor resource name (genw1) in the **Name** box. Click **Next**.

Monitor Resource Definition
genw ✕

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

Type* Custom monitor ▾

Name* genw1

Comment

Get Licence Info

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

◀ Back
Next ▶
Cancel

3. The **Monitor (common)** window is displayed.
 Confirm that **Monitor Timing** is **Always** and click **Next**.

Monitor Resource Definition
genw ✕

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

Interval* 60 sec

Timeout* 120 sec

Do Not Retry at Timeout Occurrence ☐

Do Not Execute Recovery Action at Timeout Occurrence ☐

Retry Count* 1 time

Wait Time to Start Monitoring* 3 sec

Monitor Timing

☒ Always

☐ Active

Target Resource Browse

Choose servers that execute monitoring Server

◀ Back
Next ▶
Cancel

4. The **Monitor (special)** window is displayed.
 Select **Script created with this product**.
 The following shows the sample of a script to be created.

```
< EXPRESSCLUSTER_installation_path>\bin\clpazure_port_checker -h_
↪management.core.windows.net -p 443
EXIT %ERRORLEVEL%
```

Select **Synchronous** for **Monitor Type**. Click **Next**.

Monitor Resource Definition genw ✕

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

☐ User Application
☒ Script created with this product

File genw.bat Edit View Replace

Monitor Type
☒ Synchronous
☐ Asynchronous

Normal Return Value* 0

Kill the application when exit ☐

Wait for activation monitoring to stop before stopping the cluster ☐

Execution user ▼

◀ Back Next ▶ Cancel

5. The **Recovery Action** window is displayed.

Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final action**.

Monitor Resource Definition genw ✕

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

Recovery Action Execute only the final action ▼

Recovery Target* LocalServer Browse

Recovery Script Execution Count 0 time

Execute Script before Reactivation ☐

Maximum Reactivation Count 0 time

Execute Script before Failover ☐

Execute migration before Failover ☐

Failover Target Server
☒ Stable server
☐ Maximum priority server

Maximum Failover Count 0 time

Execute Script before Final Action ☐

Final Action No operation ▼

Script Settings

◀ Back Finish Cancel

6. Click **Finish** to finish setting.

- IP monitor resource

Creates an IP monitor resource to monitor communication between clusters that are configured with virtual machines, and also to monitor whether communication with an internal network is health.

For details about the IP monitor resource, see "Understanding IP monitor resources" in the Reference Guide.

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

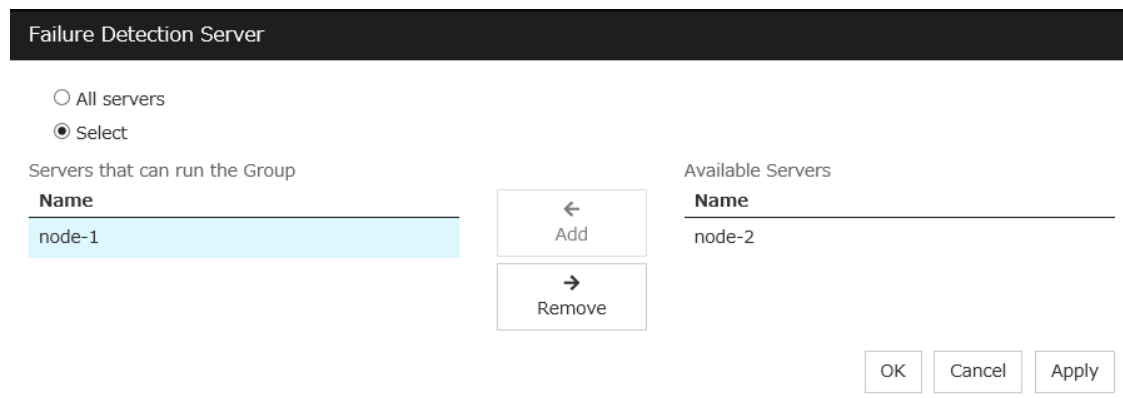
The screenshot shows the 'Monitor Resource Definition' window with the title bar 'ipw X'. The breadcrumb navigation is 'Info → Monitor(common) → Monitor(special) → Recovery Action'. The 'Type' dropdown is set to 'IP monitor'. The 'Name' text box contains 'ipw1'. There is a 'Comment' text box below it.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

3. The **Monitor (common)** window is displayed.
 Confirm that **Monitor Timing** is **Always**.

The screenshot shows the 'Monitor Resource Definition' window with the title bar 'ipw X'. The breadcrumb navigation is 'Info ✓ → Monitor(common) → Monitor(special) → Recovery Action'. The 'Interval' is 60 sec and 'Timeout' is 60 sec. There are checkboxes for 'Do Not Retry at Timeout Occurrence' and 'Do Not Execute Recovery Action at Timeout Occurrence'. 'Retry Count' is 1 time and 'Wait Time to Start Monitoring' is 0 sec. Under 'Monitor Timing', the 'Always' radio button is selected. There is a 'Target Resource' field with a 'Browse' button. At the bottom, there is a 'Choose servers that execute monitoring' field with 'Server' entered. Navigation buttons 'Back', 'Next', and 'Cancel' are at the bottom right.

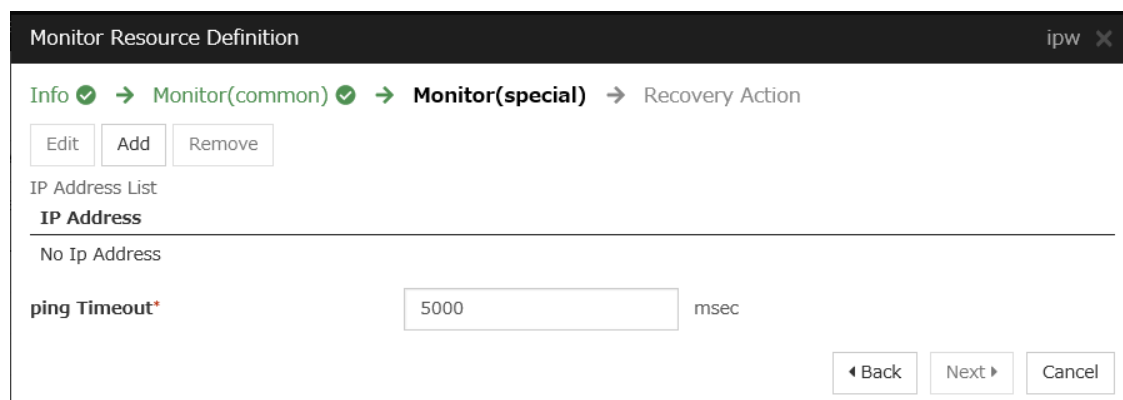
Select one available server for **Choose servers that execute monitoring**.

Click **OK** and click **Next**.



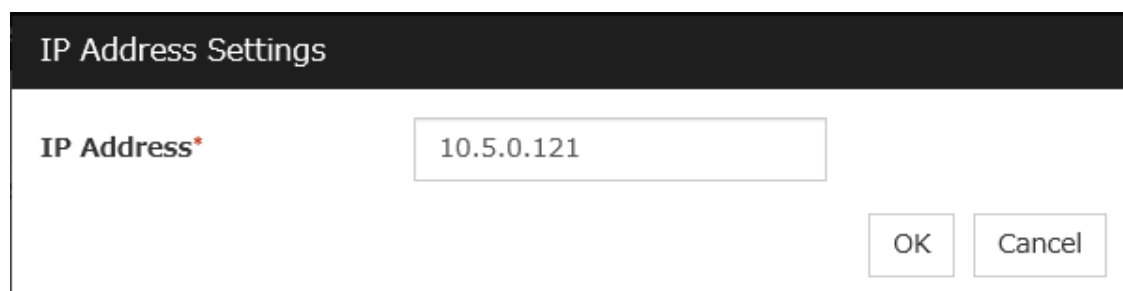
The 'Failure Detection Server' window has a dark header. Below it, there are two radio buttons: 'All servers' and 'Select' (which is selected). Under 'Select', the text 'Servers that can run the Group' is followed by a table with one row: 'node-1'. To the right of this table are two buttons: 'Add' (with a left arrow) and 'Remove' (with a right arrow). Further right, under 'Available Servers', there is a table with one row: 'node-2'. At the bottom right are three buttons: 'OK', 'Cancel', and 'Apply'.

4. The **Monitor (special)** window is displayed.



The 'Monitor Resource Definition' window has a dark header with 'ipw' and a close button. Below the header, there is a breadcrumb trail: 'Info' (with a checkmark) → 'Monitor(common)' (with a checkmark) → 'Monitor(special)' (bold) → 'Recovery Action'. Below this are three buttons: 'Edit', 'Add', and 'Remove'. Under the heading 'IP Address List', there is a table with one row: 'No Ip Address'. Below this, there is a label 'ping Timeout*' followed by a text box containing '5000' and the unit 'msec'. At the bottom right are three buttons: 'Back', 'Next', and 'Cancel'.

On the **Common** tab, select **Add** of **IP Address** and set an IP address of a server other than the server selected in step 3. Click **Next**.



The 'IP Address Settings' window has a dark header. Below it, there is a label 'IP Address*' followed by a text box containing '10.5.0.121'. At the bottom right are two buttons: 'OK' and 'Cancel'.

The screenshot shows the 'Monitor Resource Definition' window with the 'Recovery Action' tab selected. The breadcrumb trail is 'Info' → 'Monitor(common)' → 'Monitor(special)' → 'Recovery Action'. There are 'Edit', 'Add', and 'Remove' buttons. The 'IP Address List' contains one entry: '10.5.0.121'. The 'ping Timeout*' is set to '5000' msec. At the bottom are 'Back', 'Next', and 'Cancel' buttons.

5. The **Recovery Action** window is displayed.

Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final action**.

The screenshot shows the 'Monitor Resource Definition' window with the 'Recovery Action' tab selected. The breadcrumb trail is 'Info' → 'Monitor(common)' → 'Monitor(special)' → 'Recovery Action'. The 'Recovery Action' dropdown is set to 'Execute only the final action'. The 'Recovery Target' is 'LocalServer' with a 'Browse' button. Below are sections for 'Recovery Script Execution Count' (0 time), 'Execute Script before Reactivation' (checkbox), 'Maximum Reactivation Count' (0 time), 'Execute Script before Failover' (checkbox), 'Execute migration before Failover' (checkbox), 'Failover Target Server' (radio buttons for 'Stable server' and 'Maximum priority server'), and 'Maximum Failover Count' (0 time). At the bottom, 'Execute Script before Final Action' is a checkbox, and 'Final Action' is a dropdown set to 'No operation'. There is a 'Script Settings' button and 'Back', 'Finish', and 'Cancel' buttons at the bottom right.

6. Click **Finish** to finish setting.
7. Then, create a monitor resource on the other server. Click **Add** on the **Monitor Resource List** page.
8. Select the monitor resource type (IP monitor) from the **Type** box and enter the monitor resource name (ipw2) in the **Name** box. Click **Next**.
9. The **Monitor (common)** window is displayed.
Confirm that **Monitor Timing** is **Always**.

Select one available server for **Choose servers that execute monitoring**. Click **OK** and Click **Next**.

10. The **Monitor (special)** window is displayed.

On the **Common** tab, select **Add** of **IP Address** and set an IP address of a server other than the server selected in step 9. Click **Next**.

11. The **Recovery Action** window is displayed.

Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final action**.

12. Click **Finish** to finish setting.

- Multi target monitor resource

Creates a multi target monitor resource to check the statuses of the custom monitor resource and IP monitor resource. The custom monitor resource monitors communication to Microsoft Azure Service Management API. The IP monitor resource monitors communication between clusters that are configured with virtual machines.

If their statuses are abnormal, execute the script in which the processing for NP resolution is described.

For details about the multi target monitor resource, see "Understanding multi target monitor resources" in the Reference Guide.

1. Click **Add** on the **Monitor Resource List** page.
2. Select the monitor resource type (Multi target monitor) from the **Type** box and enter the monitor resource name (mtw1) in the **Name** box. Click **Next**.

Monitor Resource Definition mtw X

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

Type* Multi target monitor ▼

Name* mtw1

Comment

Get Licence Info

Select the type of monitor resource and enter its name.

◀ Back Next ▶ Cancel

3. The **Monitor (common)** window is displayed.
Confirm that **Monitor Timing** is **Always** and click **Next**.

The screenshot shows the 'Monitor Resource Definition' window with the 'Monitor(common)' tab selected. The breadcrumb trail is 'Info' (checked) → 'Monitor(common)' → 'Monitor(special)' → 'Recovery Action'. The following settings are visible:

- Interval***: 60 sec
- Timeout***: 60 sec
- Do Not Retry at Timeout Occurrence**: ☐
- Do Not Execute Recovery Action at Timeout Occurrence**: ☐
- Retry Count***: 1 time
- Wait Time to Start Monitoring***: 0 sec
- Monitor Timing**:
 - ☒ Always
 - ☐ Active
- Target Resource**: [Empty text box] Browse
- Choose servers that execute monitoring**: [Server] Server

Navigation buttons at the bottom: ◀ Back, Next ▶, Cancel.

4. The **Monitor (special)** window is displayed.

From **Available Monitor Resources**, select the custom monitor resource (genw1) for checking communication with Service Management API and two IP monitor resources (ipw1 and ipw2) that are set to both servers. Then, click **Add** to add them to **Monitor Resource List**. Click **Next**.

The screenshot shows the 'Monitor Resource Definition' window with the 'Monitor(special)' tab selected. The breadcrumb trail is 'Info' (checked) → 'Monitor(common)' (checked) → 'Monitor(special)' → 'Recovery Action'. The window is divided into two main sections:

- Monitor Resources**: A table with columns 'Monitor Resource' and 'Type'.

Monitor Resource	Type
genw1	genw
ipw1	ipw
ipw2	ipw
- Available Monitor Resources**: A table with columns 'Monitor Resource' and 'Type'.

Monitor Resource	Type
userw	userw

Between the tables are 'Add' (left arrow) and 'Remove' (right arrow) buttons. A 'Tuning' button is located below the 'Monitor Resources' table. Navigation buttons at the bottom: ◀ Back, Next ▶, Cancel.

5. The **Recovery Action** window is displayed.

Specify **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **Stop the cluster service and shutdown OS** for **Final action**.

Monitor Resource Definition

mtw

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

Recovery Action

Execute only the final action

Recovery Target *

LocalServer

Browse

Recovery Script Execution Count

0

time

Execute Script before Reactivation

Maximum Reactivation Count

0

time

Execute Script before Failover

Execute migration before Failover

Failover Target Server

Stable server

Maximum priority server

Maximum Failover Count

0

time

Execute Script before Final Action

Final Action

Stop the cluster service and shutdown OS

Script Settings

Back

Finish

Cancel

6. Click **Finish** to finish setting.

4) **Setting the cluster properties**

For details about the cluster properties, see "Cluster properties" in the Reference Guide.

- Cluster properties

Configure the settings in **Cluster Properties** to link Microsoft Azure and EXPRESSCLUSTER.

- Enter **Config Mode** from Cluster WebUI, click the property icon of the cluster name.

Cluster Name

Cluster1

Comment

Language

English

OK

Cancel

Apply

- Select the **Timeout** tab. For **Timeout** of **Heartbeat**, specify a value calculated by "A+B+C" as described below.
 - A: **Interval** of the monitor resource being monitored by the multi target monitor resource for NP resolution x (**Retry Count**+1)
 - * Among three monitor resources, select the monitor resource whose calculation result is the largest.
 - B: **Interval** of the multi target monitor resource x (**Retry Count**+1)

- C: 30 seconds (Waiting time for heartbeat not to time out before the multi target monitor resource detects an error. The time can be changed accordingly.

Note: If **Timeout of Heartbeat** is shorter than the time that the multi target monitor resource requires to detect an error, a heartbeat timeout will be detected before starting the NP resolution processing. In this case, the same service may start doubly in the cluster because the service also starts on the standby server.

Network initialization complete wait time*	3	min
Server Sync Wait Time*	5	min
Heartbeat		
Interval*	3	sec
Timeout*	270	sec
Server Internal Timeout*	180	sec
<input type="button" value="Initialize"/>		
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>		

3. Click **OK**.

5) Applying the settings and starting the cluster

1. Click **Apply the Configuration File** in the config mode of Cluster WebUI.
 A popup message asking "Do you want to perform the operations?" is displayed. Click **OK**.
 When the upload ends successfully, a popup message saying "The application finished successfully." is displayed. Click **OK**.
 If the upload fails, perform the operations by following the displayed message.
2. Select the **Operation Mode** on the drop down menu of the toolbar in Cluster WebUI to switch to the operation mode. Select **Start Cluster** in the **Status** tab of Cluster WebUI and click.
3. Confirm that a cluster system starts and the status of the cluster is displayed to the Cluster WebUI.
 If the cluster system does not start normally, take action according to an error message.

For details, refer to the following:

Installation and Configuration Guide
 -> How to create a cluster

4.4 Verifying the created environment

Verify whether the created environment works properly by generating a monitoring error to fail over a failover group.

If the cluster is running normally, the verification procedure is as follows:

1. Start the failover group (failover1) on the active node (node-1). In the Status tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node-1 is **Normal**.
2. Log in to the Microsoft Azure portal, select cluster1.zone on the **DNS zone** blade, and then select **Summary**. Check the DNS servers displayed on the upper right of the window (name server 1, name server 2, name server 3, and name server 4 in the window example).
3. Confirm that the relevant record set exists in the DNS servers checked in the above step by executing the nslookup command as follows:

```
nslookup test-record1.cluster1.zone <DNS_servers_checked_in_the_above_
↪step>
```

4. On the Microsoft Azure portal, delete an A record from the DNS zone. This causes azurednsw1 to detect a monitoring error. On the **DNS zone** blade, select cluster1.zone and then **Summary**.
5. Select the record you want to delete and click **Delete**. When the deletion confirmation dialog box is displayed, select **Yes**.
6. When the time specified for **Interval** of azurednsw1 elapses, the failover group (failover1) enters an error status and fails over to node-2. In the Status tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node-2 is **Normal**.
7. Confirm that the relevant record set exists in the DNS servers checked in the above step by executing the nslookup command as follows:

```
nslookup test-record1.cluster1.zone <DNS_servers_checked_in_the_above_
↪step>
```

Verifying the failover operation when an A record is deleted from the DNS server is now complete.

Verify the operations in case of other failures if necessary.

CLUSTER CREATION PROCEDURE (FOR AN HA CLUSTER USING A PUBLIC LOAD BALANCER)

5.1 Creation example

This guide introduces the procedure for creating a 2-node unidirectional standby cluster using EXPRESSCLUSTER on Microsoft Azure. This procedure is intended to create a mirror disk type configuration in which node-1 is used as an active server.

The following tables describe the parameters that do not have a default value and the parameters whose values are to be changed from the default values.

- Microsoft Azure settings (common to node-1 and node-2)

Setting item	Setting value
Resource group setting	
Resource group	TestGroup1
Region	(Asia Pacific) Japan East
Virtual network setting	
Name	Vnet1
Address space	10.5.0.0/24
Subnet Name	Vnet1-1
Subnet Address range	10.5.0.0/24
Resource group	TestGroup1
Location	(Asia Pacific) Japan East
Load balancer setting	
Name	TestLoadBalancer
Type	Public
Public IP address name	TestLoadBalancerPublicIP
Public IP address: Assignment	Static
Resource group	TestGroup1
Region	(Asia Pacific) Japan East
Backend pool: Name	TestBackendPool
Associated to	Availability set
Target virtual machine	node-1 node-2

Continued on next page

Table 5.1 – continued from previous page

Setting item	Setting value
Network IP configuration	10.5.0.120 10.5.0.121
Health probe: Name	TestHealthProbe
Health probe: Port	26001
Load balancing rule: Name	TestLoadBalancingRule
Load balancing rule: Port	80 (Port number offering the operation)
Load balancing rule: Backend port	8080 (Port number offering the operation)
Inbound security rule setting	
Name	TestHTTP
Protocol	TCP
Destination Port range	8080 (Port number offering the operation)

- Microsoft Azure settings (specific to each of node-1 and node-2)

Setting item	Setting value	
	node-1	node-2
Virtual machine setting		
– Disk type	Standard HDD	
– User name	testlogin	
– Password	PassWord_123	
– Resource group	TestGroup1	
– Region	(Asia Pacific) Japan East	
Network security group setting		
– Name	node-1-nsg	node-2-nsg
Availability set setting		
– Name	AvailabilitySet-1	
– Update domains	5	
– Fault domains	2	
Diagnostics storage account setting		
– Name	Automatically generated	
– Performance	Standard	
– Replication	Locally-redundant storage (LRS)	
IP configuration setting		
– IP address	10.5.0.120	10.5.0.121
Disk setting		
– Name	node-1_DataDisk_0	node-2_DataDisk_0
– Source type	None (empty disk)	
– Account type	Standard HDD	
– Size	20	

- EXPRESSCLUSTER settings (cluster properties)

Setting item	Setting value	
	node-1	node-2
– Cluster Name	Cluster1	
– Server Name	node-1	node-2
– Timeout Tab: Heartbeat timeout	210	

- EXPRESSCLUSTER settings (failover group)

Resource name	Setting item	Setting value
Mirror disk resource	Name	md
	Details Tab: Data Partition Drive Letter	G:
	Details Tab: Cluster Partition Drive Letter	F:
Azure probe port resource	Name	azurepp1
	Probe port	26001 (Value specified for Port of Health probe)

- EXPRESSCLUSTER settings (monitor resource)

Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	Name	mdw1
Azure probe port monitor resource	Name	azureppw1
	Recovery Target	azurepp1
Azure load balance monitor resource	Name	aurelbw1
	Recovery Target	azurepp1
Custom monitor resource	Name	genw1
	Script created with this product	On
	Monitor Type	Synchronous
	Normal Return Value	0
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
IP monitor resource	Name	ipw1
	Server to monitor	node-1
	IP address	10.5.0.121
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
IP monitor resource	Name	ipw2
	Server to monitor	node-2
	IP address	10.5.0.120
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
Multi target monitor resource	Name	mtw1

Continued on next page

Table 5.3 – continued from previous page

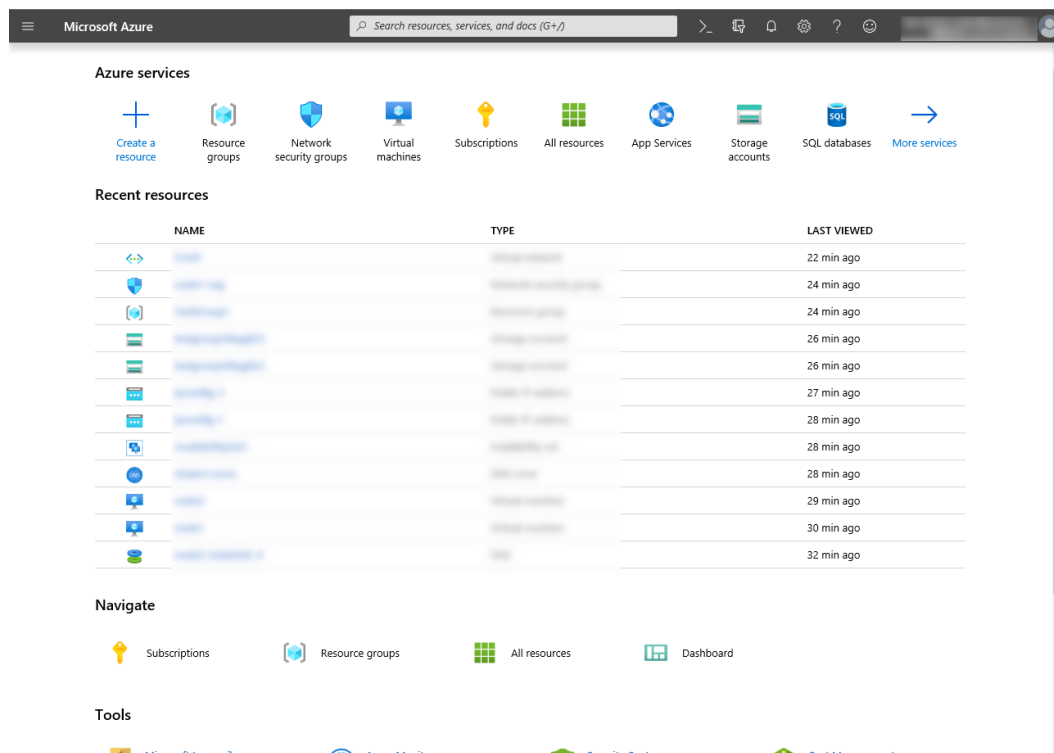
Monitor resource name	Setting item	Setting value
	Monitor resource list	genw1 ipw1 ipw2
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
	Execute Script before Final Action	On
	Timeout	30

5.2 Configuring Microsoft Azure

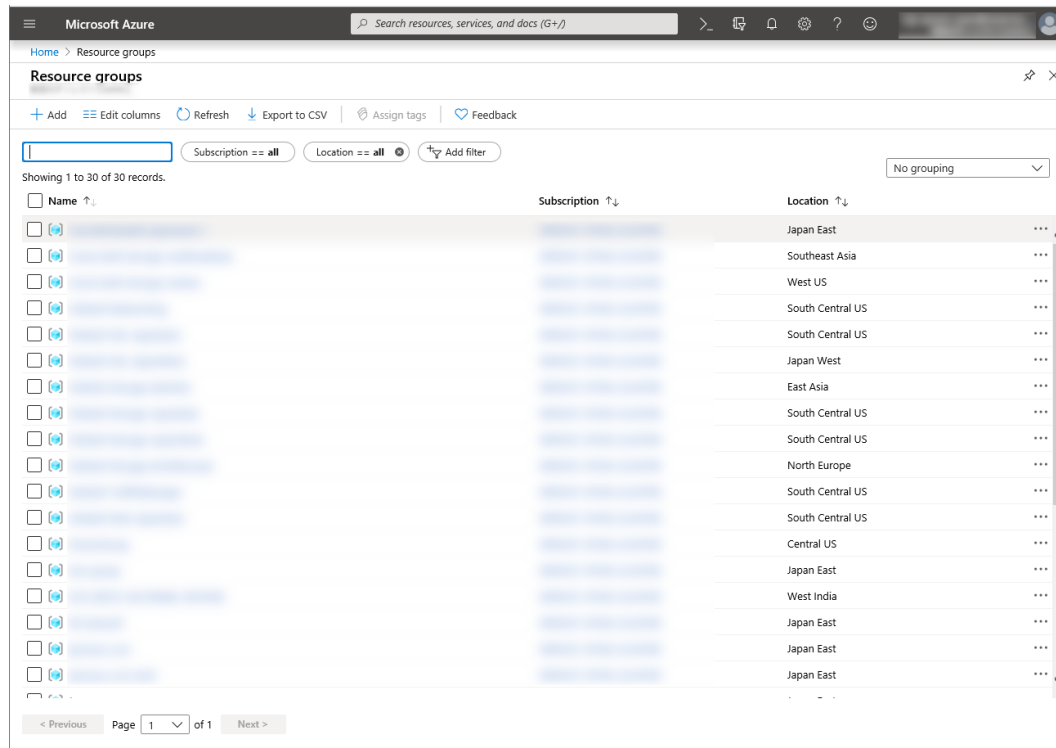
1. Creating a resource group

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create a resource group following the steps below.

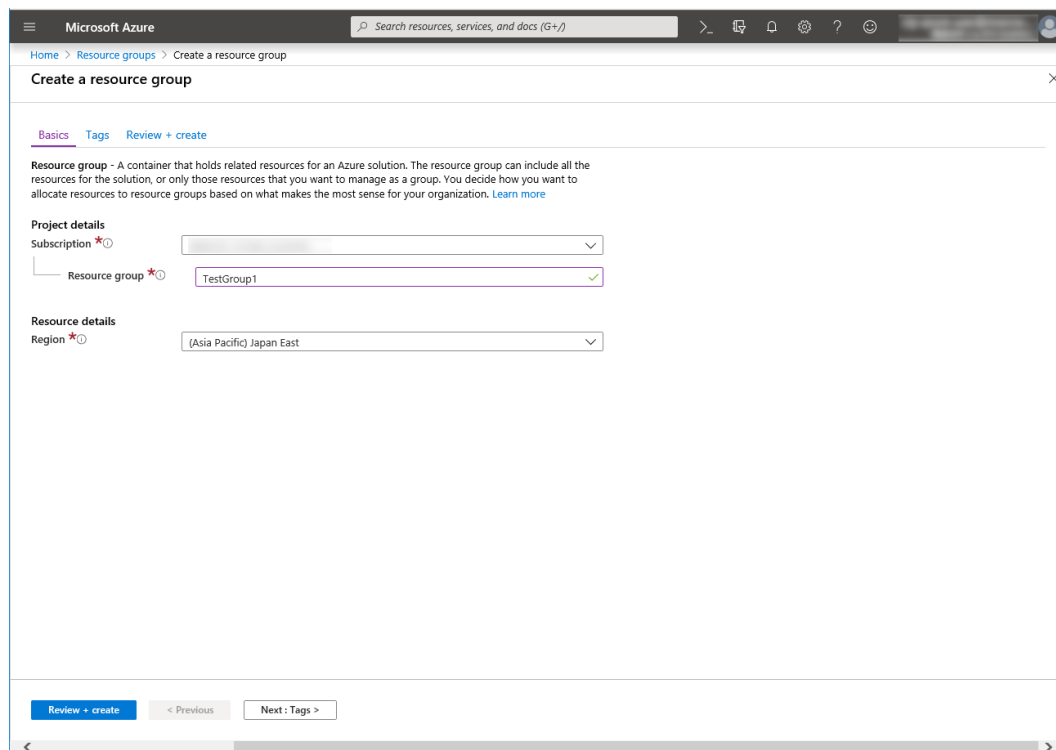
1. Select **Resource groups** on the upper part of the window. If there are existing resource groups, they are displayed in a list.



2. Select **+Add** on the upper part of the window.



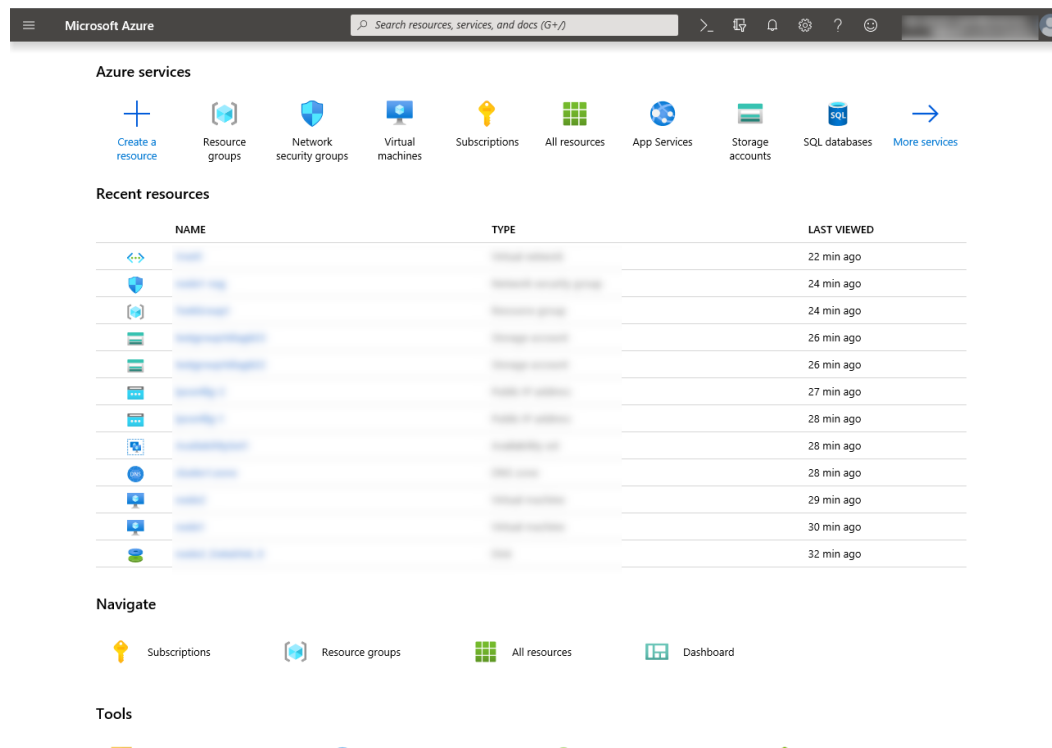
3. Specify **Subscription**, **Resource group**, and **Region**, and click **Review+Create**.



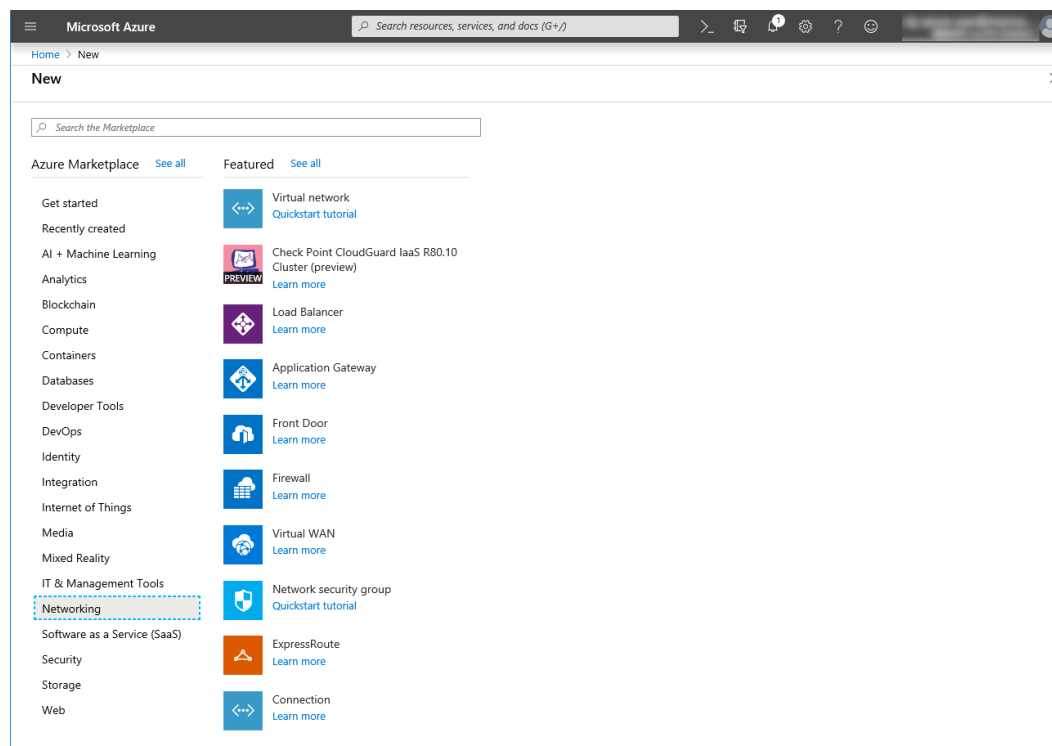
2. Creating a virtual network

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create a virtual network following the steps below.

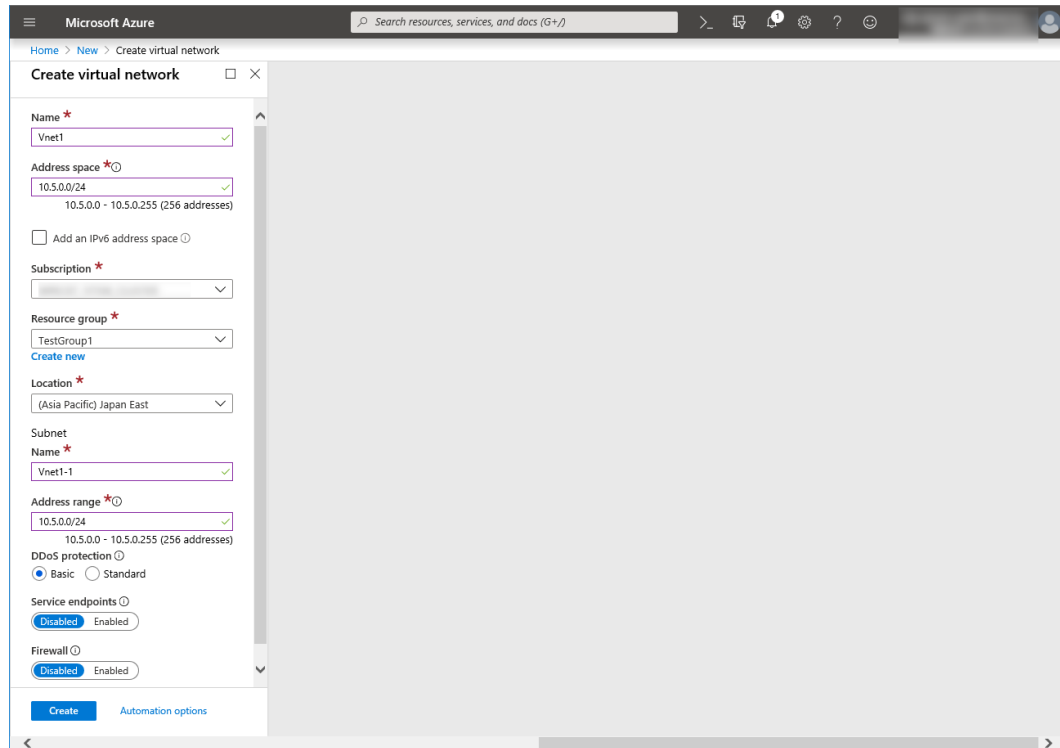
1. Select **Create a resource** on the upper part of the window.



2. Select **Networking** and then **Virtual network**.



3. Specify **Name**, **Address space**, **Subscription**, **Resource group**, **Location**, **Name of Subnet**, and **Address range**, and click **Create**.

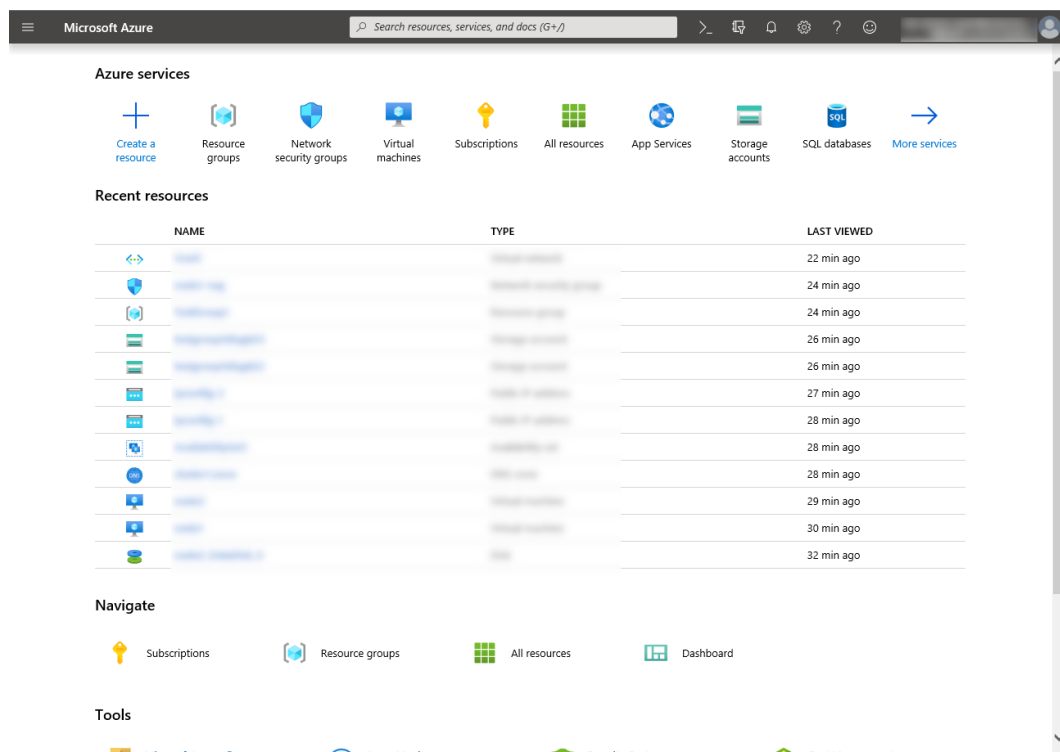


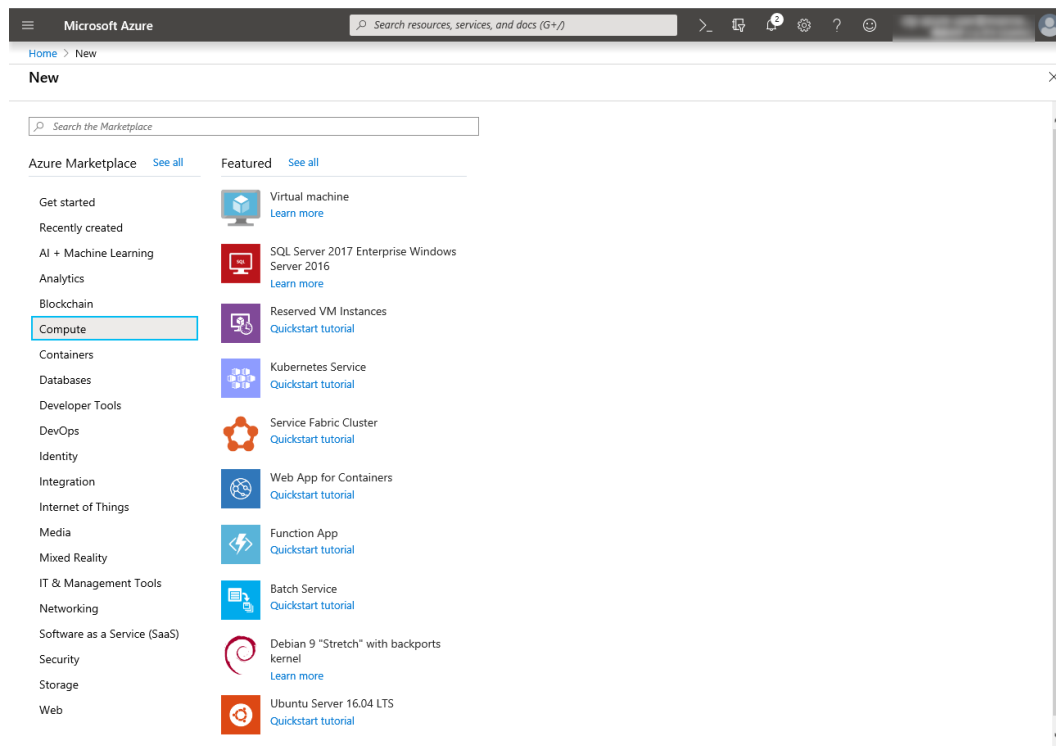
3. Creating a virtual machine

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create virtual machines and disks following the steps below.

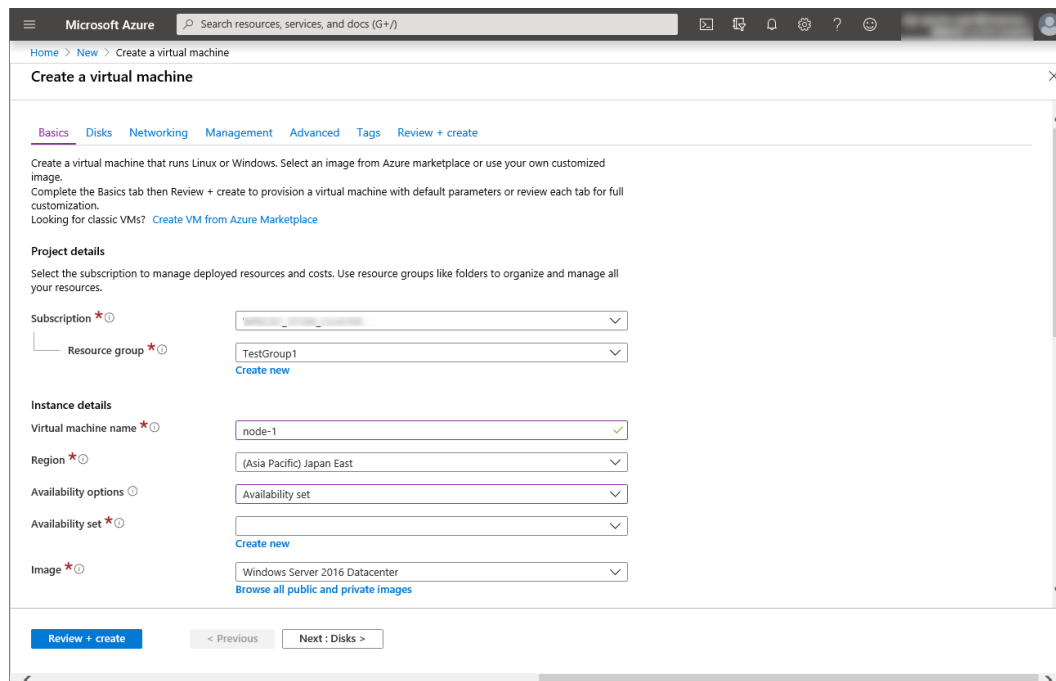
Create as many virtual machines as required to create a cluster. Create node-1 and then node-2.

1. Select **Create a resource** on the upper part of the window.



2. Select **Compute** and then **See all**.3. Select **Windows Server 2016 Datacenter**.

4. When the **Basics** tab appears, specify the settings of **Subscription**, **Resource group**, **Virtual machine name**, **Region**, **Image**, **Size**, **Username**, **Password**, and **Confirm password**. Select **Availability set** from **Availability options**, and click **Create new** under the **Availability set** field. When the **Create new** blade appears, specify the settings of **Name**, **Fault domains**, and **Update domains**. Then click **OK**.



Click **Change size** to display the **Select a VM size** blade.

From the list, choose a size (**A1 - Standard** in this guide) suitable for your virtual machine and click **Select**.

Regarding the **Virtual machine name**, node-1 is for node-1, and node-2 is for node-2.

Click **Next: Disks >**

- When the **Disks** tab appears, go through the following steps to add a disk to be used for a mirror disk (cluster partition or data partition).

From the **DATA DISKS** list, click **Create and attach a new disk**.

Microsoft Azure Search resources, services, and docs (G+/I)

Home > New > Create a virtual machine

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type *

Enable Ultra Disk compatibility ☐ Yes ☒ No

Ultra Disk compatibility is not available for this VM size and location.

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
Create and attach a new disk Attach an existing disk				

Advanced

[Review + create](#) [< Previous](#) [Next: Networking >](#)

6. The **Create a new disk** blade appears.
- Specify **Name**, **Source type**, and **Size**. Then click **OK**.
- Click **Next: Networking >**.

Microsoft Azure Search resources, services, and docs (G+/I)

Home > New > Create a virtual machine > Create a new disk

Create a new disk

Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions. [Learn more about Azure Managed Disks](#)

Name *

Source type *

Size *
Standard HDD
[Change size](#)

[OK](#)

7. The **Networking** tab appears.
- Specify the settings of **Virtual network**, **Subnet**, **Network security group**, and **Configure network security group**.
- Click **Create new** under the **Configure network security group** field to display the **Create network security group** blade. Specify the setting of **Name** and then click **OK**.
- Click **Next: Management >**

The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal, specifically the 'Networking' tab. The page title is 'Create a virtual machine'. Below the title are tabs for 'Basics', 'Disks', 'Networking' (selected), 'Management', 'Advanced', 'Tags', and 'Review + create'. The main content area is titled 'Network interface' and contains the following settings:

- Virtual network ***: A dropdown menu showing 'Vnet1' with a 'Create new' link below it.
- Subnet ***: A dropdown menu showing 'Vnet1-1 (10.5.0.0/24)' with a 'Manage subnet configuration' link below it.
- Public IP**: A dropdown menu showing 'None' with a 'Create new' link below it.
- NIC network security group**: Radio buttons for 'None', 'Basic', and 'Advanced' (selected).
- Configure network security group ***: A dropdown menu showing '(new) node-1-nsg' with a 'Create new' link below it.
- Accelerated networking**: Radio buttons for 'On' and 'Off' (selected). A note below states: 'The selected VM size does not support accelerated networking.'
- Load balancing**: A section with a description and a 'Learn more' link.

At the bottom, there are three buttons: 'Review + create' (in blue), '< Previous', and 'Next : Management >'.

8. The **Management** tab appears.

Click **Create new** under the **Diagnostics storage account** field to display the **Create storage account** blade.

Specify the settings of **Name**, **Account kind**, and **Replication**. Then click **OK**.

In the **Diagnostics storage account** field, the default value is automatically generated and entered.

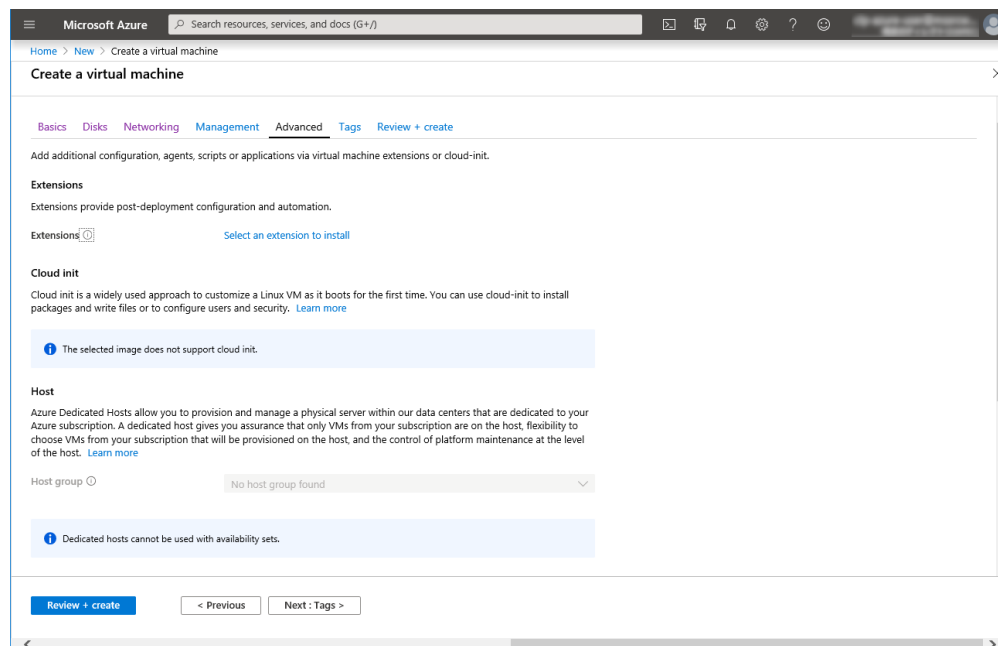
Click **Next: Advanced >**.

The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal, specifically the 'Management' tab. The page title is 'Create a virtual machine'. Below the title are tabs for 'Basics', 'Disks', 'Networking', 'Management' (selected), 'Advanced', 'Tags', and 'Review + create'. The main content area is titled 'Configure monitoring and management options for your VM.' and contains the following settings:

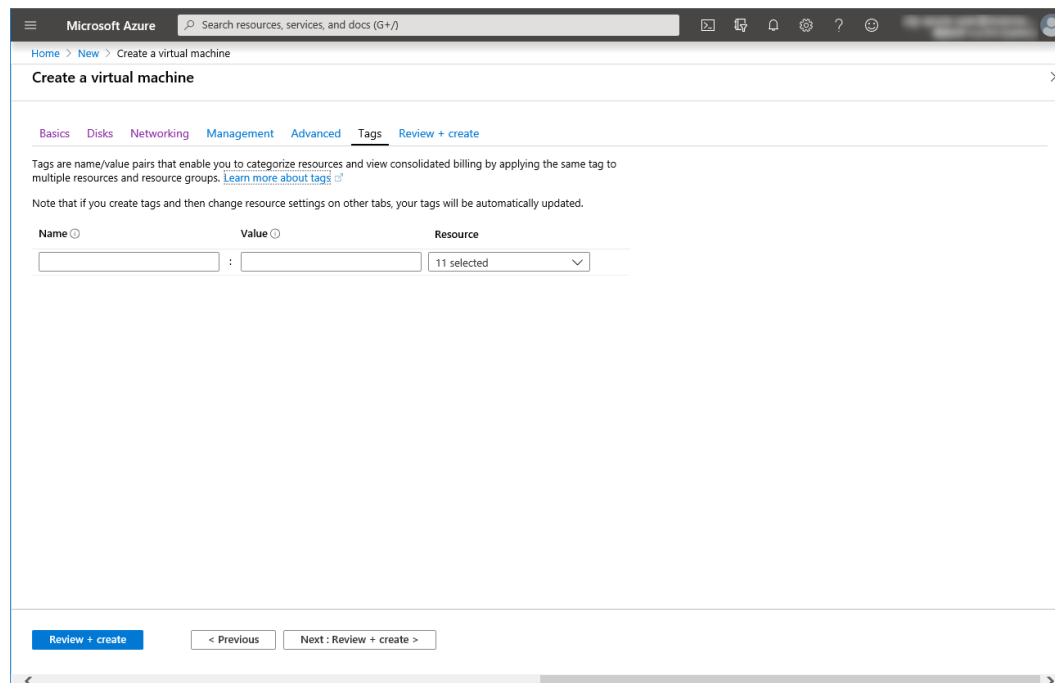
- Azure Security Center**: A section with a description and a 'Learn more' link. Below it, a green checkmark indicates 'Your subscription is protected by Azure Security Center basic plan.'
- Monitoring**:
 - Boot diagnostics**: Radio buttons for 'On' (selected) and 'Off'.
 - OS guest diagnostics**: Radio buttons for 'On' and 'Off' (selected).
 - Diagnostics storage account ***: A dropdown menu showing 'testgroup1diag600' with a 'Create new' link below it.
- Identity**:
 - System assigned managed identity**: Radio buttons for 'On' and 'Off' (selected).
- Azure Active Directory**:
 - Login with AAD credentials (Preview)**: Radio buttons for 'On' and 'Off' (selected).

At the bottom, there are three buttons: 'Review + create' (in blue), '< Previous', and 'Next : Advanced >'.

9. Click **Next: Tags >**.



10. Click **Next: Review + create** >.

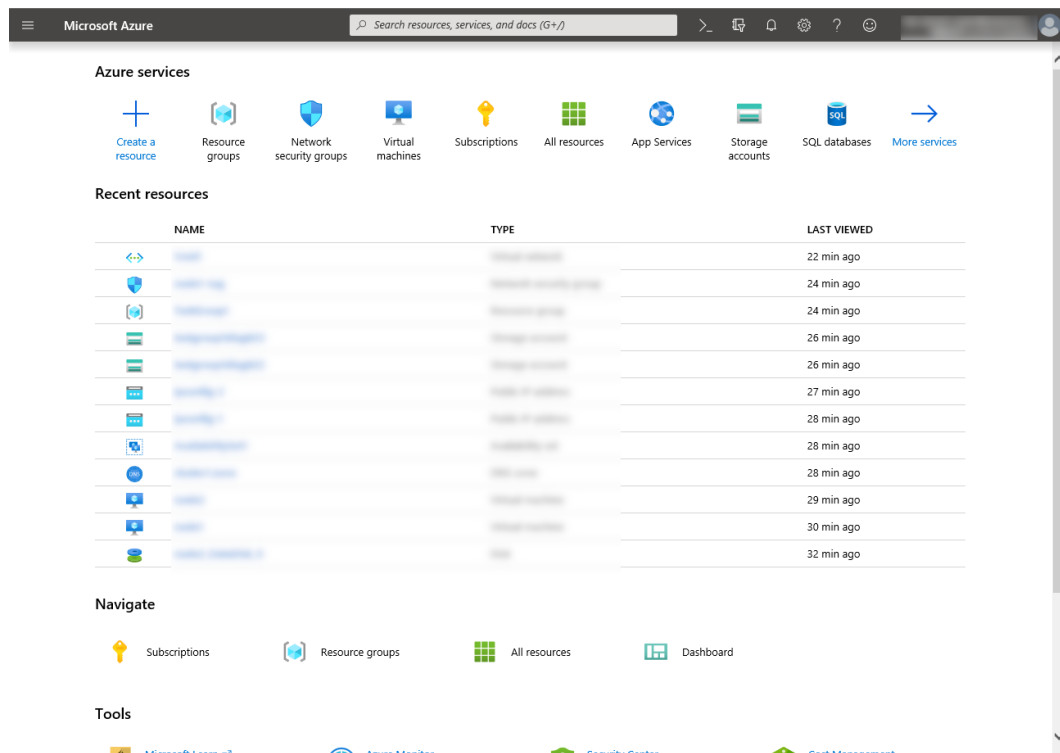


11. The **Review + create** tab appears. Check the contents. If there is no problem, click **Create**. The deployment starts and takes several minutes.

4. Setting a private IP address

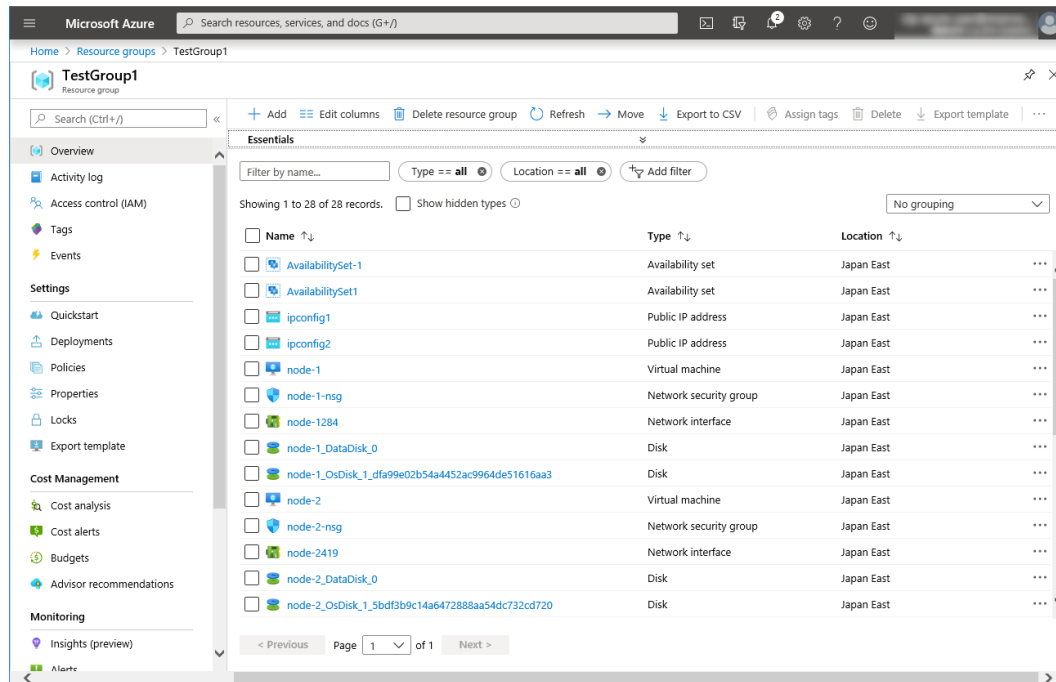
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and change the private IP address setting following the steps below. Since an IP address is initially set to be assigned dynamically, change the setting so that an IP address is assigned statically. Change the settings of node-1 and then node-2.

1. Select **Resource groups** on the upper part of the window.

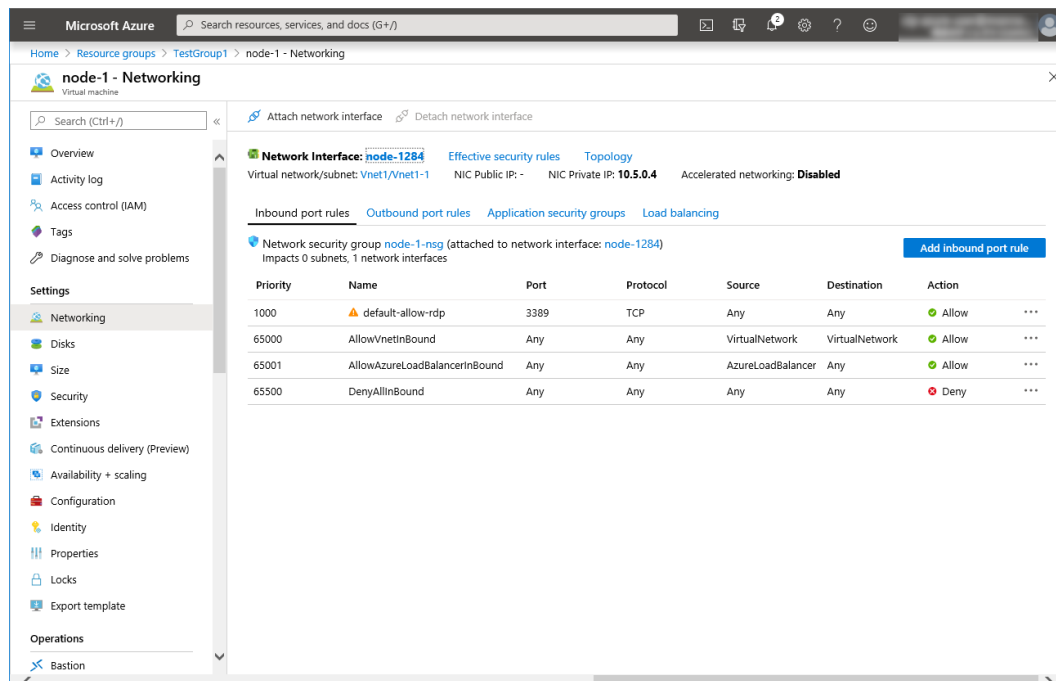


2. Select TestGroup1 from the resource group list.

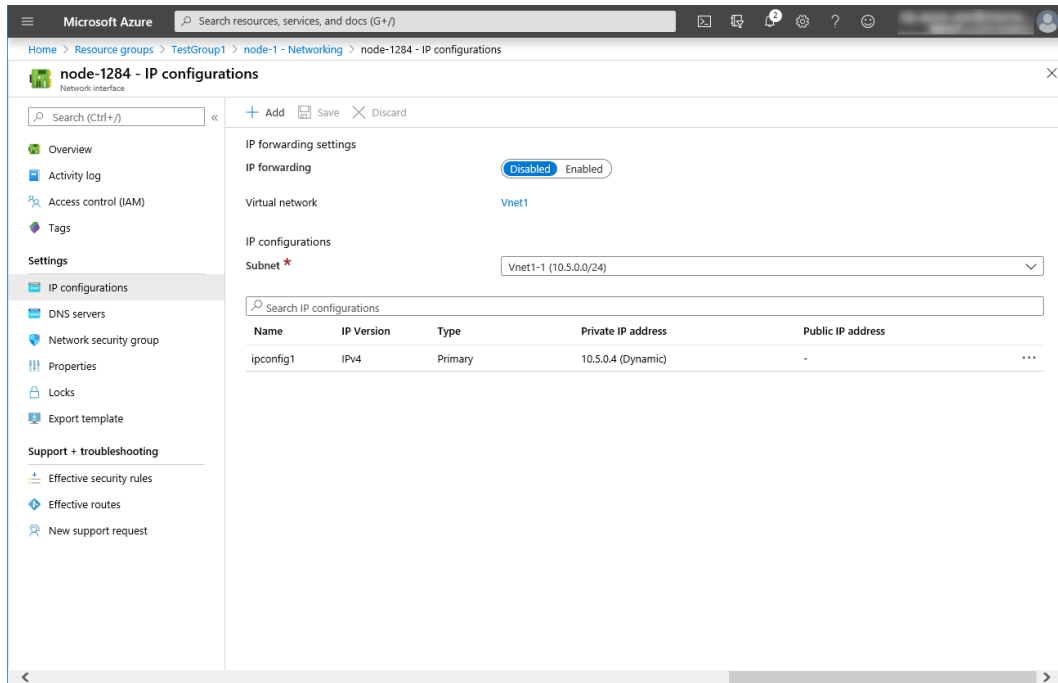
3. The summary of TestGroup1 is displayed. Select virtual machine node-1 or node-2 from the item list.



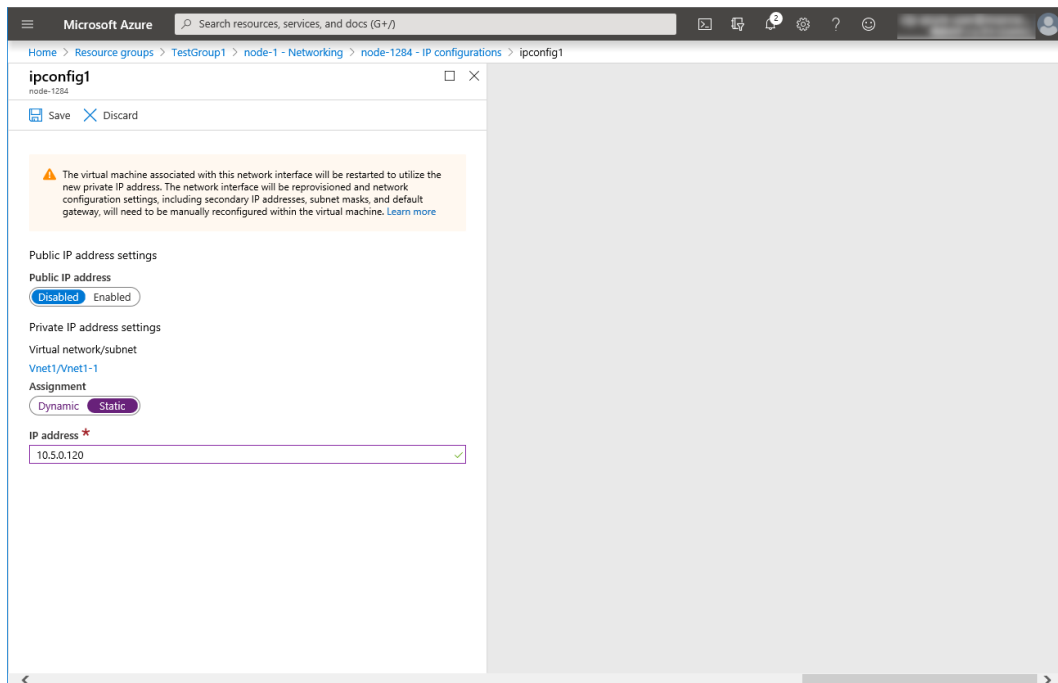
4. Select **Networking**.



5. Select a network interface displayed in the list. The network interface name is generated automatically.
6. Select **IP configurations**.



7. Only ipconfig1 is displayed in the list. Select it.
8. Select **Static** for **Assignment** under **Private IP address settings**. Enter the IP address to be assigned statically in the **IP address** text box and click **Save** at the top of the window. The IP address of node-1 is 10.5.0.120. The IP address of node-2 is 10.5.0.121.

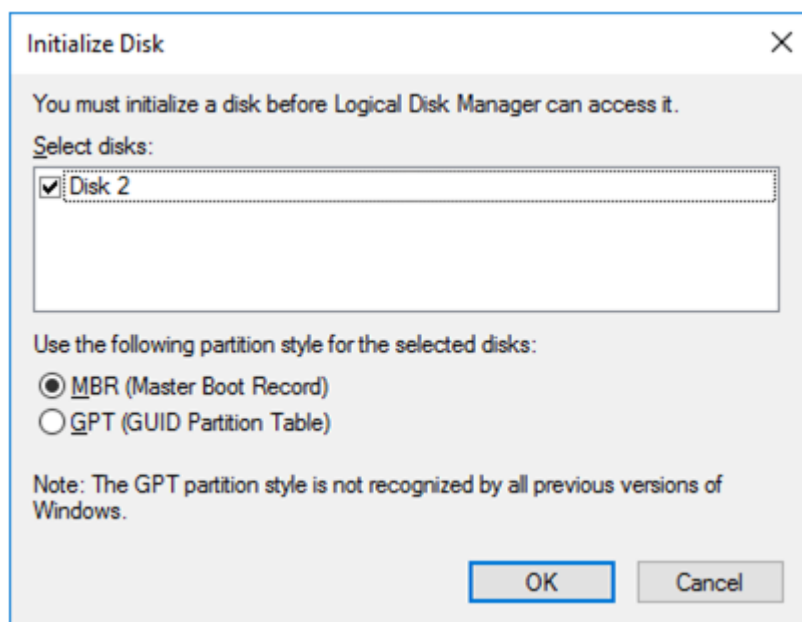


9. The virtual machines restart automatically so that new private IP addresses can be used.
5. **Configuring virtual machines**
- Log in to the created node-1 and node-2 and specify the settings following the procedure below.

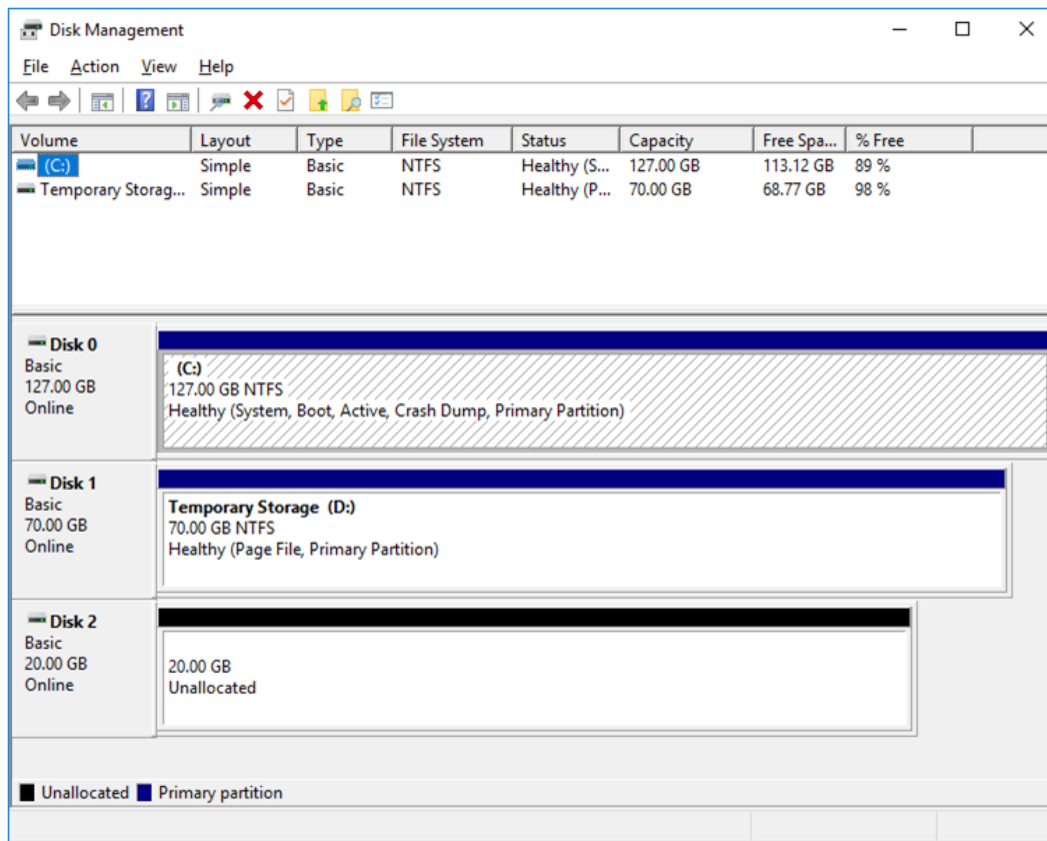
Set a partition for the mirror disk resource. Create a file system in the added disk.

For details about a partition for the mirror disk resource, see "Partition settings for mirror disk resource (when using Replicator)" in "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.

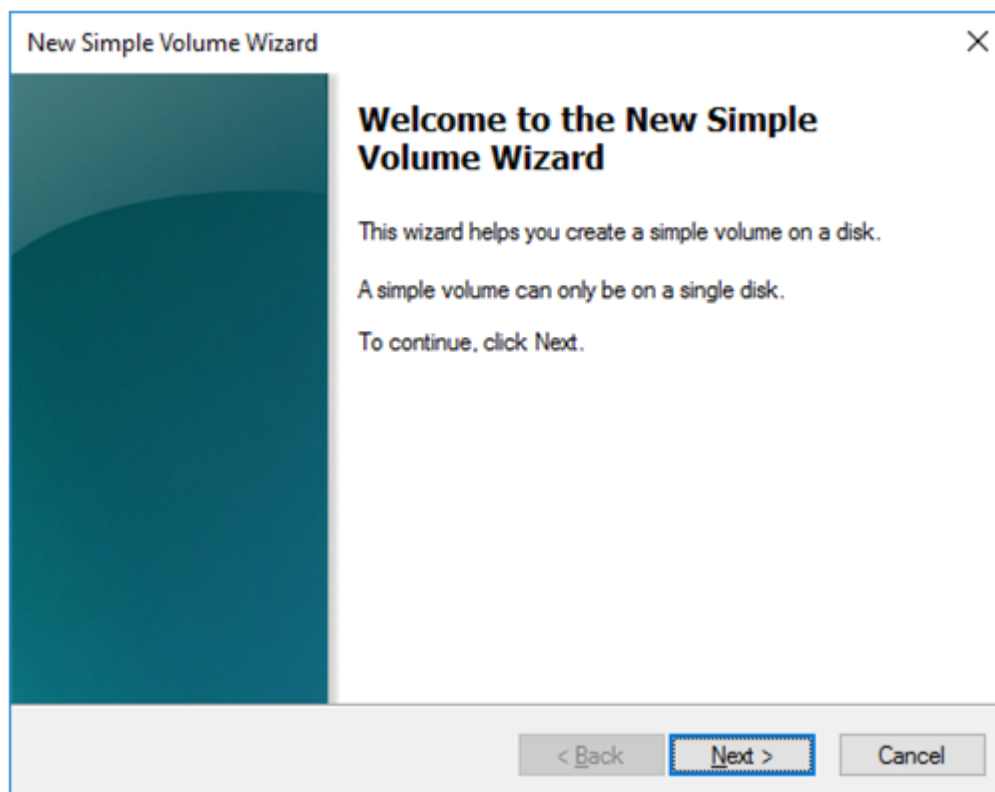
1. Open the **Disk Management** window. The **Initialize Disk** dialog box is displayed.



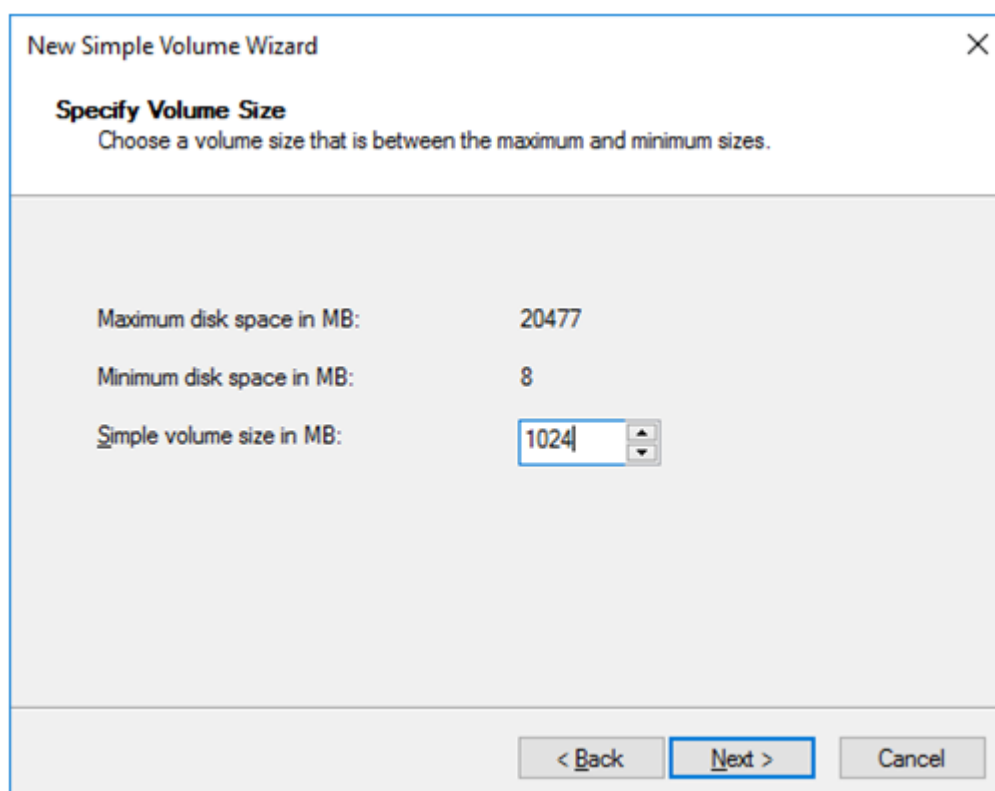
2. Confirm that the added disk is displayed as "Disk 2" in unassigned state under the existing C drive and D drive.



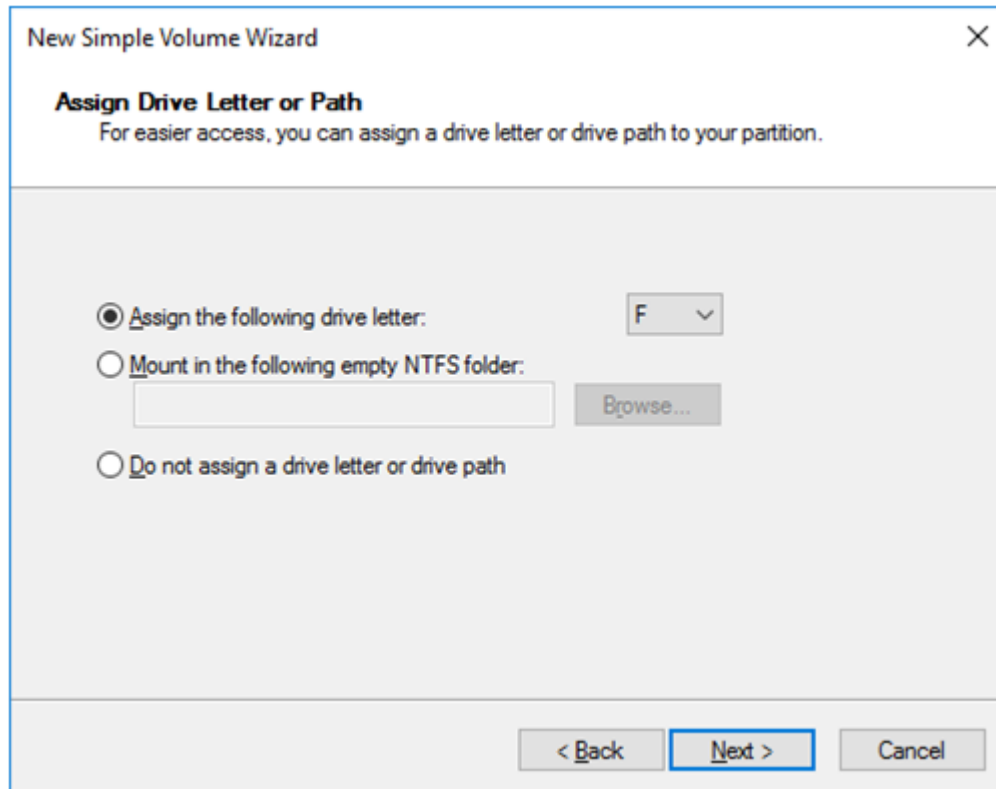
3. Create a cluster partition. Right-click "Disk 2" and select **New Simple Volume**.
4. The **Welcome to the New Simple Volume Wizard** is displayed. Click **Next**.



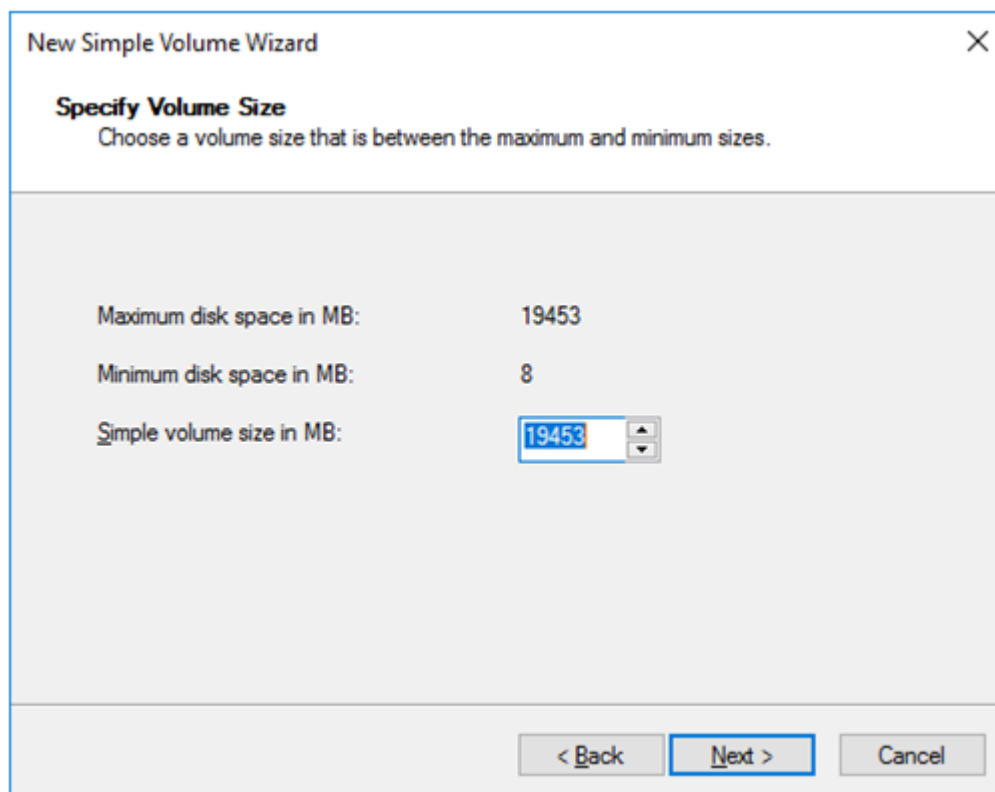
5. The **Specify Volume Size** window is displayed. Allocate 1024 MB (1,073,741,824 bytes) or more to a cluster partition. Click **Next**.



6. The **Assign Drive Letter or Path** window is displayed. Select the F drive for **Assign the following drive letter:.** Use the disk as a raw partition without formatting.



7. Next, create a data partition. Right-click "Disk 2" and select **New Simple Volume**.
8. The **Welcome to the New Simple Volume Wizard** is displayed. Click **Next**.
9. The **Specify Volume Size** window is displayed. Click **Next**.



The screenshot shows the 'New Simple Volume Wizard' window at the 'Specify Volume Size' step. The window title is 'New Simple Volume Wizard' with a close button (X) in the top right corner. Below the title bar, the text 'Specify Volume Size' is followed by the instruction 'Choose a volume size that is between the maximum and minimum sizes.' The main area contains three labels and their corresponding values: 'Maximum disk space in MB:' with the value '19453', 'Minimum disk space in MB:' with the value '8', and 'Simple volume size in MB:' with a text box containing '19453' and a spinner control. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

New Simple Volume Wizard

Specify Volume Size
Choose a volume size that is between the maximum and minimum sizes.

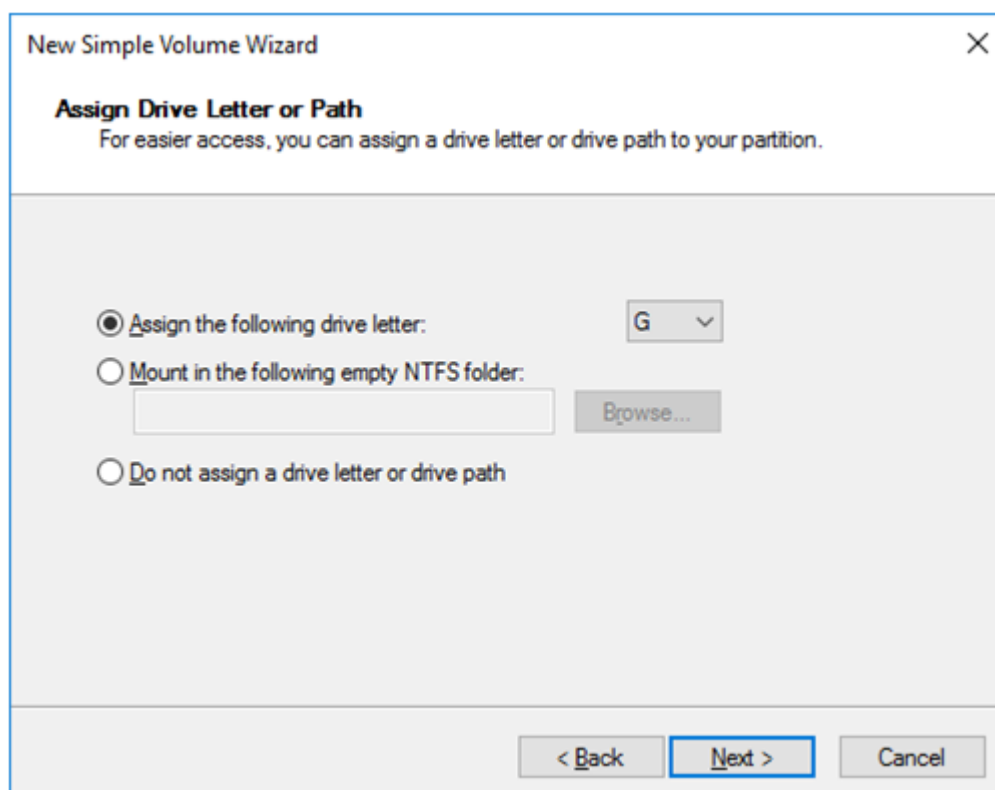
Maximum disk space in MB: 19453

Minimum disk space in MB: 8

Simple volume size in MB: 19453

< Back Next > Cancel

10. The **Assign Drive Letter or Path** window is displayed. Select the G drive for **Assign the following drive letter:** and click **Next**.



The screenshot shows the 'New Simple Volume Wizard' window at the 'Assign Drive Letter or Path' step. The window title is 'New Simple Volume Wizard' with a close button (X) in the top right corner. Below the title bar, the text 'Assign Drive Letter or Path' is followed by the instruction 'For easier access, you can assign a drive letter or drive path to your partition.' The main area contains three radio button options: 'Assign the following drive letter:' (selected) with a dropdown menu showing 'G', 'Mount in the following empty NTFS folder:' with a text box and a 'Browse...' button, and 'Do not assign a drive letter or drive path'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

New Simple Volume Wizard

Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.

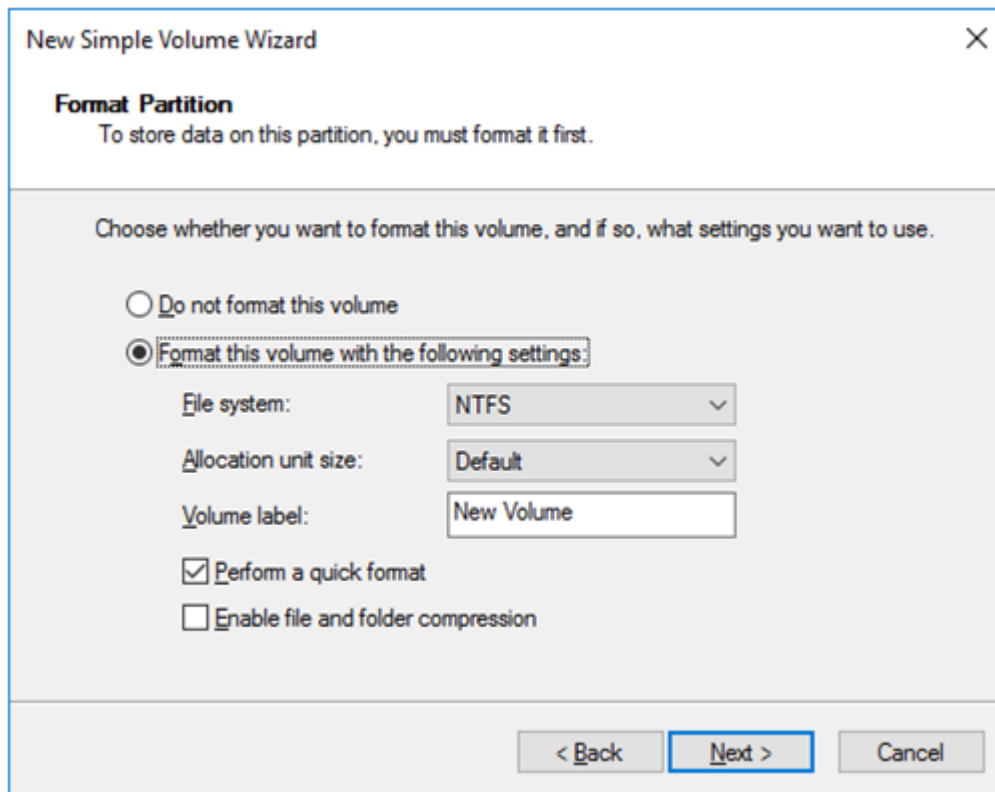
☒ Assign the following drive letter: G

☐ Mount in the following empty NTFS folder: Browse...

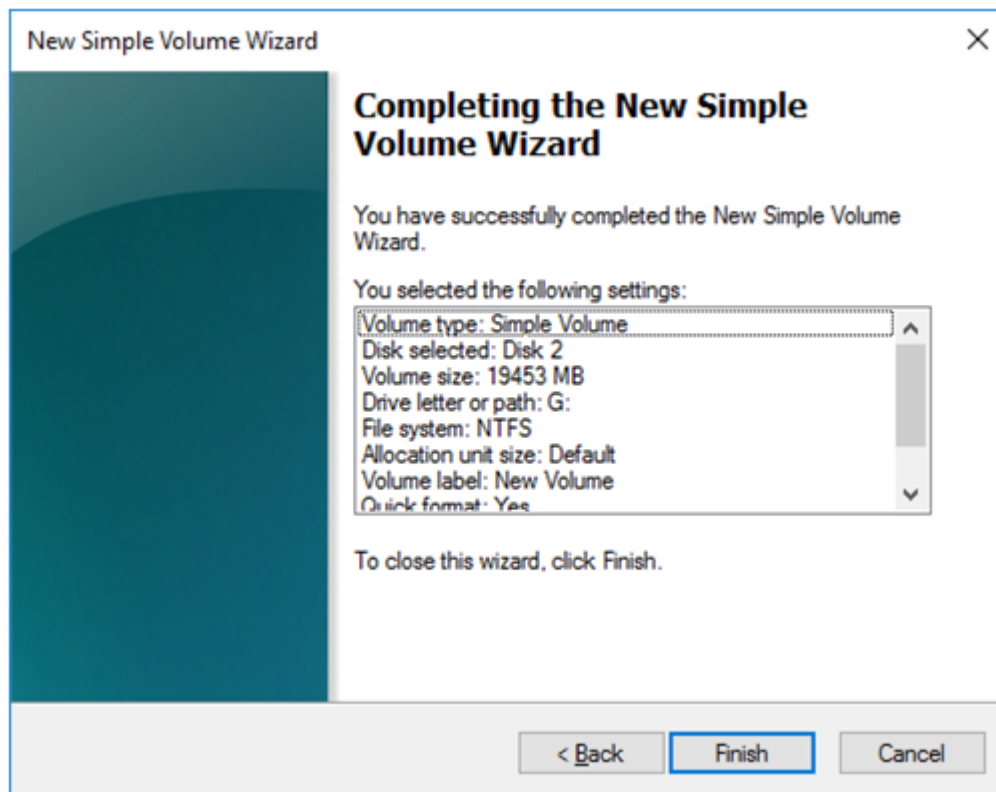
☐ Do not assign a drive letter or drive path

< Back Next > Cancel

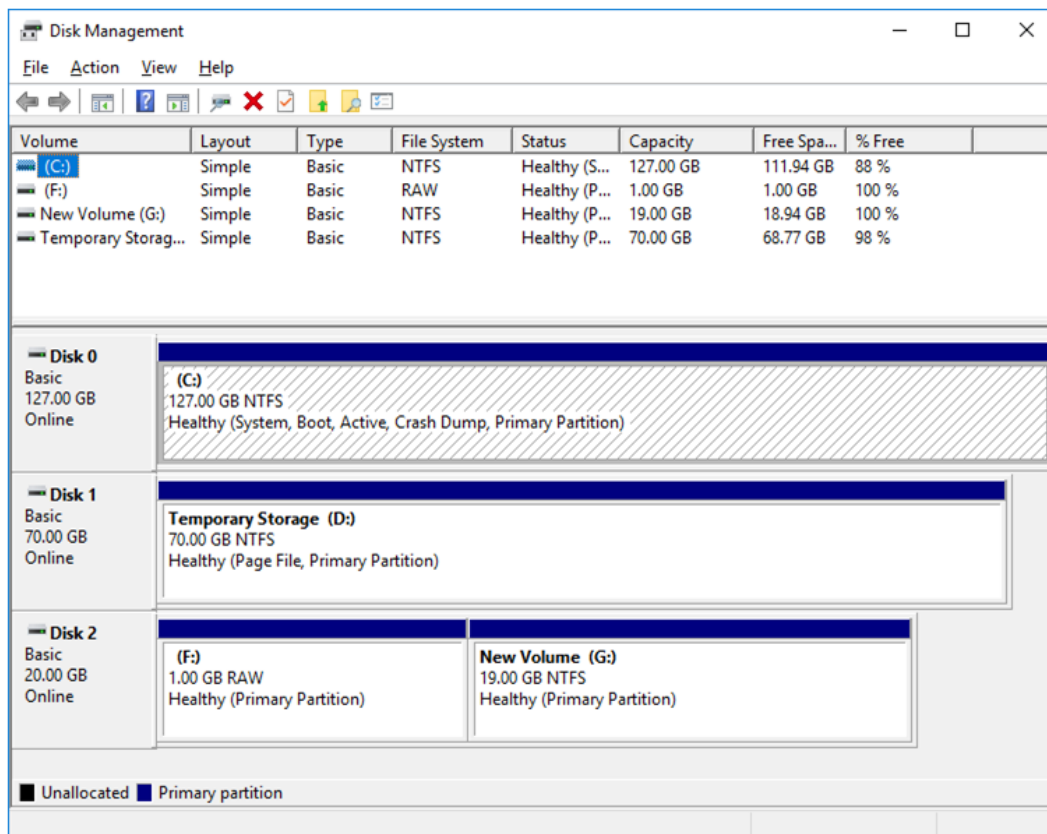
11. The **Format Partition** window is displayed. Confirm that **File system** is NTFS.



12. Click **Next**.
13. The **Completing the New Simple Volume Wizard** window is displayed. Check the displayed contents and click **Finish**.



14. Confirm that the added disks are assigned as the F drive and G drive.



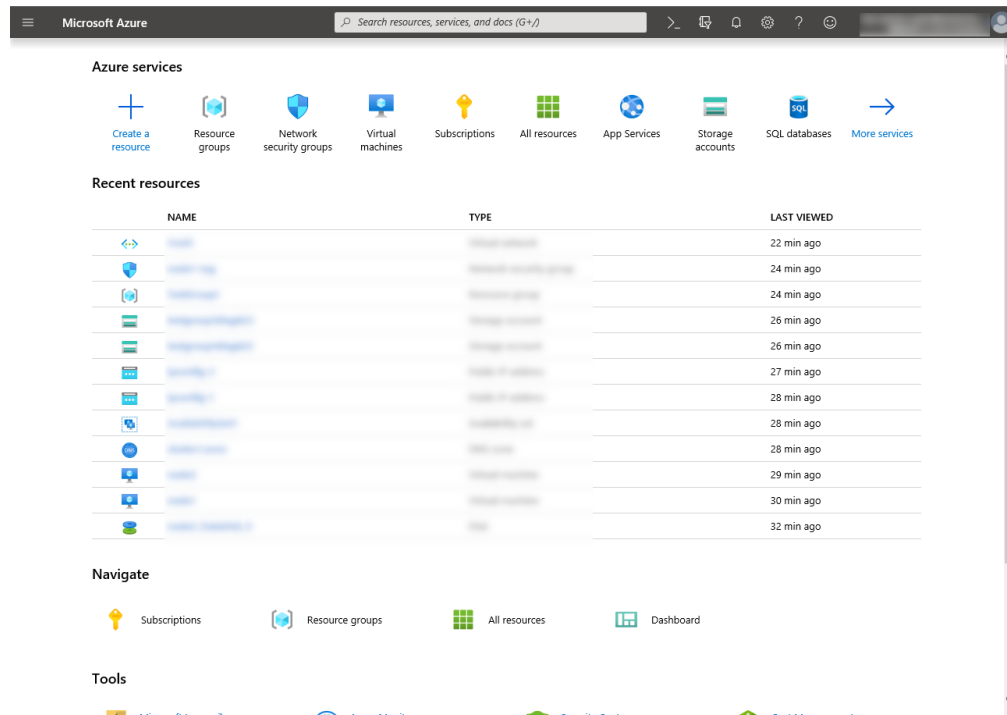
6. Configuring a load balancer

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and add a load balancer following the steps below.

For details, see the following websites:

- Load Balancer:
<https://docs.microsoft.com/en-us/azure/load-balancer/>

1. Select **Create a resource** on the upper part of the window.



2. Select **Networking** and then **Load Balancer**.
 3. The **Create load balancer** blade is displayed. Specify **Name**. Select **Public** for **Type** and **Basic** for **SKU**, respectively.
 4. Specify **Create new**, **Public IP address name** and **Assignment** for **Public IP address**.
 5. Specify **Subscription**, **Resource group**, and **Region**, and click **Review+create**. Then click **Create**.
- Deploying the load balancer starts. This processing takes several minutes.

Microsoft Azure Search resources, services, and docs (G+/)

Home > New > Create load balancer

Create load balancer

Basics Tags Review + create

Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. Load balancers uses a hash-based distribution algorithm. By default, it uses a 5-tuple (source IP, source port, destination IP, destination port, protocol type) hash to map traffic to available servers. Load balancers can either be internet-facing where it is accessible via public IP addresses, or internal where it is only accessible from a virtual network. Azure load balancers also support Network Address Translation (NAT) to route traffic between public and private IP addresses. [Learn more.](#)

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name * ✓

Region * ✓

Type * ☐ Internal ☒ Public

SKU * ☒ Basic ☐ Standard

Public IP address

Public IP address * ☒ Create new ☐ Use existing

Public IP address name * ✓

Public IP address SKU Basic

Assignment * ☐ Dynamic ☒ Static

[Review + create](#) < Previous Next: Tags > [Download a template for automation](#)

7. Configuring a load balancer (configuring a backend pool)

1. Associate a virtual machine registered to the availability set to the load balancer. After the load balancer has been deployed, select **Resource groups** on the upper part of the window.

Microsoft Azure Search resources, services, and docs (G+/)

Azure services

[Create a resource](#) [Resource groups](#) [Network security groups](#) [Virtual machines](#) [Subscriptions](#) [All resources](#) [App Services](#) [Storage accounts](#) [SQL databases](#) [More services](#)

Recent resources

	NAME	TYPE	LAST VIEWED
	TestGroup1	Resource group	22 min ago
	TestNSG	Network security group	24 min ago
	TestVM	Virtual machine	24 min ago
	TestStorage	Storage account	26 min ago
	TestDB	SQL database	26 min ago
	TestApp	App service	27 min ago
	TestLB	Load balancer	28 min ago
	TestAS	Availability set	28 min ago
	TestVM2	Virtual machine	29 min ago
	TestVM3	Virtual machine	30 min ago
	TestVM4	Virtual machine	32 min ago

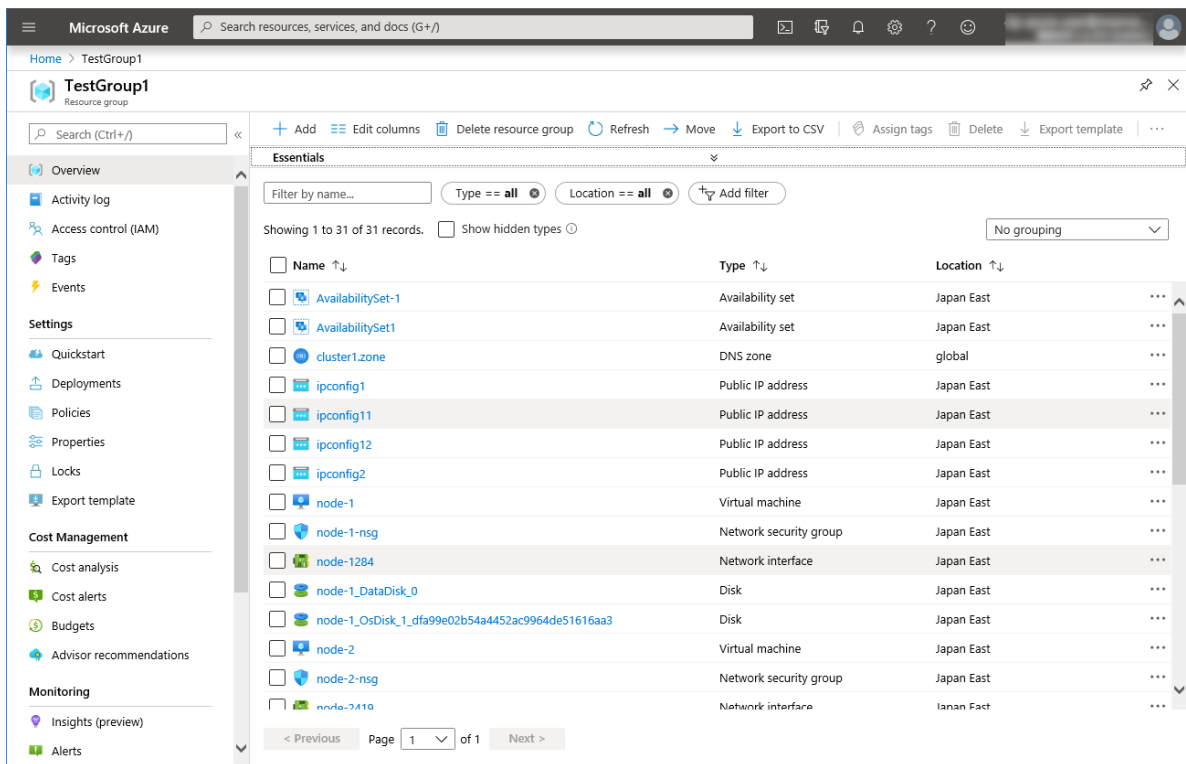
Navigate

[Subscriptions](#) [Resource groups](#) [All resources](#) [Dashboard](#)

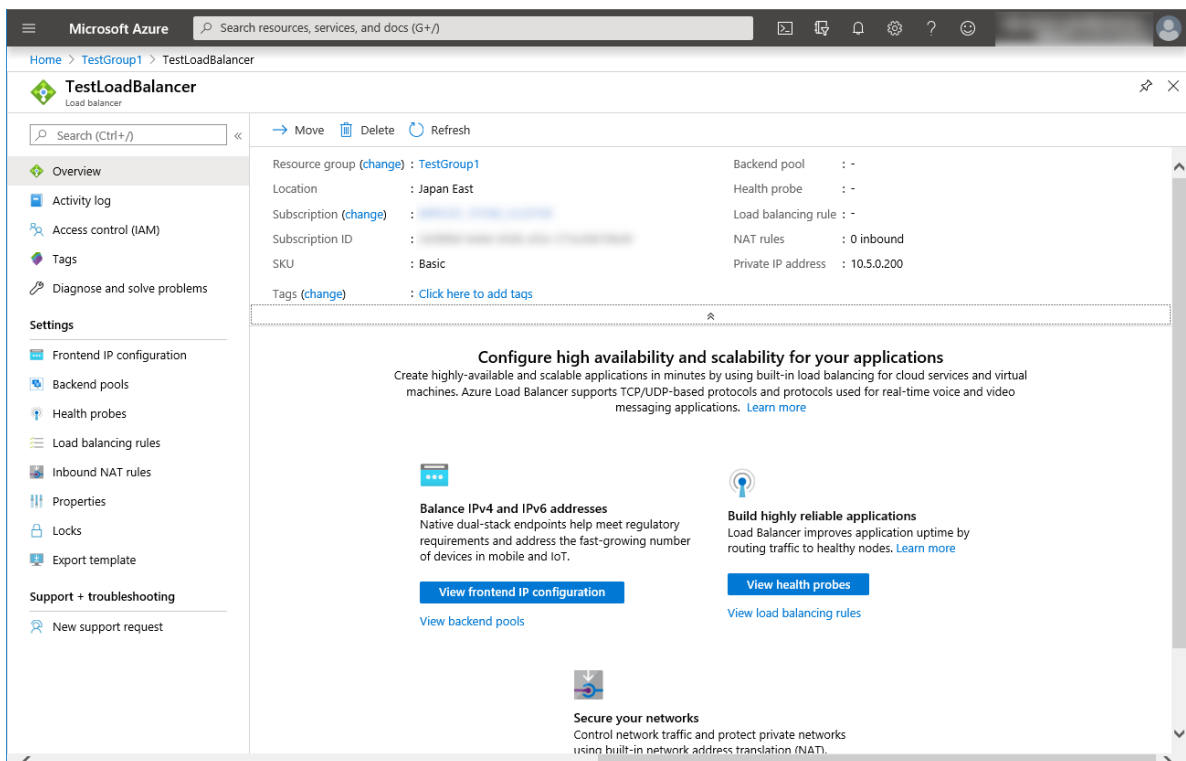
Tools

[Microsoft Learn](#) [Azure Monitor](#) [Security Center](#) [Cost Management](#)

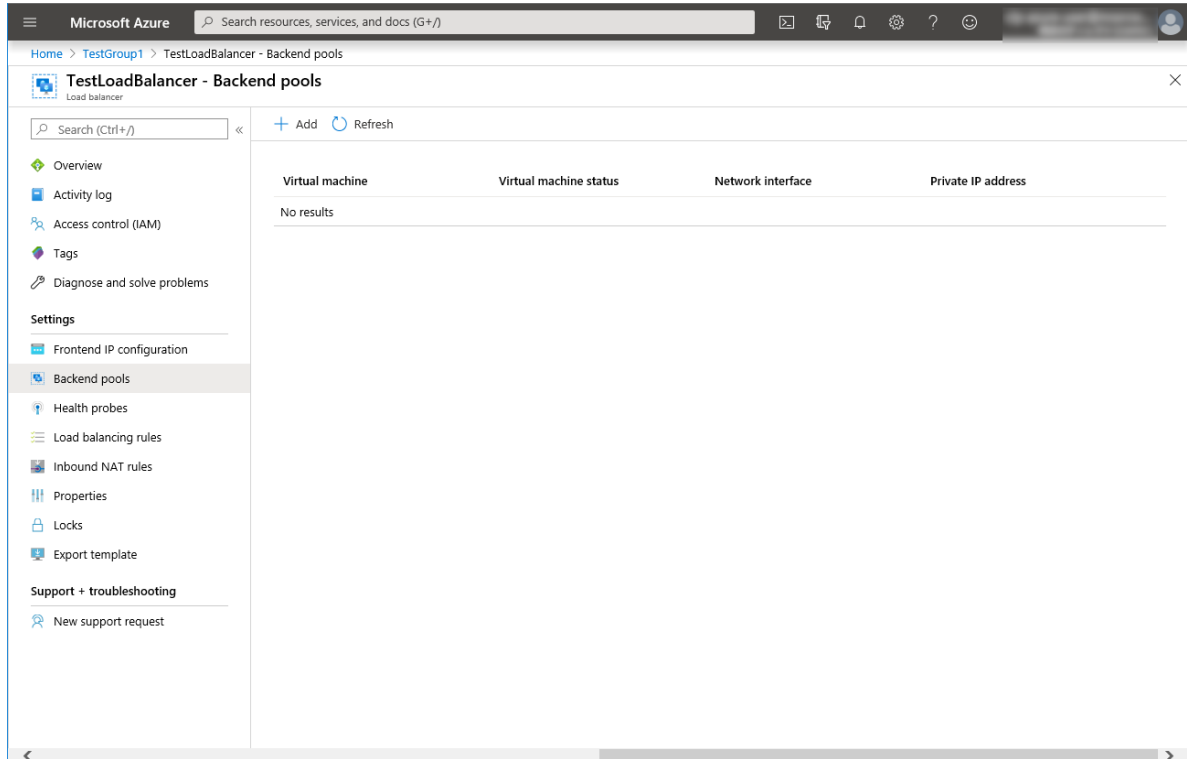
2. Select the resource group to which the created load balancer belongs from the resource group list.
3. The summary of the selected resource group is displayed. Select the created load balancer from the item list.



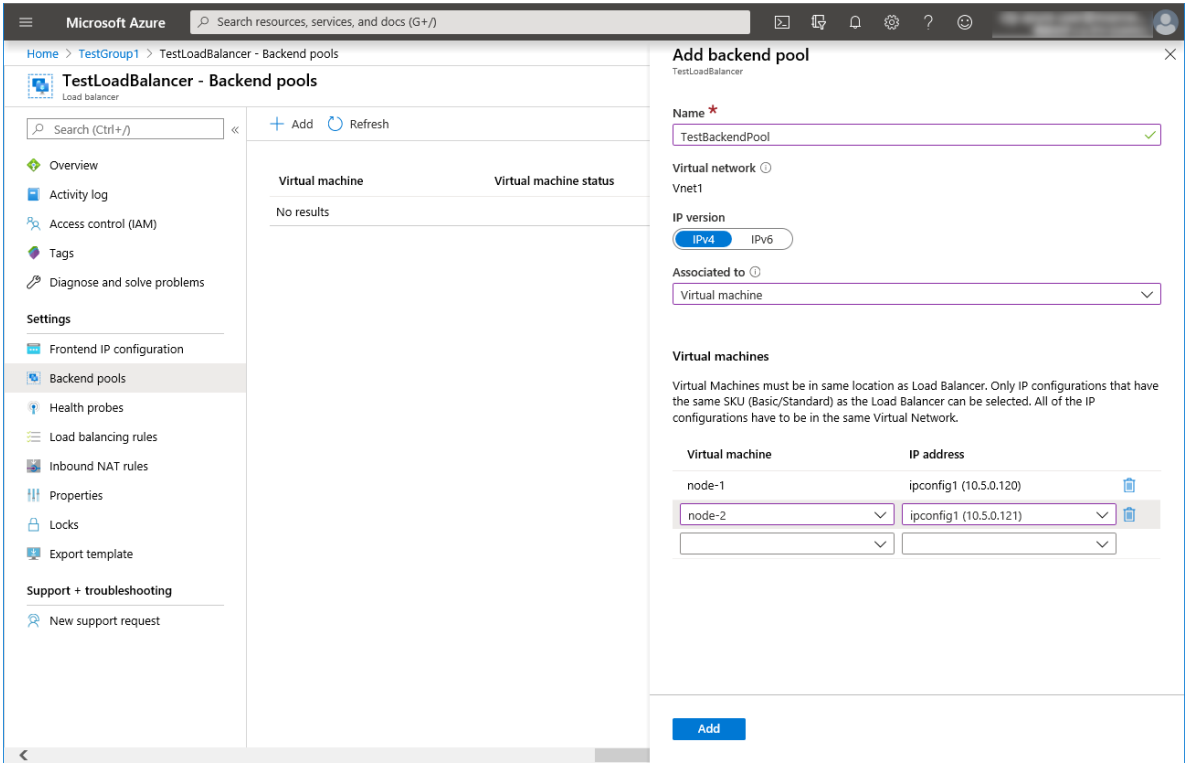
4. Select **Backend pools**.



5. Click **Add**.

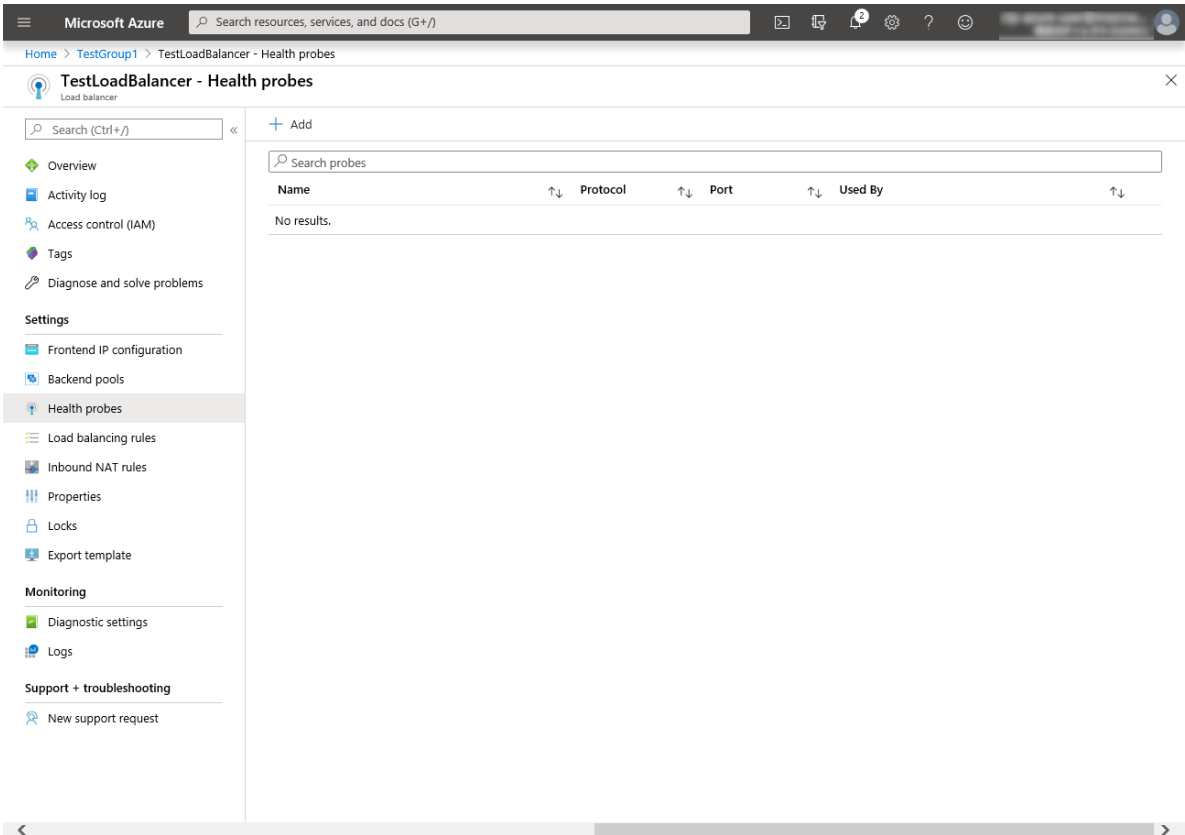


6. The **Add backend pool** blade is displayed. Specify **Name**.
7. Select **Virtual machine** for **Associated to**.
8. Specify **Virtual machine** and **IP address** for the virtual machine you want to associate. Repeat this procedure for the rest of such virtual machines.
9. Then click **Add**.



8. Configuring a load balancer (configuring a health probe)

1. Select **Health probes**.



2. Click **Add**.
3. The **Add health probe** blade is displayed. Specify **Name**.
4. Specify **Protocol** and **Port**, and click **OK**.

Microsoft Azure Search resources, services, and docs (G+)

Home > TestLoadBalancer > Health probes > Add health probe

Add health probe

TestLoadBalancer

Name *

Protocol

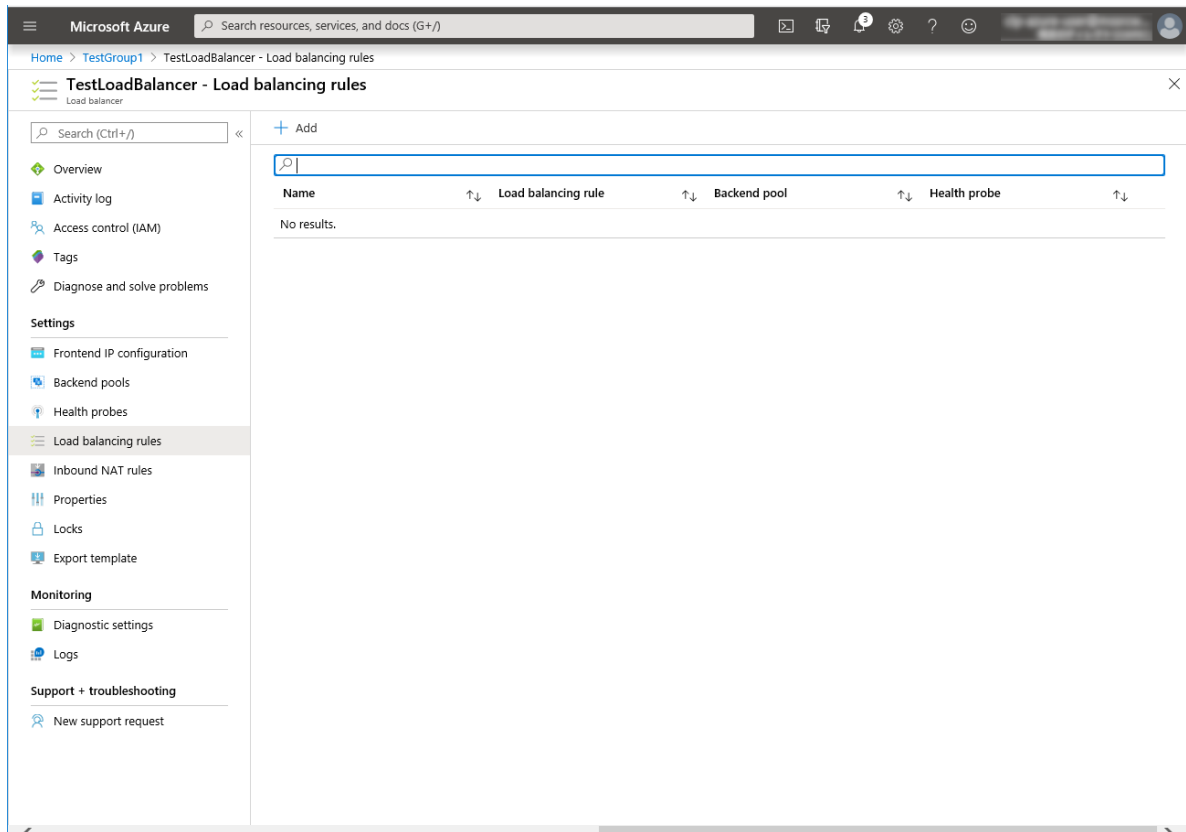
Port *

Interval * seconds

Unhealthy threshold * consecutive failures

OK

9. **Configuring a load balancer (setting the load balancing rules)**
 1. Select **Load balancing rules**.



2. Click **Add**.
3. The **Add load balancing rule** blade is displayed. Specify **Name**.
4. Specify **Port** and **Backend port**, and click **OK**.

The screenshot shows the 'Add load balancing rule' configuration page in the Microsoft Azure portal. The breadcrumb navigation is: Home > TestGroup1 > TestLoadBalancer > Load balancing rules > Add load balancing rule. The form fields are as follows:

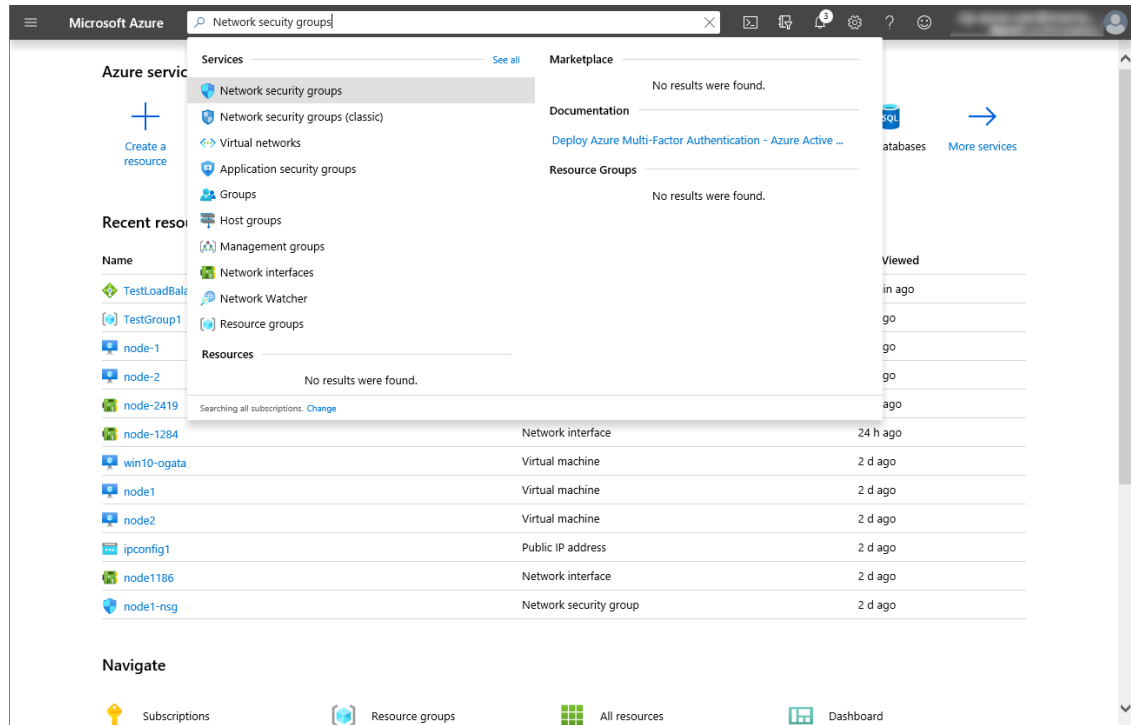
- Name ***: TestLoadBalancingRule (with a green checkmark)
- IP Version ***: ☒ IPv4 ☐ IPv6
- Frontend IP address ***: 10.5.0.200 (LoadBalancerFrontEnd)
- Protocol**: ☒ TCP ☐ UDP
- Port ***: 80
- Backend port ***: 8080 (with a green checkmark)
- Backend pool**: TestBackendPool (2 virtual machines)
- Health probe**: TestHealthProbe (TCP:26001)
- Session persistence**: None
- Idle timeout (minutes)**: 4 (with a slider bar)
- Floating IP (direct server return)**: ☒ Disabled ☐ Enabled

An 'OK' button is located at the bottom left of the form.

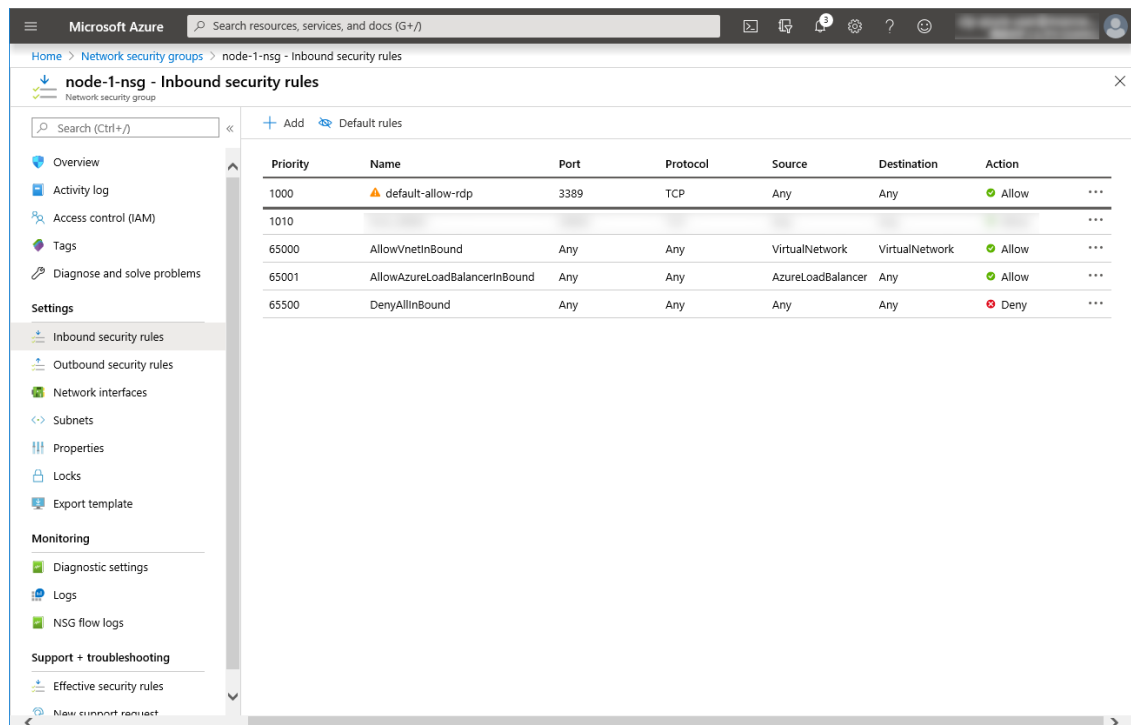
10. Setting the inbound security rules

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and set the inbound security rules following the steps below.

1. Search for Network security groups.
2. Select **Network security groups**.



3. From the network security group list, select node-1-nsg for node-1 or node-2-nsg for node-2.
4. The summary is displayed.
5. Select **Inbound security rules**.



6. Click **Add**.
7. The **Add inbound security rule** blade is displayed. Specify **Name**.

8. Specify **Destination port range** and **Protocol**, and click **Add**.

The screenshot displays the Azure portal interface for configuring an inbound security rule. The left sidebar shows the navigation menu with 'Inbound security rules' selected. The main pane shows a table of existing rules and a configuration form for a new rule.

Priority	Name	Port
1000	default-allow-rdp	3389
1010		
65000	AllowVnetInBound	Any
65001	AllowAzureLoadBalancerInBound	Any
65500	DenyAllInBound	Any

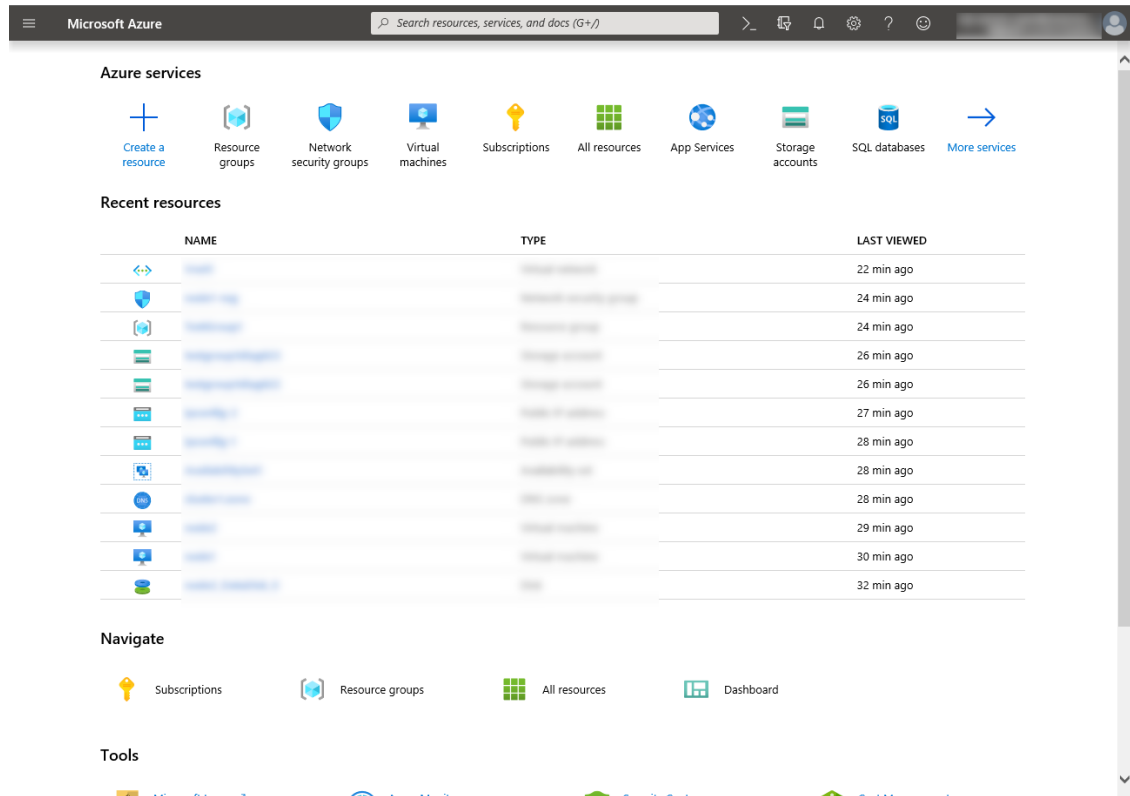
The 'Add inbound security rule' form on the right includes the following fields:

- Source:** Any
- Source port ranges:** *
- Destination:** Any
- Destination port ranges:** 8080
- Protocol:** TCP (selected)
- Action:** Allow (selected)
- Priority:** 1020
- Name:** TestHTTP
- Description:** (empty)

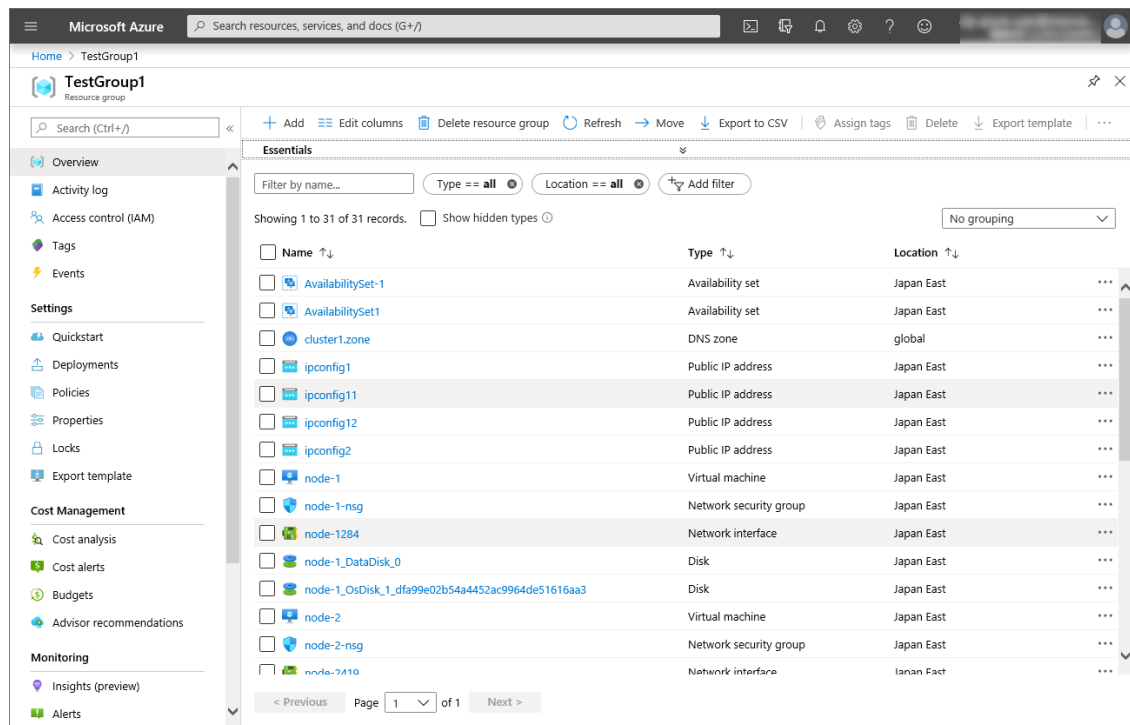
The 'Add' button is visible at the bottom right of the form.

Then, check `<Load_balancer_frontend_IP(public_IP_address)>` specified in the script before recovery action of the multi target monitor resource that is set in "3)Adding a monitor resource." Write down the confirmatory result.

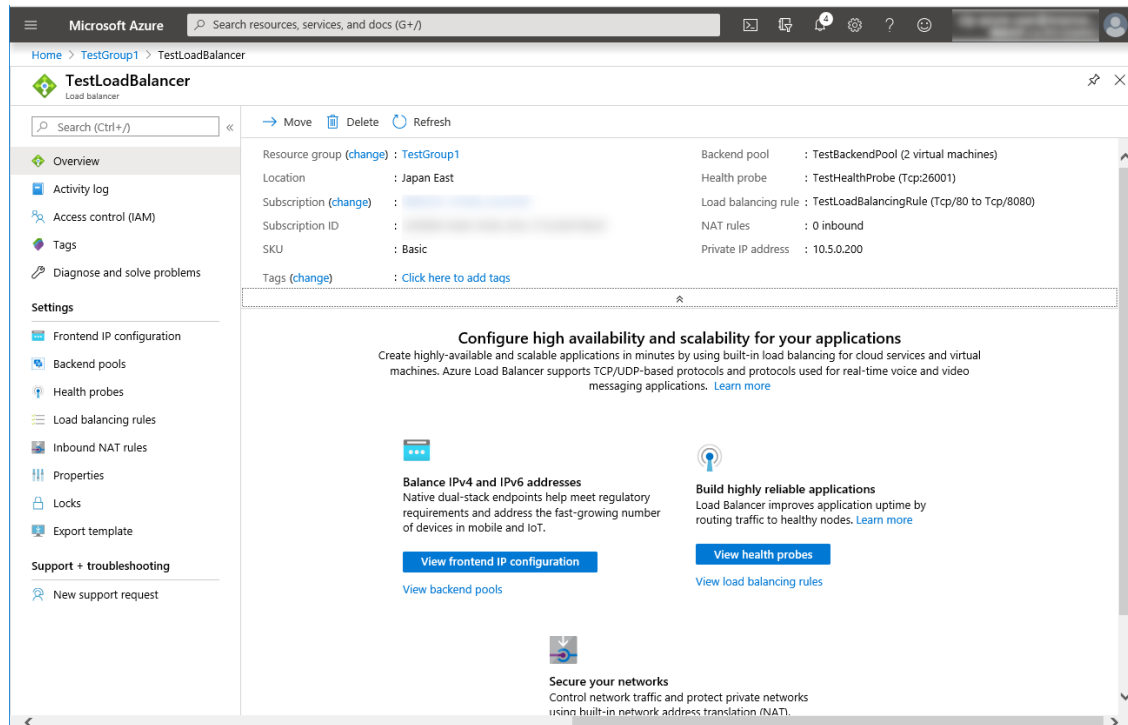
1. Select **Resource groups** on the upper part of the window.



2. Select the resource group to which the created load balancer belongs from the resource group list.
3. The summary of the selected resource group is displayed. Select the created load balancer from the item list.



4. The summary of the load balancer is displayed. Select **Public IP address** from the item list.



11. **Adjusting the OS startup time, checking the network setting, checking the firewall setting, synchronizing the server time, and disabling the power saving function.**

For each procedure, see "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.

12. **Installing EXPRESSCLUSTER**

For the installation procedure, see the Installation and Configuration Guide.

After installation is complete, restart the OS.

13. **Registering the EXPRESSCLUSTER license**

For the license registration procedure, see the Installation and Configuration Guide.

5.3 Configuring the EXPRESSCLUSTER settings

For the Cluster WebUI setup and connection procedures, see "Creating the cluster configuration data" in the the Installation and Configuration Guide.

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

- Mirror disk resource
- Azure probe port resource
- Azure probe port monitor resource
- Azure load balance monitor resource
- Custom monitor resource (for NP resolution)
- IP monitor resource (for NP resolution)
- Multi target monitor resource (for NP resolution)

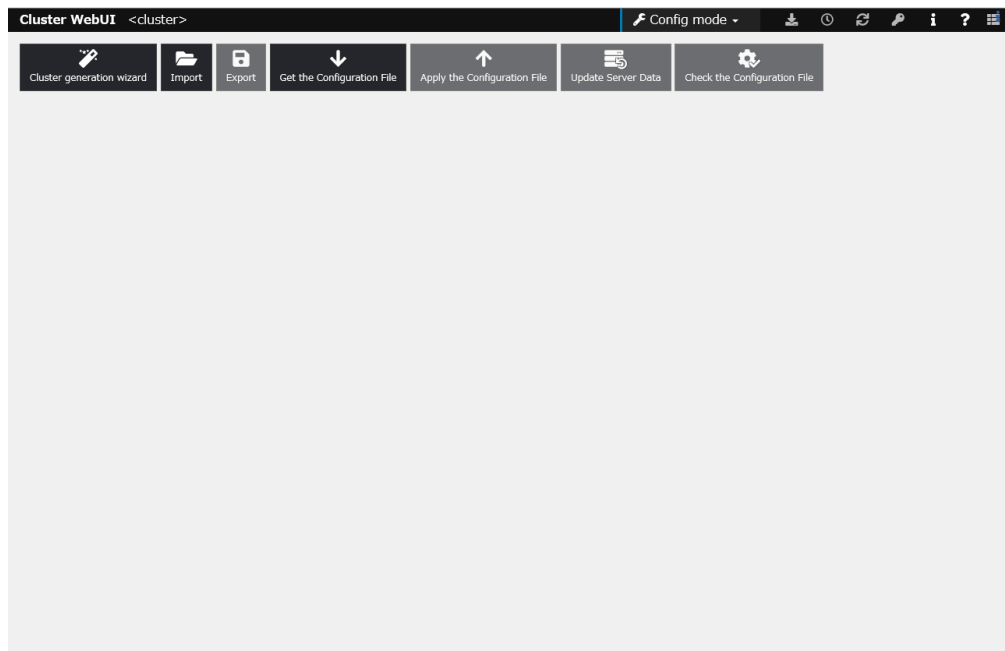
For the settings of other resources and monitor resources, see the Installation and Configuration Guide and the Reference Guide.

1) Creating a cluster

Start the Cluster generation wizard to create a cluster.

- Creating a cluster

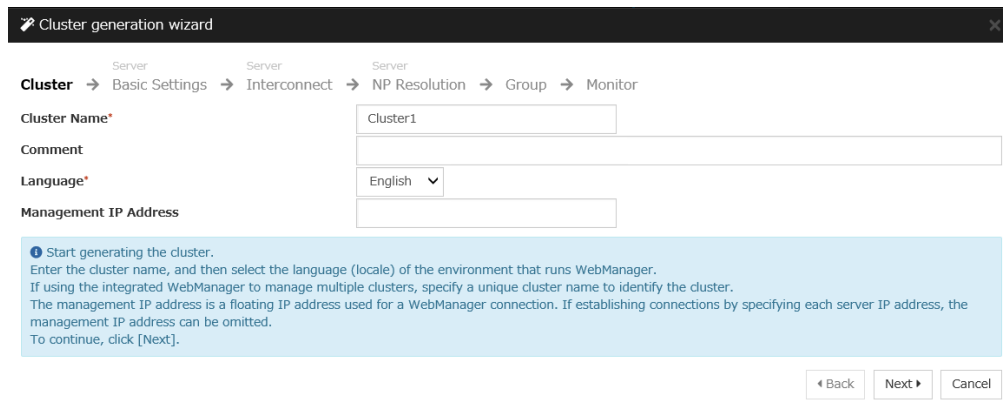
1. Access Cluster WebUI, and click **Cluster generation wizard**.



2. The **Cluster** window on the **Cluster generation wizard** is displayed.

Enter a desired name in **Cluster Name**.

Select an appropriate language in **Language**. Click **Next**.



Cluster generation wizard

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

Cluster Name*

Comment

Language* English ▾

Management IP Address

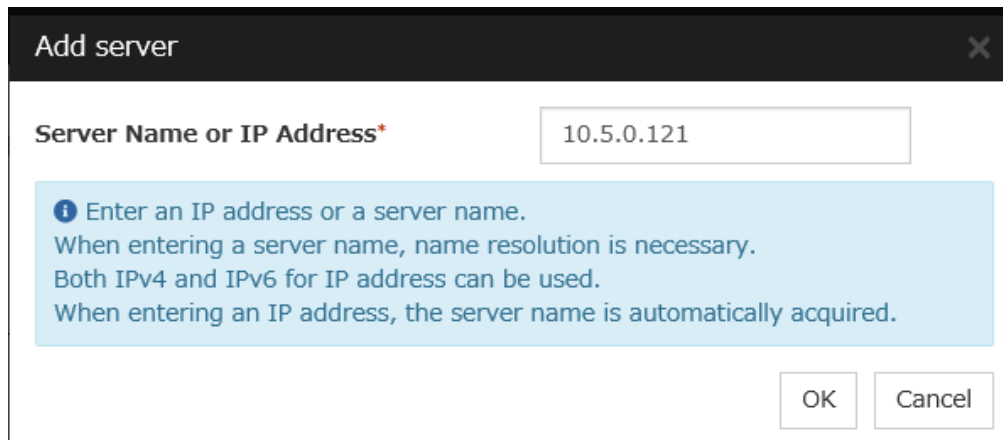
Start generating the cluster.
 Enter the cluster name, and then select the language (locale) of the environment that runs WebManager.
 If using the integrated WebManager to manage multiple clusters, specify a unique cluster name to identify the cluster.
 The management IP address is a floating IP address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

◀ Back Next ▶ Cancel

3. The **Basic Settings** window is displayed.

The instance connected to Cluster WebUI is displayed as a registered master server.

Click **Add** to add the remaining instances (by specifying the private IP address of each instance). Click **Next**.

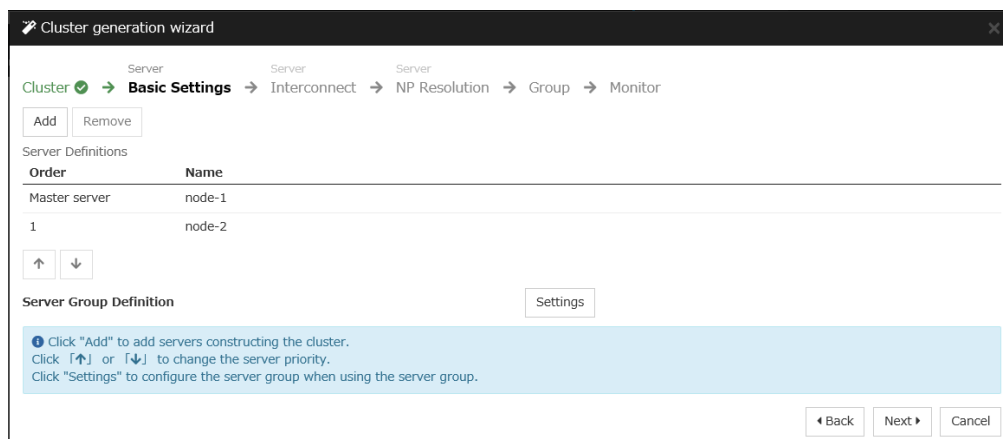


Add server

Server Name or IP Address*

Enter an IP address or a server name.
 When entering a server name, name resolution is necessary.
 Both IPv4 and IPv6 for IP address can be used.
 When entering an IP address, the server name is automatically acquired.

OK Cancel



Cluster generation wizard

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

Add Remove

Server Definitions

Order	Name
Master server	node-1
1	node-2

⬆ ⬇

Server Group Definition Settings

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

◀ Back Next ▶ Cancel

4. The **Interconnect** window is displayed.

Specify the IP addresses (IP address of each instance) to be used for interconnect. In addition, select mdc1 for **MDC** as a communication path of a mirror disk resource to be created later.

Click **Next**.

Cluster generation wizard

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

Properties Add Remove

Interconnect List

Priority	Type	MDC	node-1	node-2
1	Kernel Mode	mdc1	10.5.0.120	10.5.0.121

↑ ↓

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

Back Next Cancel

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

Note that NP resolution is not configured on this window. The equivalent feature is achieved by adding the IP monitor resource, custom monitor resource, and multi target monitor resource. Configure NP resolution in "3)Adding a monitor resource."

You need to examine the NP resolution destination and method depending on the location of clients accessing a cluster system and the condition for connecting to an on-premise environment (for example, using a dedicated line). There is no NP resolution destination nor method to recommend. Additionally, you can use network partition resolution resources for NP resolution.

Click **Next**.

Cluster generation wizard

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

Properties Add Remove

NP Resolution List

Type	Target	node-1	node-2
No NP resolutions			

Tuning

Configure network partition (NP) resolution function. Click "Add" to add NP resolution resource and select the type. For "COM" setting, click each server column cell to configure COM port. For "DISK" setting, click each server column cell to configure driver letter of the partition for disk heartbeat. For "Ping" setting, click Target column cell to configure IP address of Ping destination, and then click each server column cell to configure "Use" or "Do not use". For "HTTP" setting, click Target column cell to configure HTTP packet destination, and then click each server column cell to configure "Use" or "Do not use". For "Majority" setting, click each server column cell to configure "Use" or "Do not use". For "DISK", "Ping", and "HTTP" settings, the detailed settings can be verified and changed by clicking "Properties". Click "Tuning" to configure the actions at NP occurrence.

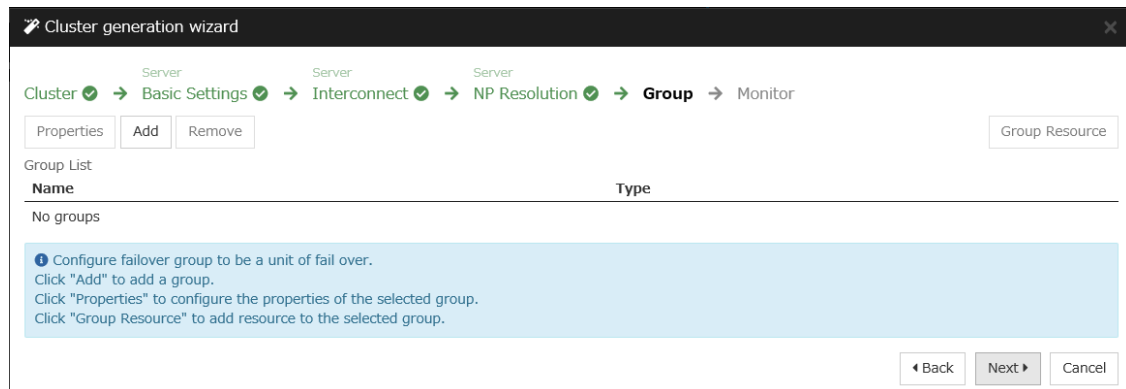
Back Next Cancel

2) **Adding a group resource**

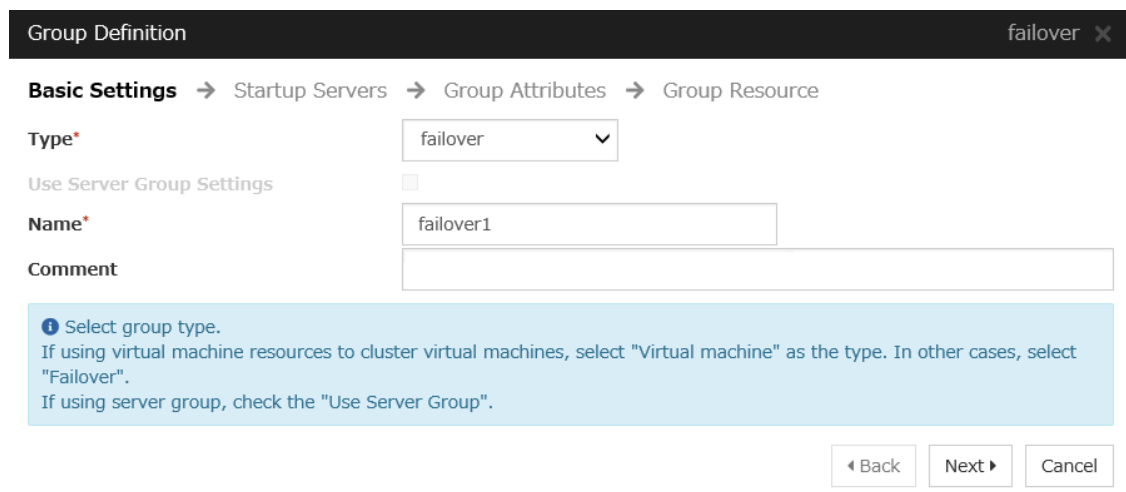
- Defining a group

Create a failover group.

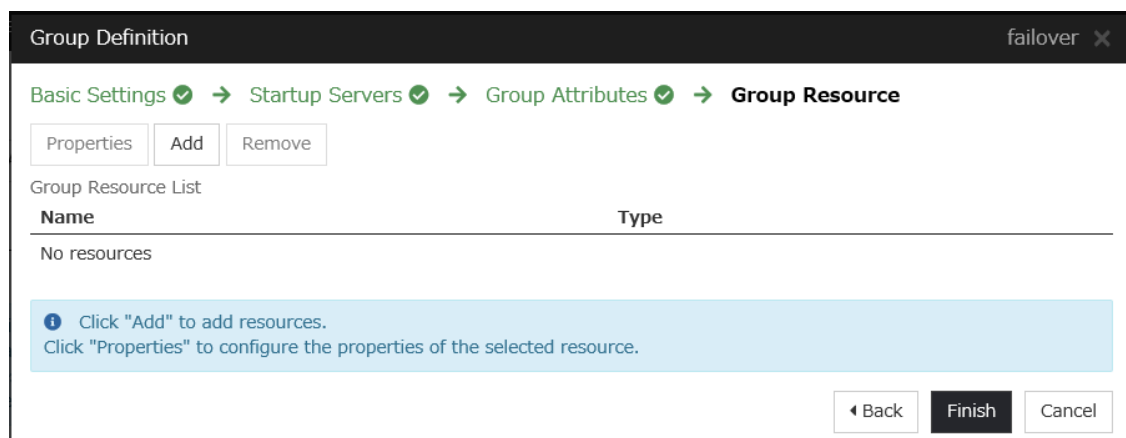
- The **Group List** window is displayed.
Click **Add**.



2. The **Group Definition** window is displayed.
Specify a failover group name (failover1) for **Name**. Click **Next**.



3. The **Startup Servers** window is displayed.
Click **Next** without specifying anything.
4. The **Group Attributes** window is displayed.
Click **Next** without specifying anything.
5. The **Group Resource** window is displayed.
On this page, add a group resource following the procedure below.



- Mirror disk resource

Create a mirror disk resource.

For details, see "Understanding mirror disk resources" in "Group resource details" in the Reference Guide.

1. Click **Add** on the **Group Resource List** page.
2. The **Resource Definition of Group | failover1** window is displayed.
Select the group resource type (Mirror disk resource) from the **Type** box and enter the group name (md) in the **Name** box. Click **Next**.

Resource Definition of Group | failover1 md X

Info → Dependency → Recovery Operation → Details

Type* Mirror disk resource ▼

Name* md

Comment

Get License Info

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

◀ Back Next ▶ Cancel

3. The **Dependency** window is displayed.
Click **Next** without specifying anything.
4. The **Recovery Operation** window is displayed.
Click **Next**.
5. The **Details** window is displayed.
Select a server name in the **Name** column of **Servers that can run the group** and click **Add**.

Resource Definition of Group | failover1 md x

Info → Dependency → Recovery Operation → Details

Mirror Disk No.*

Data Partition Drive Letter*

Cluster Partition Drive Letter*

Cluster Partition Offset Index*

Mirror Disk Connect

Servers that can run the group

Name	Data Partition	Cluster Partition
<input type="button" value="Add"/>		
<input type="button" value="Remove"/>		

Add Servers that can run the group

6. The **Selection of partition** dialog box is displayed. Click **Connect**, select the data partition and cluster partition created in "5)Configuring virtual machines", and click **OK**.

Selection of partition

Obtain information

Data Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	10238MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

Cluster Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	10238MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

- Perform steps 5 and 6 for node-1 and then node-2 and click **Finish**.

- Azure probe port resource

When EXPRESSCLUSTER is used on Microsoft Azure, EXPRESSCLUSTER provides a mechanism to wait for alive monitoring from a load balancer on a port specific to a node in which operations are running. For details about the Azure probe port resources", see "Understanding Azure probe port resources" in the Reference Guide.

- Click **Add** on the **Group Resource List** page.
- The **Resource Definition of Group | failover1** window is displayed. Select the group resource type (Azure probe port resource) from the **Type** box and enter the group name (azurepp1) in the **Name** box. Click **Next**.

- The **Dependency** window is displayed. Click **Next** without specifying anything.

4. The **Recovery Operation** window is displayed. Click **Next**.
5. For **Probeport**, enter the value specified for **Port** when configuring a load balancer (configuring health probe).

6. Click **Finish**.

3) Adding a monitor resource

- Azure probe port monitor resource

The port monitoring mechanism for alive monitoring is provided for the node in which the Microsoft Azure probe port resource is running.

For details about the Azure probe port monitor resource, see "Understanding Azure probe port monitor resources" in the Reference Guide.

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

- Azure load balance monitor resource

The mechanism to monitor whether the port with the same port number as the probe port is open or not is provided for the node in which the Microsoft Azure probe port resource is not running.

For details about the Azure load balance monitor resource, see "Understanding Azure load balance monitor resources" in the Reference Guide.

Adding one Azure probe port resource creates one Azure load balance monitor resource automatically.

- Custom monitor resource

Sets a script to monitor whether communication with Microsoft Azure Service Management API is possible, and also monitors health of communication with an external network.

For details about the custom monitor resource, see "Understanding custom monitor resources" in the Reference Guide.

1. Click **Add** on the **Monitor Resource List** page.
2. Select the monitor resource type (Custom monitor) from the **Type** box and enter the monitor resource name (genw1) in the **Name** box. Click **Next**.

Monitor Resource Definition
genw ✕

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

Type* Custom monitor ▾

Name* genw1

Comment

Get Licence Info

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

◀ Back
Next ▶
Cancel

3. The **Monitor (common)** window is displayed.
 Confirm that **Monitor Timing** is **Always** and click **Next**.

Monitor Resource Definition
genw ✕

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

Interval* 60 sec

Timeout* 120 sec

Do Not Retry at Timeout Occurrence ☐

Do Not Execute Recovery Action at Timeout Occurrence ☐

Retry Count* 1 time

Wait Time to Start Monitoring* 3 sec

Monitor Timing

☒ Always

☐ Active

Target Resource Browse

Choose servers that execute monitoring Server

◀ Back
Next ▶
Cancel

4. The **Monitor (special)** window is displayed.
 Select **Script created with this product**.
 The following shows the sample of a script to be created.

```
< EXPRESSCLUSTER_installation_path>\bin\clpazure_port_checker -h_
↪management.core.windows.net -p 443
EXIT %ERRORLEVEL%
```

Select **Synchronous** for **Monitor Type**. Click **Next**.

Monitor Resource Definition genw x

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

☐ User Application
☒ Script created with this product

File: genw.bat Edit View Replace

Monitor Type: ☒ Synchronous
☐ Asynchronous

Normal Return Value*: 0

Kill the application when exit: ☐

Wait for activation monitoring to stop before stopping the cluster: ☐

Execution user:

◀ Back Next ▶ Cancel

5. The **Recovery Action** window is displayed.

Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final action**.

Monitor Resource Definition genw x

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

Recovery Action: Execute only the final action

Recovery Target*: LocalServer Browse

Recovery Script Execution Count: 0 time

Execute Script before Reactivation: ☐

Maximum Reactivation Count: 0 time

Execute Script before Failover: ☐

Execute migration before Failover: ☐

Failover Target Server: ☒ Stable server
☐ Maximum priority server

Maximum Failover Count: 0 time

Execute Script before Final Action: ☐

Final Action: No operation

Script Settings

◀ Back Finish Cancel

6. Click **Finish** to finish setting.

- IP monitor resource

Creates an IP monitor resource to monitor communication between clusters that are configured with virtual machines, and also to monitor whether communication with an internal network is health.

For details about the IP monitor resource, see "Understanding IP monitor resources" in the Reference Guide.

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

Monitor Resource Definition ipw ✕

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

Type* IP monitor ▼

Name* ipw1

Comment

Get Licence Info

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

◀ Back
Next ▶
Cancel

3. The **Monitor (common)** window is displayed.
 Confirm that **Monitor Timing** is **Always**.

Monitor Resource Definition ipw ✕

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

Interval* 60 sec

Timeout* 60 sec

Do Not Retry at Timeout Occurrence ☐

Do Not Execute Recovery Action at Timeout Occurrence ☐

Retry Count* 1 time

Wait Time to Start Monitoring* 0 sec

Monitor Timing

☒ Always

☐ Active

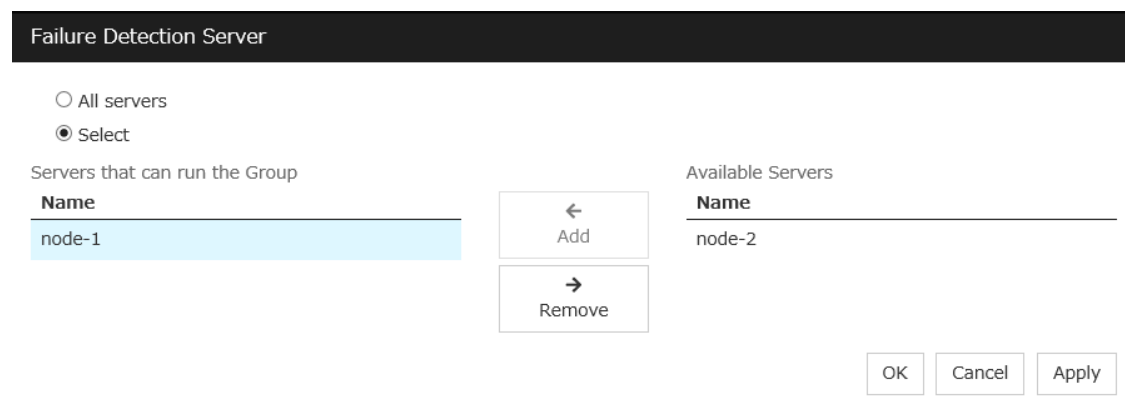
Target Resource Browse

Choose servers that execute monitoring Server

◀ Back
Next ▶
Cancel

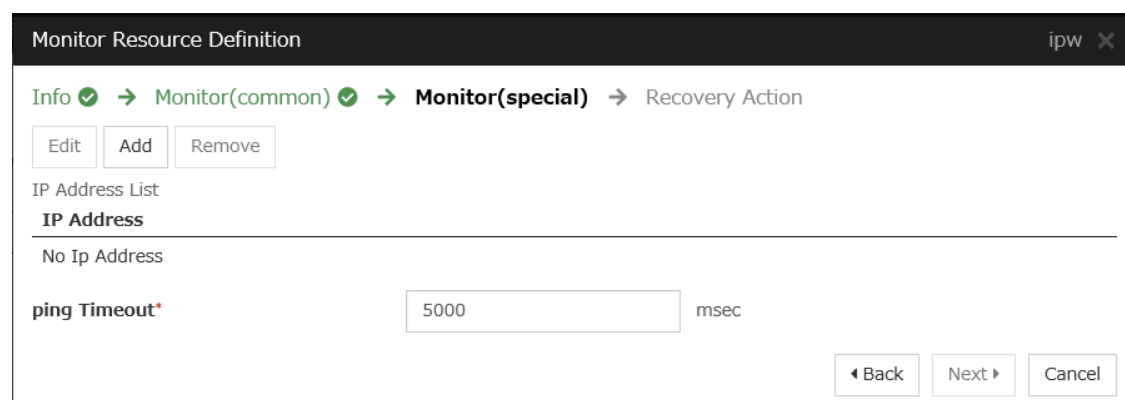
Select one available server for **Choose servers that execute monitoring**.

Click **OK** and click **Next**.



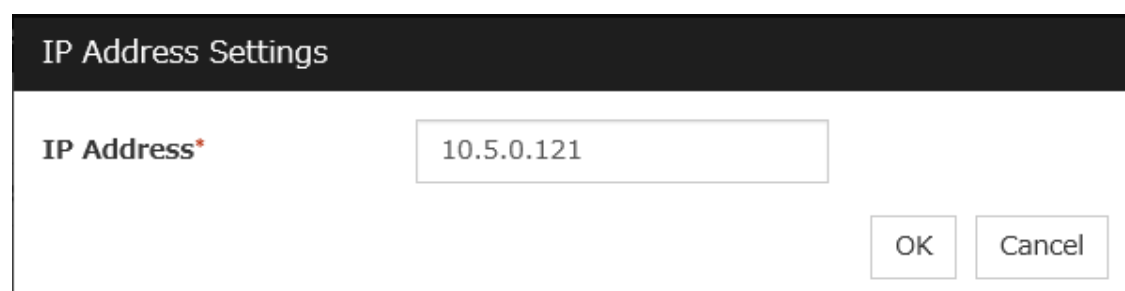
The **Failure Detection Server** dialog box is shown. It has two radio buttons: **All servers** and **Select** (which is selected). Below the radio buttons is the text "Servers that can run the Group". There are two lists: "Servers that can run the Group" and "Available Servers". The "Servers that can run the Group" list contains "node-1". The "Available Servers" list contains "node-2". Between the lists are two buttons: "Add" (with a left arrow) and "Remove" (with a right arrow). At the bottom right are three buttons: "OK", "Cancel", and "Apply".

4. The **Monitor (special)** window is displayed.



The **Monitor Resource Definition** dialog box is shown. It has a title bar with "Monitor Resource Definition" and a close button. Below the title bar is a breadcrumb trail: **Info** (with a green checkmark) → **Monitor(common)** (with a green checkmark) → **Monitor(special)** (with a green checkmark) → **Recovery Action**. Below the breadcrumb trail are three buttons: "Edit", "Add", and "Remove". Below these buttons is the text "IP Address List". There is a table with one row and one column: "IP Address". The table is empty. Below the table is the text "No Ip Address". Below the text "No Ip Address" is a text box labeled "ping Timeout*" with the value "5000" and the unit "msec". At the bottom right are three buttons: "Back", "Next", and "Cancel".

On the **Common** tab, select **Add** of **IP Address** and set an IP address of a server other than the server selected in step 3. Click **Next**.



The **IP Address Settings** dialog box is shown. It has a title bar with "IP Address Settings". Below the title bar is a text box labeled "IP Address*" with the value "10.5.0.121". At the bottom right are two buttons: "OK" and "Cancel".

The screenshot shows the 'Monitor Resource Definition' window with the 'Recovery Action' tab selected. The breadcrumb trail is 'Info' → 'Monitor(common)' → 'Monitor(special)' → 'Recovery Action'. Below the breadcrumb are 'Edit', 'Add', and 'Remove' buttons. The 'IP Address List' section shows a table with one entry: '10.5.0.121'. Below this, the 'ping Timeout*' is set to '5000' msec. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

- The **Recovery Action** window is displayed.

Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final Action**.

This screenshot shows the 'Recovery Action' configuration page. The breadcrumb trail is 'Info' → 'Monitor(common)' → 'Monitor(special)' → 'Recovery Action'. The 'Recovery Action' dropdown is set to 'Execute only the final action'. The 'Recovery Target' is 'LocalServer' with a 'Browse' button. Below are sections for 'Recovery Script Execution Count' (0 time), 'Execute Script before Reactivation' (checkbox), 'Maximum Reactivation Count' (0 time), 'Execute Script before Failover' (checkbox), 'Execute migration before Failover' (checkbox), 'Failover Target Server' (radio buttons for 'Stable server' and 'Maximum priority server'), and 'Maximum Failover Count' (0 time). At the bottom, 'Execute Script before Final Action' is a checkbox, and 'Final Action' is a dropdown set to 'No operation'. A 'Script Settings' button is on the right. At the bottom right are 'Back', 'Finish', and 'Cancel' buttons.

- Click **Finish** to finish setting.
- Then, create a monitor resource on the other server. Click **Add** on the **Monitor Resource List** page.
- Select the monitor resource type (IP monitor) from the **Type** box and enter the monitor resource name (ipw2) in the **Name** box. Click **Next**.
- The **Monitor (common)** window is displayed.
 Confirm that **Monitor Timing** is **Always**.

Select one available server for **Choose servers that execute monitoring**. Click **OK** and Click **Next**.

10. The **Monitor (special)** window is displayed.

On the **Common** tab, select **Add** of **IP Address** and set an IP address of a server other than the server selected in step 9. Click **Next**.

11. The **Recovery Action** window is displayed.

Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final action**.

12. Click **Finish** to finish setting.

- Multi target monitor resource

Creates a multi target monitor resource to check the statuses of the custom monitor resource and IP monitor resource. The custom monitor resource monitors communication to Microsoft Azure Service Management API. The IP monitor resource monitors communication between clusters that are configured with virtual machines.

If their statuses are abnormal, execute the script in which the processing for NP resolution is described.

For details about the multi target monitor resource, see "Understanding multi target monitor resources" in the Reference Guide.

1. Click **Add** on the **Monitor Resource List** page.
2. Select the monitor resource type (Multi target monitor) from the **Type** box and enter the monitor resource name (mtw1) in the **Name** box. Click **Next**.

The screenshot shows the 'Monitor Resource Definition' window with the 'Recovery Action' tab selected. The window has a breadcrumb trail: Info → Monitor(common) → Monitor(special) → Recovery Action. The 'Interval*' is set to 60 sec, and 'Timeout*' is set to 60 sec. There are checkboxes for 'Do Not Retry at Timeout Occurrence' and 'Do Not Execute Recovery Action at Timeout Occurrence', both of which are unchecked. 'Retry Count*' is set to 1 time, and 'Wait Time to Start Monitoring*' is set to 0 sec. Under 'Monitor Timing', the 'Always' radio button is selected. There is a 'Target Resource' field with a 'Browse' button next to it. At the bottom, there is a 'Choose servers that execute monitoring' section with a 'Server' button. Navigation buttons at the bottom right are 'Back', 'Next', and 'Cancel'.

3. The **Monitor (common)** window is displayed.
Confirm that **Monitor Timing** is **Always** and click **Next**.

The screenshot shows the 'Monitor Resource Definition' window with the 'Monitor(special)' step selected in the breadcrumb trail. The 'Monitor Resources' table on the left contains three entries: 'genw1' (type 'genw'), 'ipw1' (type 'ipw'), and 'ipw2' (type 'ipw'). The 'ipw2' row is highlighted. Between the tables are 'Add' and 'Remove' buttons. The 'Available Monitor Resources' table on the right contains one entry: 'userw' (type 'userw'). At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Monitor Resource	Type
genw1	genw
ipw1	ipw
ipw2	ipw

Monitor Resource	Type
userw	userw

4. The **Monitor (special)** window is displayed.

From **Available Monitor Resources**, select the custom monitor resource (genw1) for checking communication with Service Management API and two IP monitor resources (ipw1 and ipw2) that are set to both servers. Then, click **Add** to add them to **Monitor Resource List**. Click **Next**.

The screenshot shows the 'Monitor Resource Definition' window with the 'Recovery Action' step selected. The 'Recovery Action' dropdown is set to 'Execute only the final action'. The 'Recovery Target' is 'LocalServer'. Below are fields for 'Recovery Script Execution Count' (0), 'Execute Script before Reactivation' (unchecked), 'Maximum Reactivation Count' (0), 'Execute Script before Failover' (unchecked), 'Execute migration before Failover' (unchecked), 'Failover Target Server' (Stable server selected), and 'Maximum Failover Count' (0). At the bottom, 'Execute Script before Final Action' is unchecked, and the 'Final Action' is 'Stop the cluster service and shutdown OS'. A 'Script Settings' button is at the bottom right, along with 'Back', 'Finish', and 'Cancel' buttons.

Recovery Action: Execute only the final action

Recovery Target: LocalServer

Recovery Script Execution Count: 0 time

Execute Script before Reactivation: ☐

Maximum Reactivation Count: 0 time

Execute Script before Failover: ☐

Execute migration before Failover: ☐

Failover Target Server: ☒ Stable server ☐ Maximum priority server

Maximum Failover Count: 0 time

Execute Script before Final Action: ☐

Final Action: Stop the cluster service and shutdown OS

Script Settings

5. The **Recovery Action** window is displayed.

Select **Execute only the final action** for **Recovery action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final action**, and select the **Execute Script before Final Action** check box.

Click **Script Settings** and create a script to be executed when the multi target monitor resource detects an error.

Monitor Resource Definition
mtw

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

Recovery Action

Execute only the final action

Recovery Target *

LocalServer

Browse

Recovery Script Execution Count

0

time

Execute Script before Reactivation
☐

Maximum Reactivation Count

0

time

Execute Script before Failover
☐

Execute migration before Failover
☐

Failover Target Server

☒ Stable server
☐ Maximum priority server

Maximum Failover Count

0

time

Execute Script before Final Action
☒

Final Action

No operation

Script Settings

Back
Finish
Cancel

6. The script editing dialog box is displayed.

Select **Script created with this product** and click **Edit** to edit the script. The following shows the sample of a script to be created.

Specify the following by referring to "4.1 Creation example" The ports differ depending on operations.

- **Load balancing rule > Backend port** of the load balancer
- **Load balancing rule > Port** of the load balancer

Set the public IP address that you wrote down in "10)Setting the inbound security rules" to the following:

– **Frontend IP** (public IP address) of the load balancer

```

rem *****
rem Check Active Node
rem *****
<EXPRESSCLUSTER_installation_path>binclpazure_port_checker -h 127.0.0.
↪1 -p < Backend_port_of_the_load_balancer_of_Load_balancing_rule>
IF NOT "%ERRORLEVEL%" == "0" (
GOTO CLUSTER_SHUTDOWN
)
rem *****
rem Check DNS
rem *****

```

```
<EXPRESSCLUSTER_installation_path>binclpazure_port_checker -h <_
↪Frontend_IP (public_IP_address)_of_the_load_balancer> -p < Port_of_
↪the_load_balancer_of_Load_balancing_rule>
IF "%ERRORLEVEL%" == "0" (
GOTO EXIT
)
rem *****
rem Cluster Shutdown
rem *****
:CLUSTER_SHUTDOWN
clpdown
rem *****
rem EXIT
rem *****
:EXIT
EXIT 0
```

For **Timeout**, specify a value larger than the timeout value of clpazure_port_checker (fixed to five seconds). In the case of the above sample script, it is recommended to set a value larger than 10 seconds in order to execute clpazure_port_checker twice.

Click **OK**.

Edit Script
✕

☐ User Application

☒ Script created with this product

File

preaction.bat

Edit

View

Replace

Timeout*

15

sec

Exec User

▼

OK

Cancel

Apply

7. Click **Finish** to finish setting.

4) Setting the cluster properties

For details about the cluster properties, see "Cluster properties" in the Reference Guide.

- Cluster properties

Configure the settings in **Cluster Properties** to link Microsoft Azure and EXPRESSCLUSTER.

1. Enter **Config Mode** from Cluster WebUI, click the property icon of the cluster name.

Cluster Name	<input type="text" value="Cluster1"/>
Comment	<input type="text"/>
Language	<input type="text" value="English"/> ▼
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

2. Select the **Timeout** tab. For **Timeout** of **Heartbeat**, specify a value calculated by "A+B+C" as described below.

- A: **Interval** of the monitor resource being monitored by the multi target monitor resource for NP resolution x (**Retry Count**+1)

* Among three monitor resources, select the monitor resource whose calculation result is the largest.

- B: **Interval** of the multi target monitor resource x (**Retry Count**+1)
- C: 30 seconds (Waiting time for heartbeat not to time out before the multi target monitor resource detects an error. The time can be changed accordingly).

Note: If **Timeout** of **Heartbeat** is shorter than the time that the multi target monitor resource requires to detect an error, a heartbeat timeout will be detected before starting the NP resolution processing. In this case, the same service may start doubly in the cluster because the service also starts on the standby server.

Network initialization complete wait time*	<input type="text" value="3"/>	min
Server Sync Wait Time*	<input type="text" value="5"/>	min
Heartbeat		
Interval*	<input type="text" value="3"/>	sec
Timeout*	<input type="text" value="270"/>	sec
Server Internal Timeout*	<input type="text" value="180"/>	sec
<input type="button" value="Initialize"/>		
<input type="button" value="OK"/> <input type="button" value="Cancel"/> <input type="button" value="Apply"/>		

3. Click **OK**.

5) Applying the settings and starting the cluster

1. Click **Apply the Configuration File** in the config mode of Cluster WebUI.
A popup message asking "Do you want to perform the operations?" is displayed. Click **OK**.
When the upload ends successfully, a popup message saying "The application finished successfully." is displayed. Click **OK**.
If the upload fails, perform the operations by following the displayed message.
2. Select the **Operation Mode** on the drop down menu of the toolbar in Cluster WebUI to switch to the operation mode. Select **Start Cluster** in the **Status** tab of Cluster WebUI and click.
3. Confirm that a cluster system starts and the status of the cluster is displayed to the Cluster WebUI.
If the cluster system does not start normally, take action according to an error message.

For details, refer to the following:

Installation and Configuration Guide

-> How to create a cluster

5.4 Verifying the created environment

Verify whether the created environment works properly by generating a (dummy) monitoring error to fail over a failover group.

If the cluster is running normally, the verification procedure is as follows:

1. Start the failover group (failover1) on the active node (node-1). In the Status tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node-1 is **Normal**.
2. Change **Operation Mode** to **Verification Mode** from the Cluster WebUI pull-down menu.
3. In the Status tab on the Cluster WebUI, click the **Enable dummy failure** icon of azureppw1 of Monitors.
4. After the Azure probe port resource (azurepp1) activated three times, the failover group (failover1) becomes abnormal and fails over to node-2. In the Status tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node-2 is **Normal**.

Also, confirm that access to the frontend IP and port of the Azure load balancer is normal after the failover.

Verifying the failover operation in case of a dummy failure is now complete. Verify the operations in case of other failures if necessary.

CLUSTER CREATION PROCEDURE (FOR AN HA CLUSTER USING AN INTERNAL LOAD BALANCER)

6.1 Creation example

This guide introduces the procedure for creating a 2-node unidirectional standby cluster using EXPRESSCLUSTER. This procedure is intended to create a mirror disk type configuration in which node-1 is used as an active server.

The following tables describe the parameters that do not have a default value and the parameters whose values are to be changed from the default values.

- Microsoft Azure settings (common to node-1 and node-2)

Setting item	Setting value
Resource group setting	
Resource group	TestGroup1
Region	(Asia Pacific) Japan East
Virtual network setting	
Name	Vnet1
Address space	10.5.0.0/24
Subnet Name	Vnet1-1
Subnet Address range	10.5.0.0/24
Resource group	TestGroup1
Location	(Asia Pacific) Japan East
Load balancer setting	
Name	TestLoadBalancer
Type	Internal
Virtual network	Vnet1
Subnet	Vnet1-1
IP address assignment	Static
Private IP address	10.5.0.200
Resource group	TestGroup1
Region	(Asia Pacific) Japan East
Backend pool: Name	TestBackendPool
Associated to	Availability set
Target virtual machine	node-1 node-2

Continued on next page

Table 6.1 – continued from previous page

Setting item	Setting value
Network IP configuration	10.5.0.120 10.5.0.121
Health probe: Name	TestHealthProbe
Health probe: Port	26001
Load balancing rule: Name	TestLoadBalancingRule
Load balancing rule: Port	80 (Port number offering the operation)
Load balancing rule: Backend port	8080 (Port number offering the operation)

- Microsoft Azure settings (specific to each of node-1 and node-2)

Setting item	Setting value	
	node-1	node-2
Virtual machine setting		
– Disk type	Standard HDD	
– User name	testlogin	
– Password	PassWord_123	
– Resource group	TestGroup1	
– Region	(Asia Pacific) Japan East	
Network security group setting		
– Name	node-1-nsg	node-2-nsg
Availability set setting		
– Name	AvailabilitySet-1	
– Update domains	5	
– Fault domains	2	
Diagnostics storage account setting		
– Name	Automatically generated	
– Performance	Standard	
– Replication	Locally-redundant storage (LRS)	
IP configuration setting		
– IP address	10.5.0.120	10.5.0.121
Disk setting		
– Name	node-1Blob1	node-2Blob1
– Source type	None (empty disk)	
– Account type	Standard HDD	
– Size	20	

- EXPRESSCLUSTER settings (cluster properties)

Setting item	Setting value	
	node-1	node-2
– Cluster name	Cluster1	
– Server name	node-1	node-2
– NP Resolution Tab: Type	Ping	
– NP Resolution Tab: Ping Target	10.5.0.5	
– NP Resolution Tab: <server> column	Use	Use

- EXPRESSCLUSTER settings (failover group)

Resource name	Setting item	Setting value
Mirror disk resource	Nama	md
	Details Tab: Data Partition Drive Letter	G:
	Details Tab: Cluster Partition Drive Letter	F:
Azure probe port resource	Name	azurepp1
	Probe port	26001 (Value specified for Port of Health probe)

- EXPRESSCLUSTER settings (monitor resource)

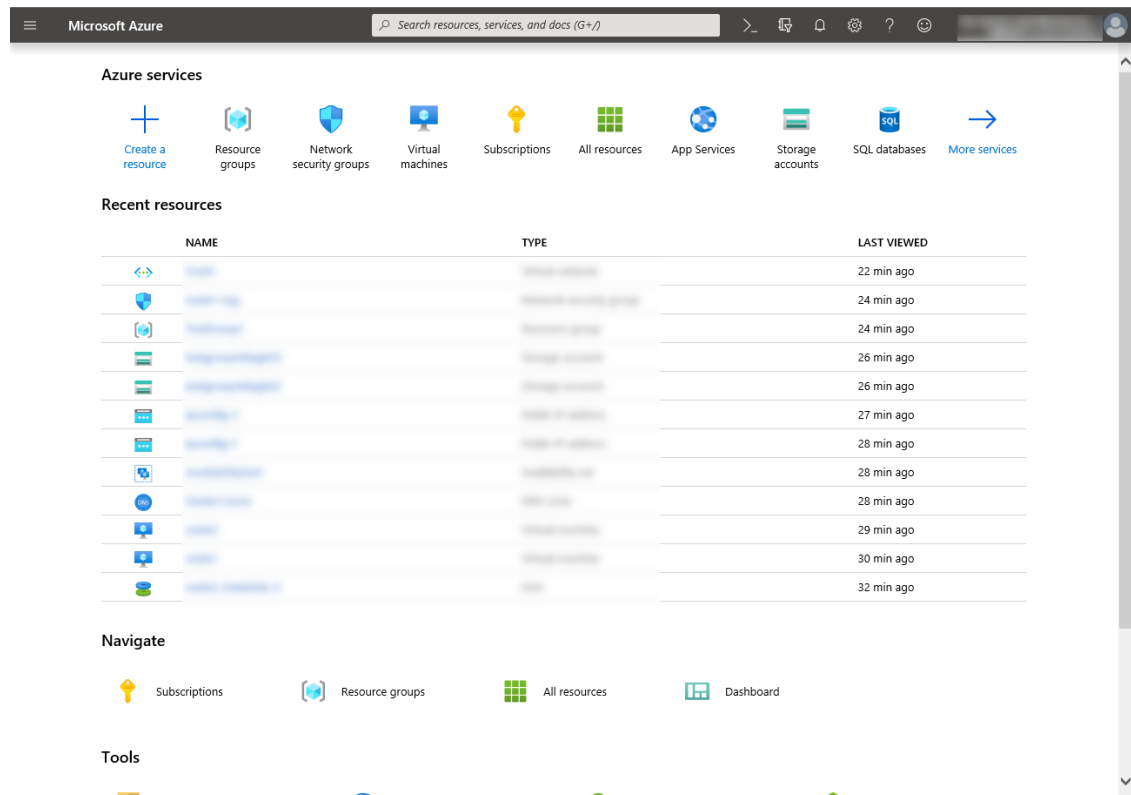
Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	Name	mdw1
Azure probe port monitor resource	Name	azureppw1
	Recovery Target	azurepp1
Azure load balance monitor resource	Name	aurelbw1
	Recovery Target	azurepp1

6.2 Configuring Microsoft Azure

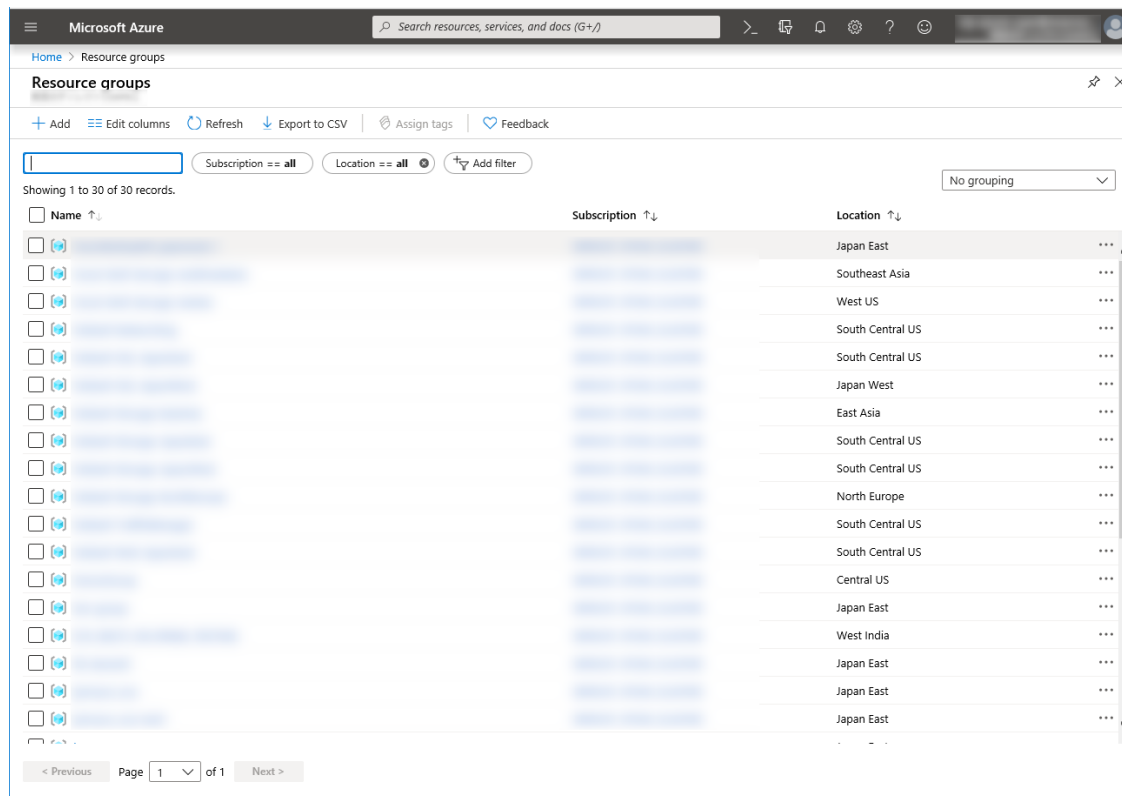
1) Creating a resource group

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create a resource group following the steps below.

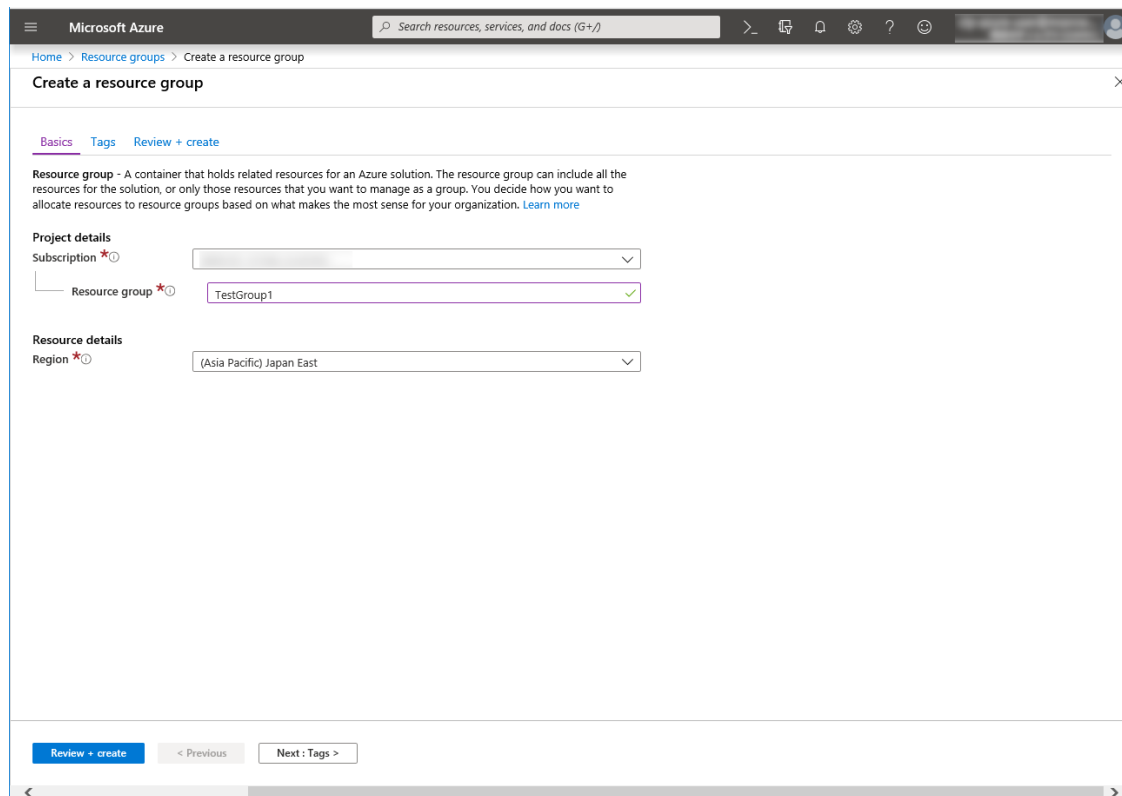
1. Select **Resource groups** on the upper part of the window. If there are existing resource groups, they are displayed in a list.



2. Select **+Add** on the upper part of the window.



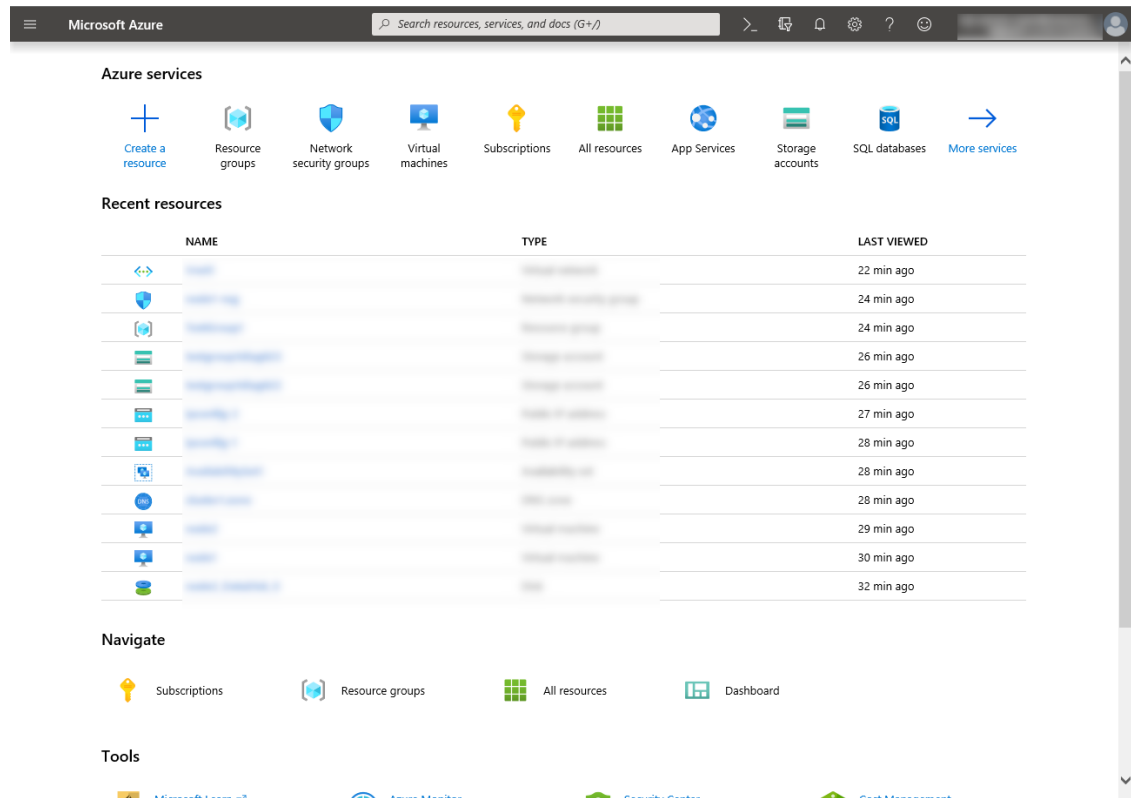
3. Specify **Subscription**, **Resource group**, and **Region**, and click **Review+Create**.



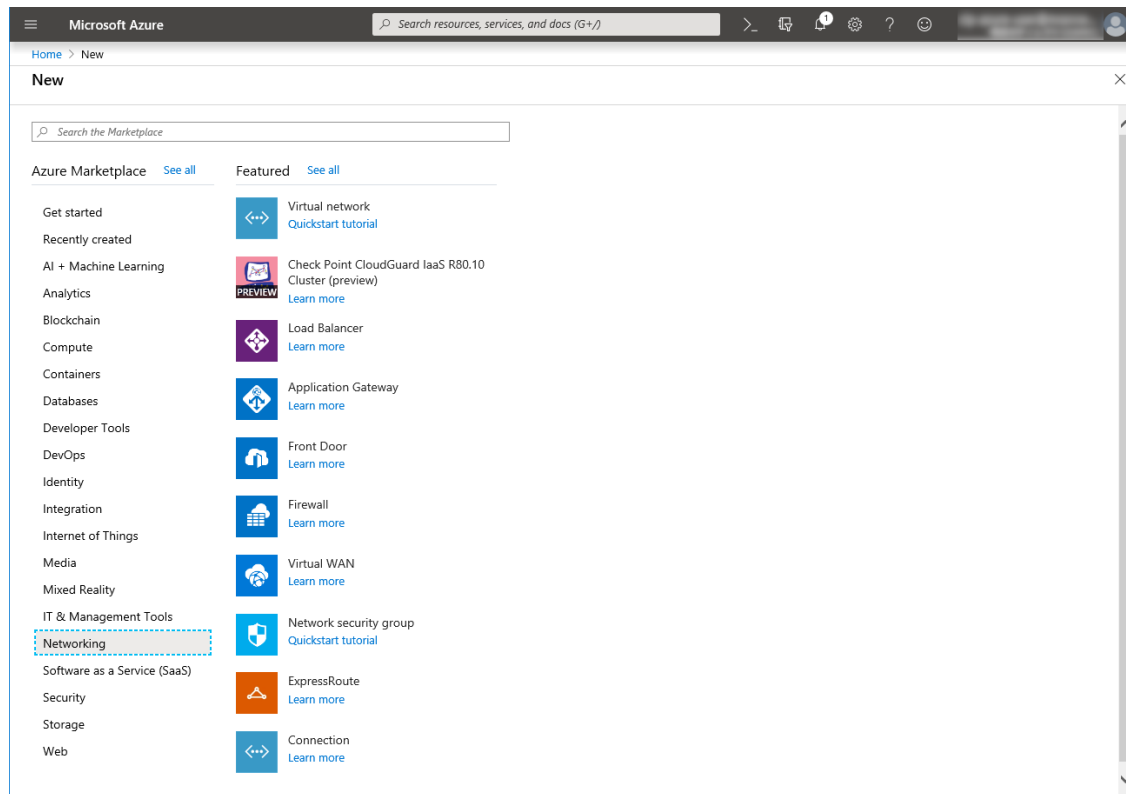
2) **Creating a virtual network**

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create a virtual network following the steps below.

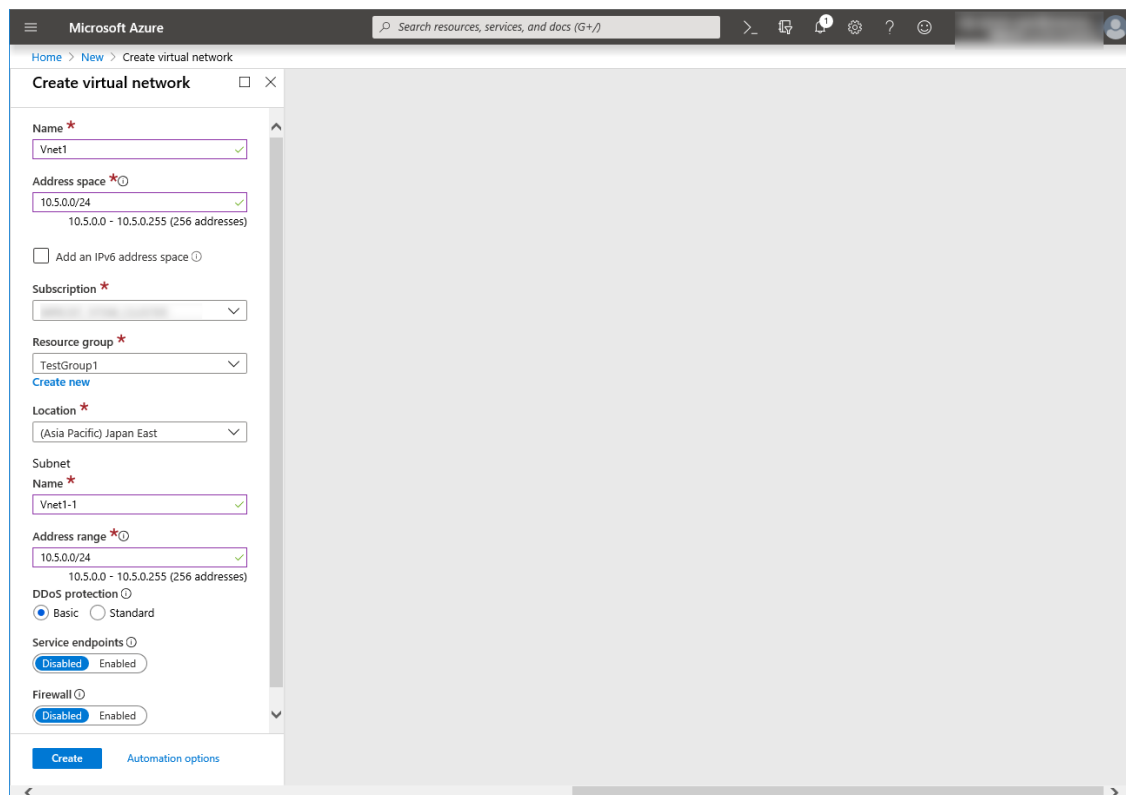
1. Select **Create a resource** on the upper part of the window.



2. Select **Networking** and then **Virtual network**.



3. Specify Name, Address space, Subscription, Resource group, Location, Name of Subnet, and Address range, and click Create.

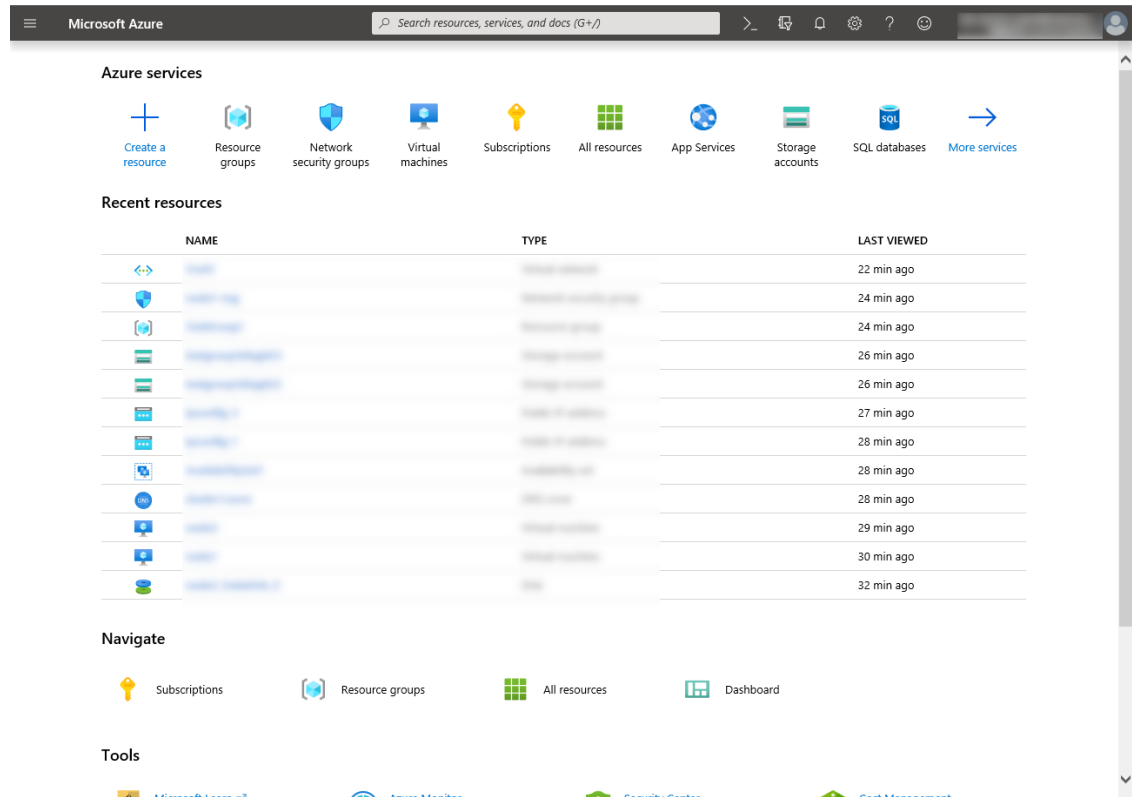


3) Creating a virtual machine

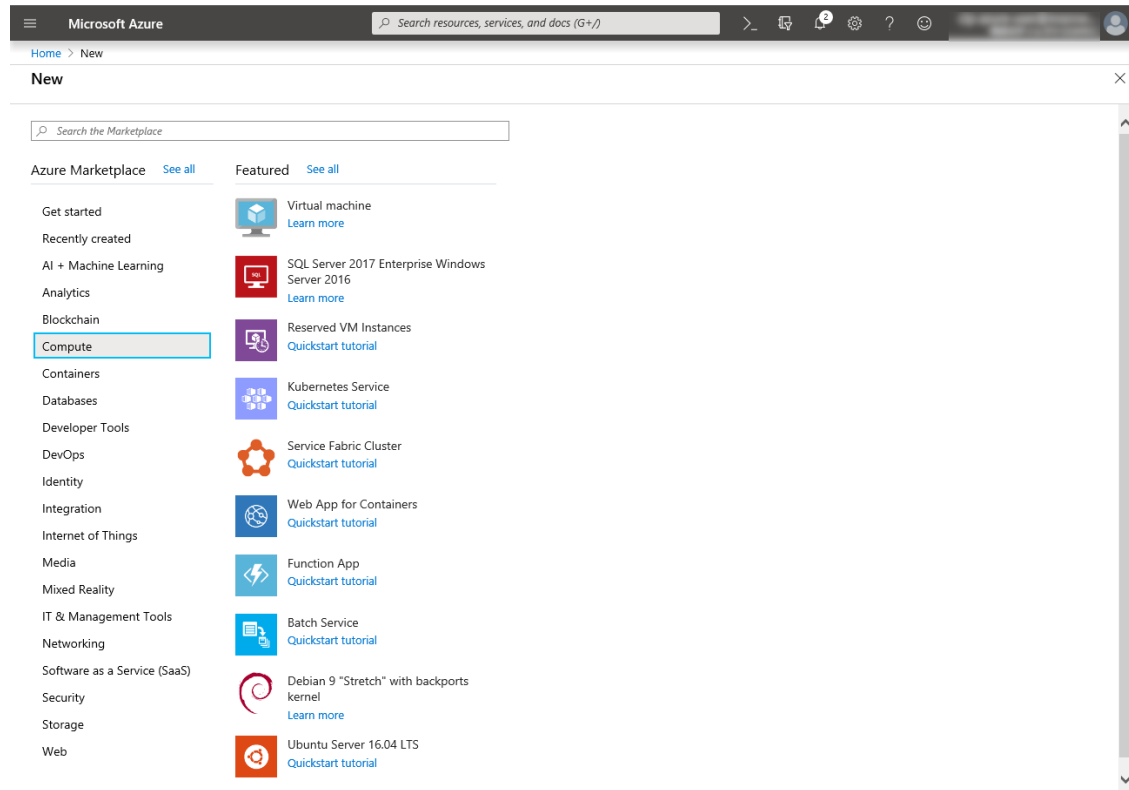
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create virtual machines and disks following the steps below.

Create as many virtual machines as required to create a cluster. Create node-1 and then node-2.

1. Select **Create a resource** on the upper part of the window.



2. Select **Compute** and then **See all**.



3. Select **Windows Server 2016 Datacenter**.
4. When the **Basics** tab appears, specify the settings of **Subscription**, **Resource group**, **Virtual machine name**, **Region**, **Image**, **Size**, **Username**, **Password**, and **Confirm password**.
Select **Availability set** from **Availability options**, and click **Create new** under the **Availability set** field.
When the **Create new** blade appears, specify the settings of **Name**, **Fault domains**, and **Update domains**. Then click **OK**.

The image displays two screenshots of the Microsoft Azure portal's 'Create a virtual machine' wizard, specifically the 'Basics' tab.

Top Screenshot: Shows the initial configuration steps. The 'Project details' section includes 'Subscription' and 'Resource group' (TestGroup1). The 'Instance details' section includes 'Virtual machine name' (node-1), 'Region' (Asia Pacific) Japan East, 'Availability options' (Availability set), and 'Image' (Windows Server 2016 Datacenter). Navigation buttons at the bottom include 'Review + create', '< Previous', and 'Next : Disks >'. A 'Create new' link is visible under the 'Resource group' and 'Availability set' fields.

Bottom Screenshot: Shows the 'Create new' sidebar on the right, which is used to create a new availability set. It includes a 'Name' field (AvailabilitySet-1), 'Fault domains' (2), 'Update domains' (5), and 'Use managed disks' (Yes (Aligned)). The 'Availability set' dropdown in the main form is highlighted with a red border and an error message: 'The value must not be empty.' The 'Next : Disks >' button is also visible at the bottom.

Click **Change size** to display the **Select a VM size** blade.

From the list, choose a size (**A1 - Standard** in this guide) suitable for your virtual machine and click **Select**.

Regarding the **Virtual machine name**, node-1 is for node-1, and node-2 is for node-2.

Click **Next: Disks >**

5. When the **Disks** tab appears, go through the following steps to add a disk to be used for a mirror disk (cluster partition or data partition).

From the **DATA DISKS** list, click **Create and attach a new disk**.

The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal. The 'Disks' tab is selected. The 'Disk options' section shows 'OS disk type' set to 'Standard HDD' and 'Enable Ultra Disk compatibility' set to 'No'. The 'Data disks' section includes a table with columns: LUN, Name, Size (GiB), Disk type, and Host caching. Below the table are links for 'Create and attach a new disk' and 'Attach an existing disk'. At the bottom, there is an 'Advanced' section and navigation buttons: 'Review + create', '< Previous', and 'Next : Networking >'.

6. The **Create a new disk** blade appears.

Specify **Name**, **Source type**, and **Size**. Then click **OK**.

Click **Next: Networking >**

The screenshot shows the 'Create a new disk' blade in the Microsoft Azure portal. The 'Name' field is set to 'node-1_DataDisk_0'. The 'Source type' is set to 'None (empty disk)'. The 'Size' is set to '20 GiB' with 'Standard HDD' as the disk type. There is a 'Change size' link. At the bottom, there is an 'OK' button.

7. The **Networking** tab appears.

Specify the settings of **Virtual network**, **Subnet**, **Network security group**, and **Configure network security group**.

Click **Create new** under the **Configure network security group** field to display the **Create network security group** blade. Specify the setting of **Name** and then click **OK**.

Click **Next: Management >**.

The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal, with the 'Networking' tab selected. The blade has a header with 'Home > New > Create a virtual machine' and a search bar. Below the header, there are tabs for 'Basics', 'Disks', 'Networking' (selected), 'Management', 'Advanced', 'Tags', and 'Review + create'. The main content area is titled 'Network interface' and contains the following settings:

- Virtual network ***: A dropdown menu showing 'Vnet1' with a 'Create new' link below it.
- Subnet ***: A dropdown menu showing 'Vnet1-1 (10.5.0.0/24)' with a 'Manage subnet configuration' link below it.
- Public IP**: A dropdown menu showing 'None' with a 'Create new' link below it.
- NIC network security group**: Radio buttons for 'None', 'Basic', and 'Advanced' (selected).
- Configure network security group ***: A dropdown menu showing '(new) node-1-nsg' with a 'Create new' link below it.
- Accelerated networking**: Radio buttons for 'On' and 'Off' (selected). A note below states: 'The selected VM size does not support accelerated networking.'

At the bottom, there is a 'Load balancing' section with a note: 'You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)'. At the very bottom, there are three buttons: 'Review + create' (blue), '< Previous', and 'Next: Management >' (disabled).

8. The **Management** tab appears.

Click **Create new** under the **Diagnostics storage account** field to display the **Create storage account** blade.

Specify the settings of **Name**, **Account kind**, and **Replication**. Then click **OK**.

In the **Diagnostics storage account** field, the default value is automatically generated and entered.

Click **Next: Advanced >**.

Microsoft Azure Search resources, services, and docs (G+/I)

Home > New > Create a virtual machine

Create a virtual machine

Basics Disks Networking Management **Advanced** Tags Review + create

Configure monitoring and management options for your VM.

Azure Security Center
 Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

✓ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Boot diagnostics ☒ On ☐ Off

OS guest diagnostics ☐ On ☒ Off

Diagnostics storage account ☒ testgroup1diag600 [Create new](#)

Identity

System assigned managed identity ☐ On ☒ Off

Azure Active Directory

Login with AAD credentials (Preview) ☐ On ☒ Off

[Review + create](#) < Previous Next: Advanced >

9. Click **Next: Tags >**.

Microsoft Azure Search resources, services, and docs (G+/I)

Home > New > Create a virtual machine

Create a virtual machine

Basics Disks Networking Management Advanced **Tags** Review + create

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions
 Extensions provide post-deployment configuration and automation.
 Extensions [Select an extension to install](#)

Cloud init
 Cloud init is a widely used approach to customize a Linux VM as it boots for the first time. You can use cloud-init to install packages and write files or to configure users and security. [Learn more](#)

The selected image does not support cloud init.

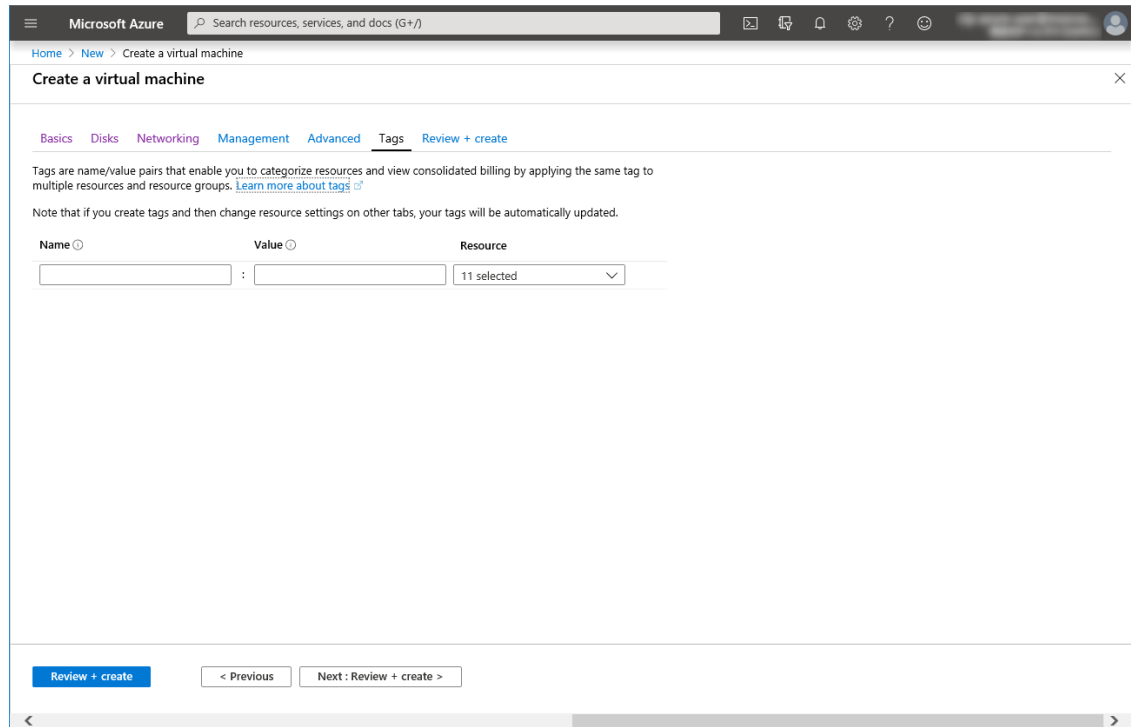
Host
 Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

Host group No host group found

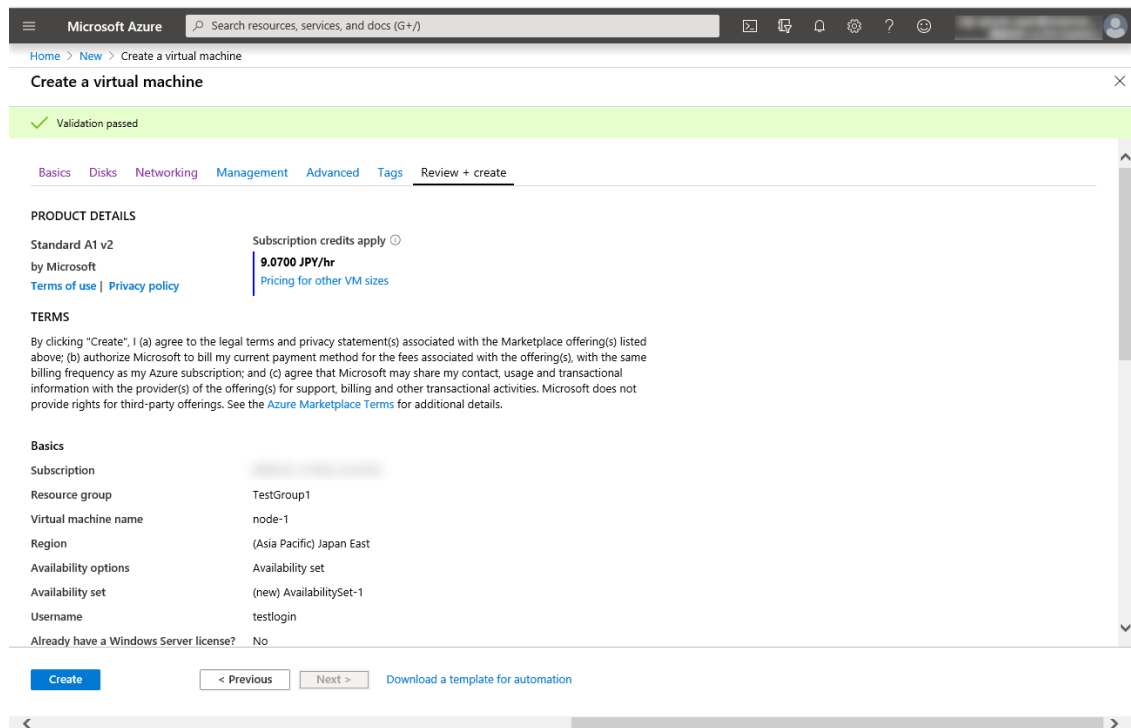
Dedicated hosts cannot be used with availability sets.

[Review + create](#) < Previous Next: Tags >

10. Click **Next: Review + create >**.



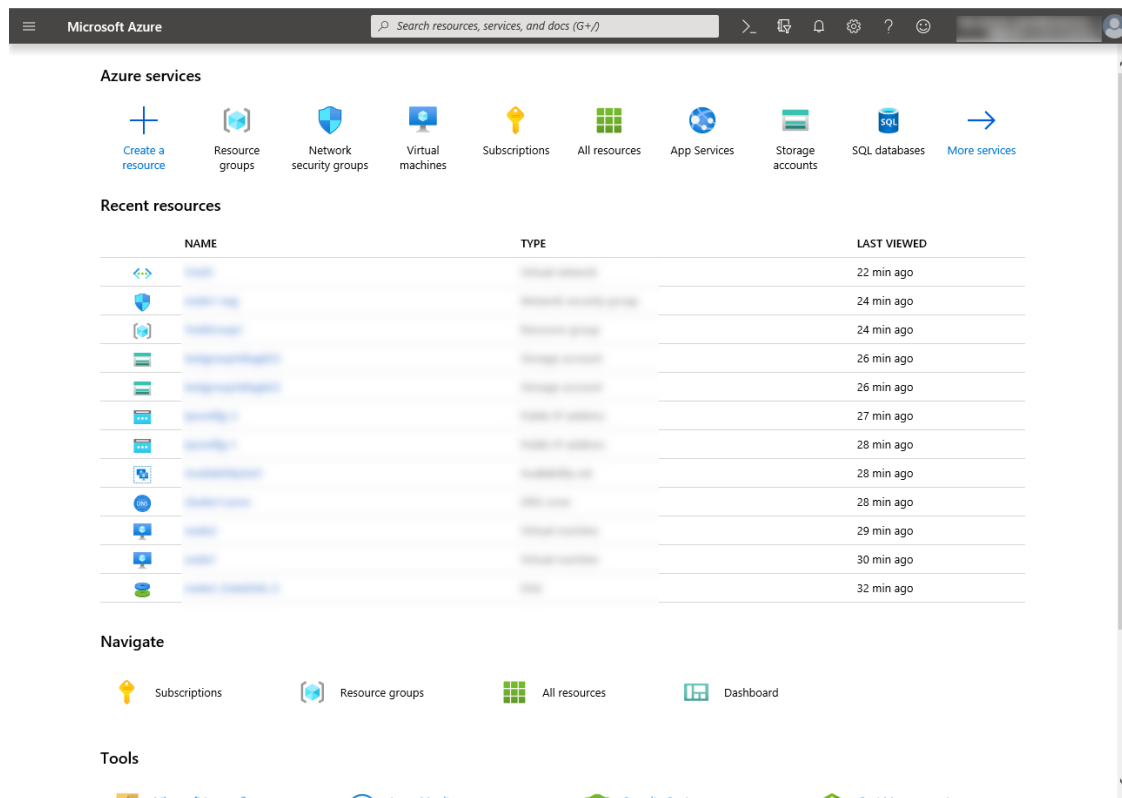
11. The **Review + create** tab appears. Check the contents. If there is no problem, click **Create**. The deployment starts and takes several minutes.



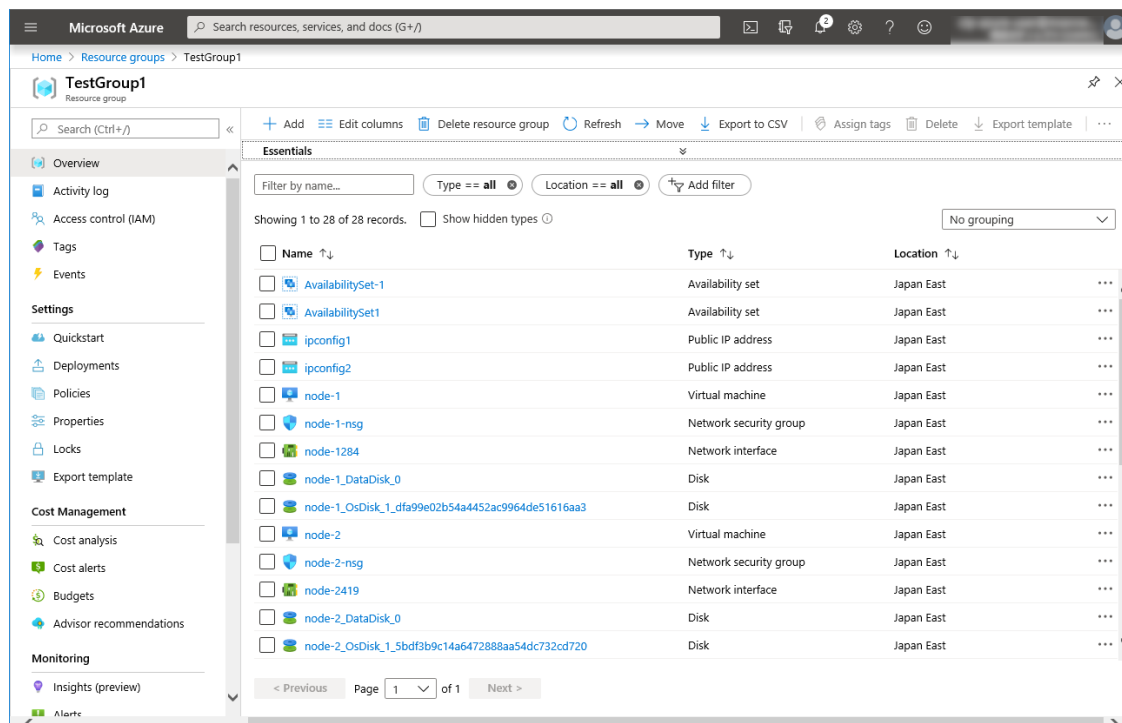
4) Setting a private IP address

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and change the private IP address setting following the steps below. Since an IP address is initially set to be assigned dynamically, change the setting so that an IP address is assigned statically. Change the settings of node-1 and then node-2.

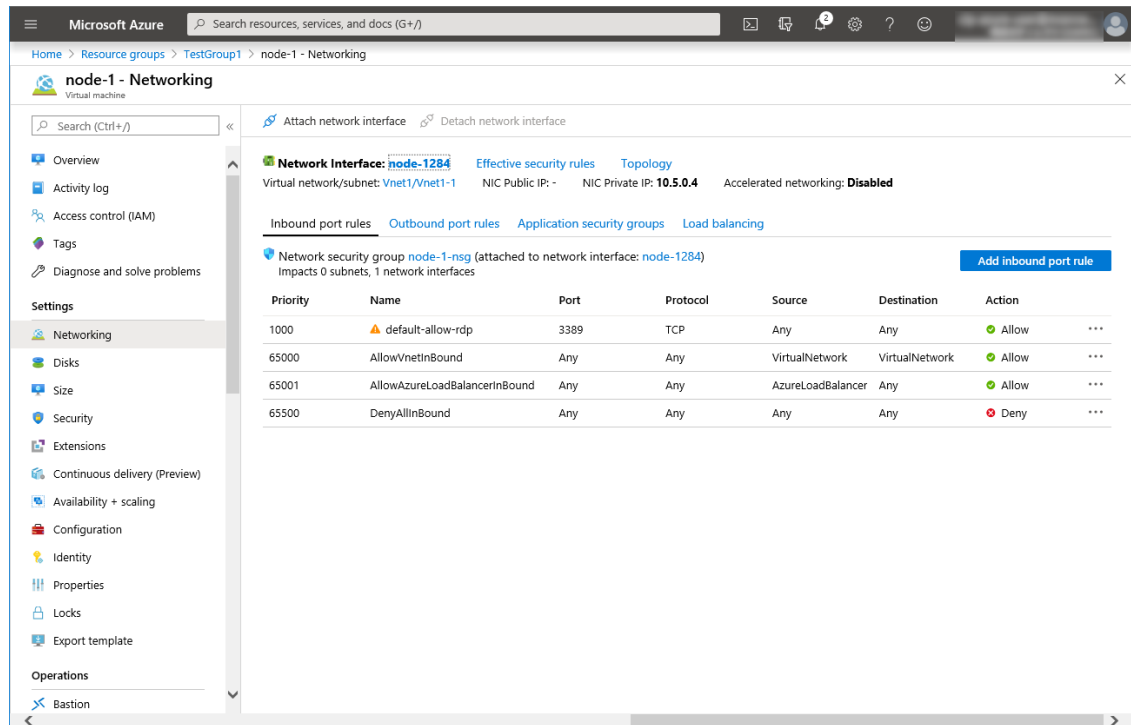
1. Select **Resource groups** on the upper part of the window.



2. Select TestGroup1 from the resource group list.
3. The summary of TestGroup1 is displayed. Select virtual machine node-1 or node-2 from the item list.

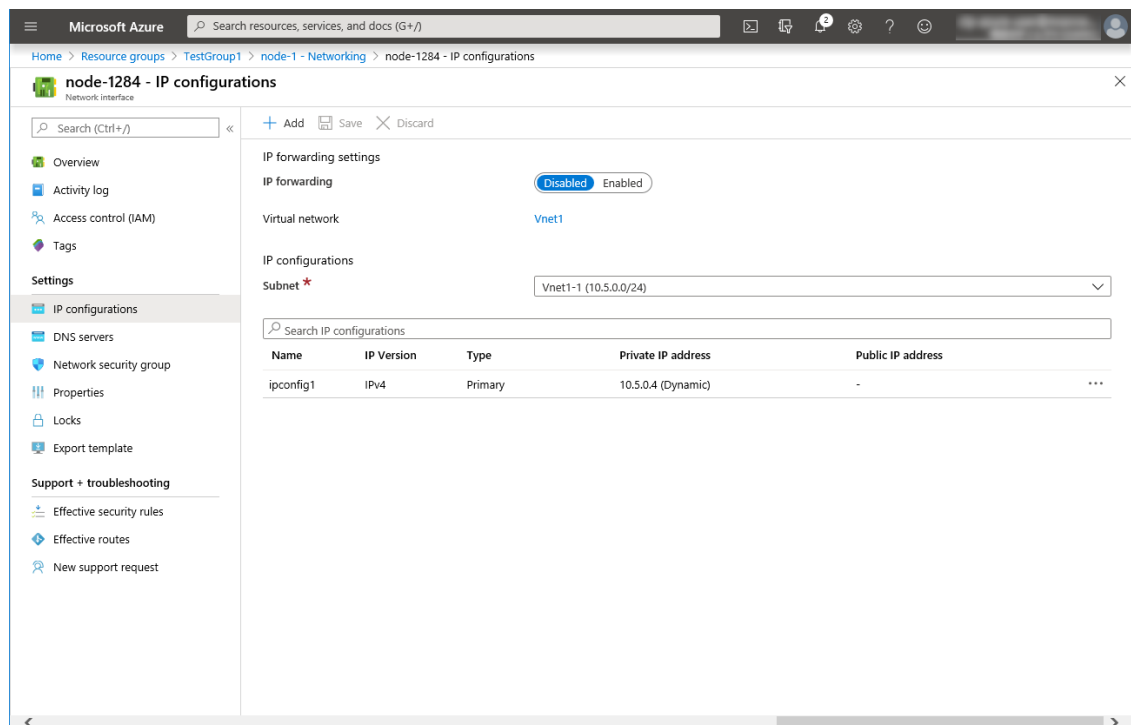


4. Select Networking.



5. Select a network interface displayed in the list. The network interface name is generated automatically.

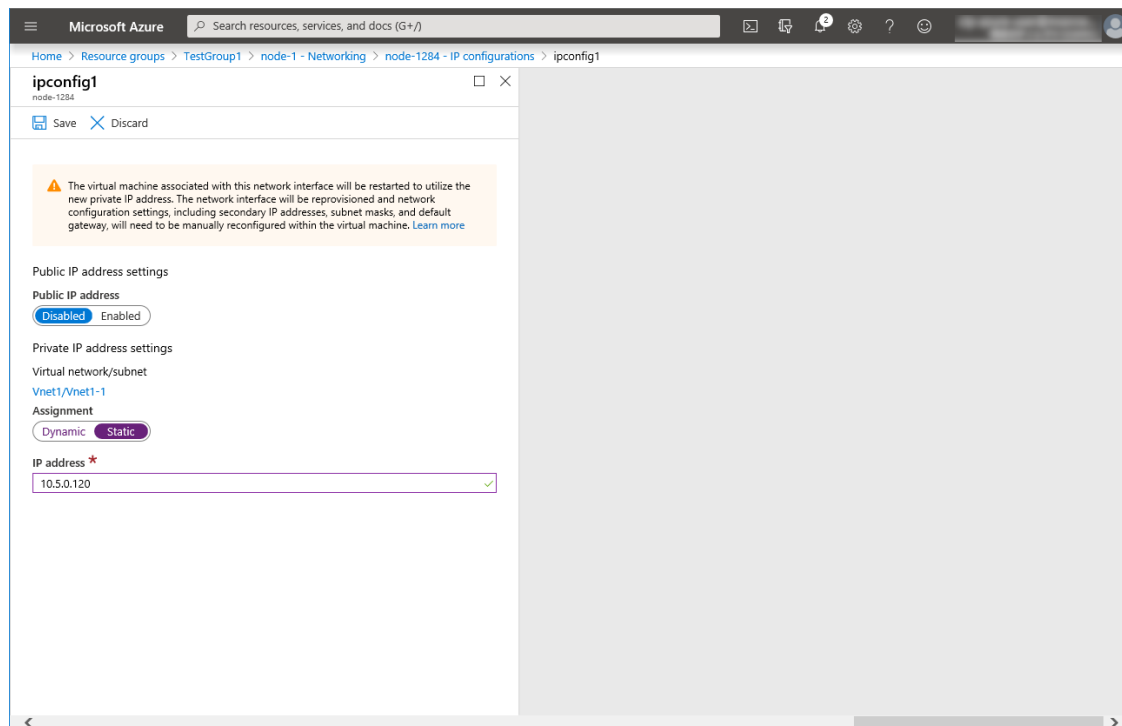
6. Select IP configurations.



7. Only ipconfig1 is displayed in the list. Select it.

8. Select **Static** for **Assignment** under **Private IP address settings**. Enter the IP address to be assigned

statically in the **IP address** text box and click **Save** at the top of the window. The IP address of node-1 is 10.5.0.120. The IP address of node-2 is 10.5.0.121.



9. The virtual machines restart automatically so that new private IP addresses can be used.

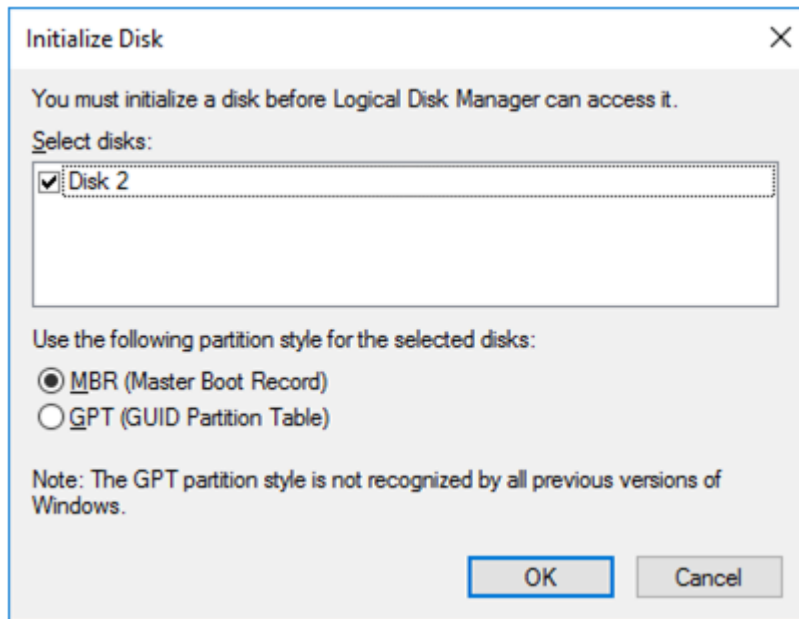
5) Configuring virtual machines

Log in to the created node-1 and node-2 and specify the settings following the procedure below.

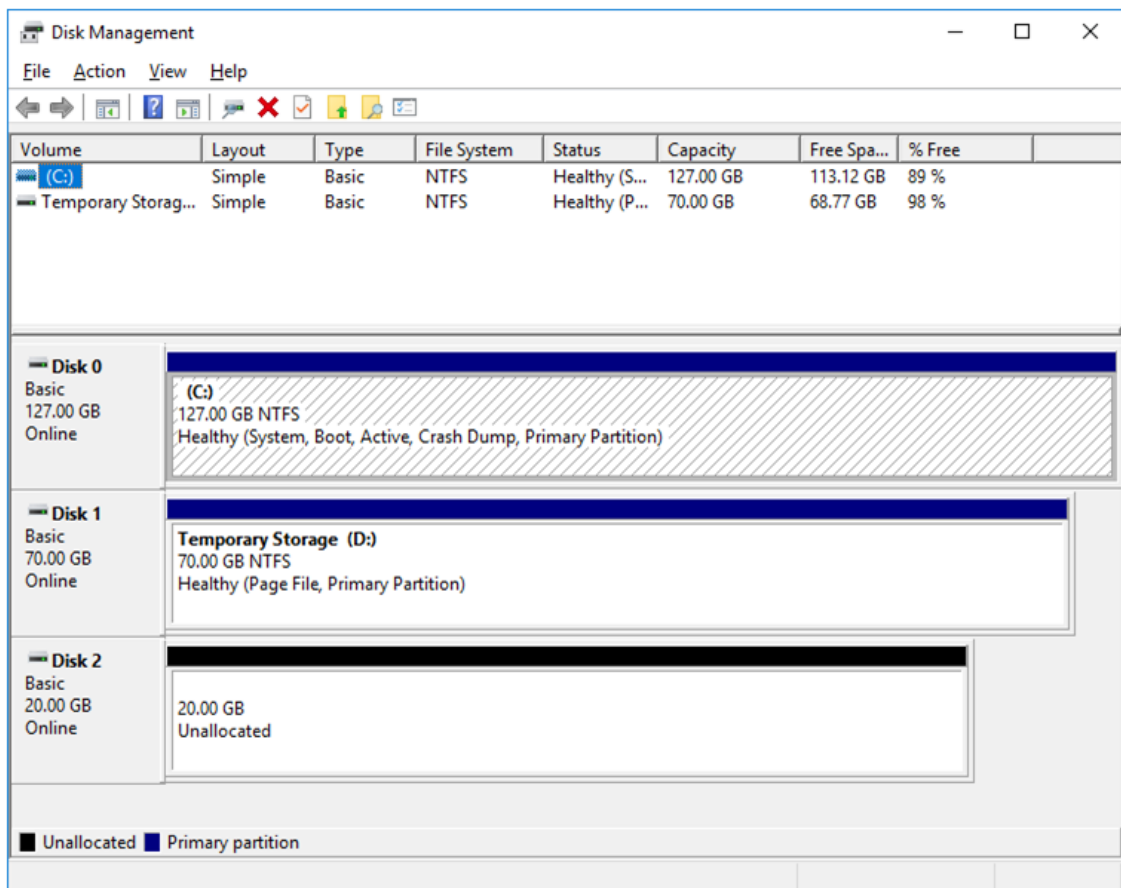
Set a partition for the mirror disk resource. Create a file system in the added disk.

For details about a partition for the mirror disk resource, see "Partition settings for mirror disk resource (when using Replicator)" in "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.

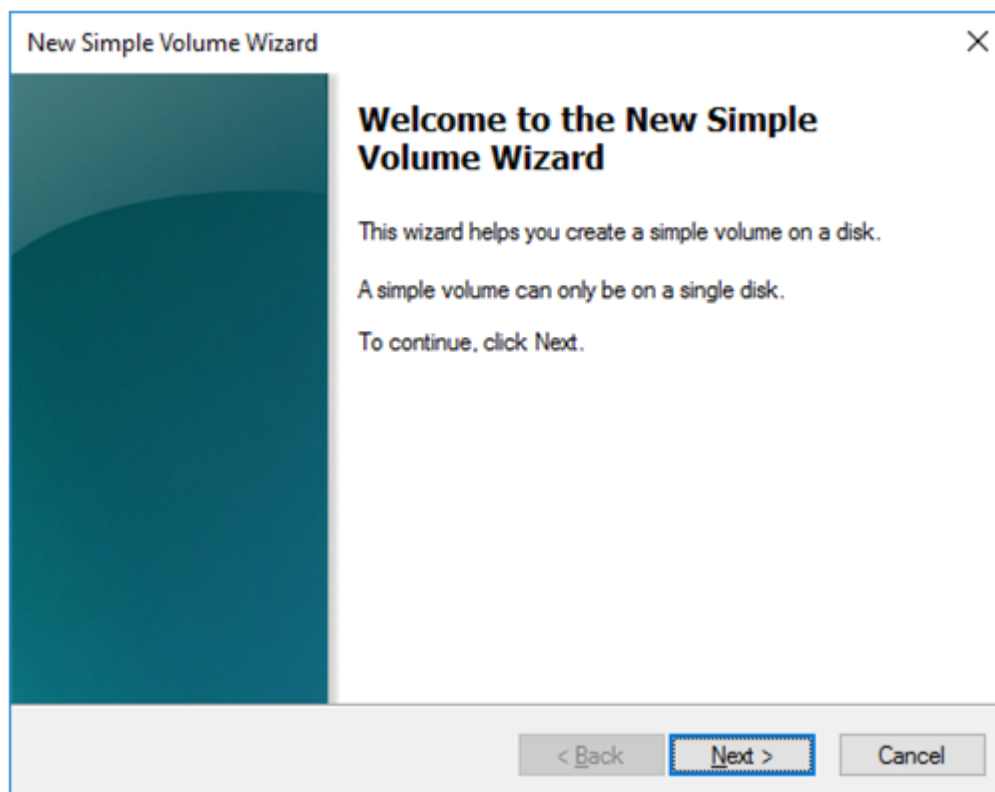
1. Open the **Disk Management** window. The **Initialize Disk** dialog box is displayed.



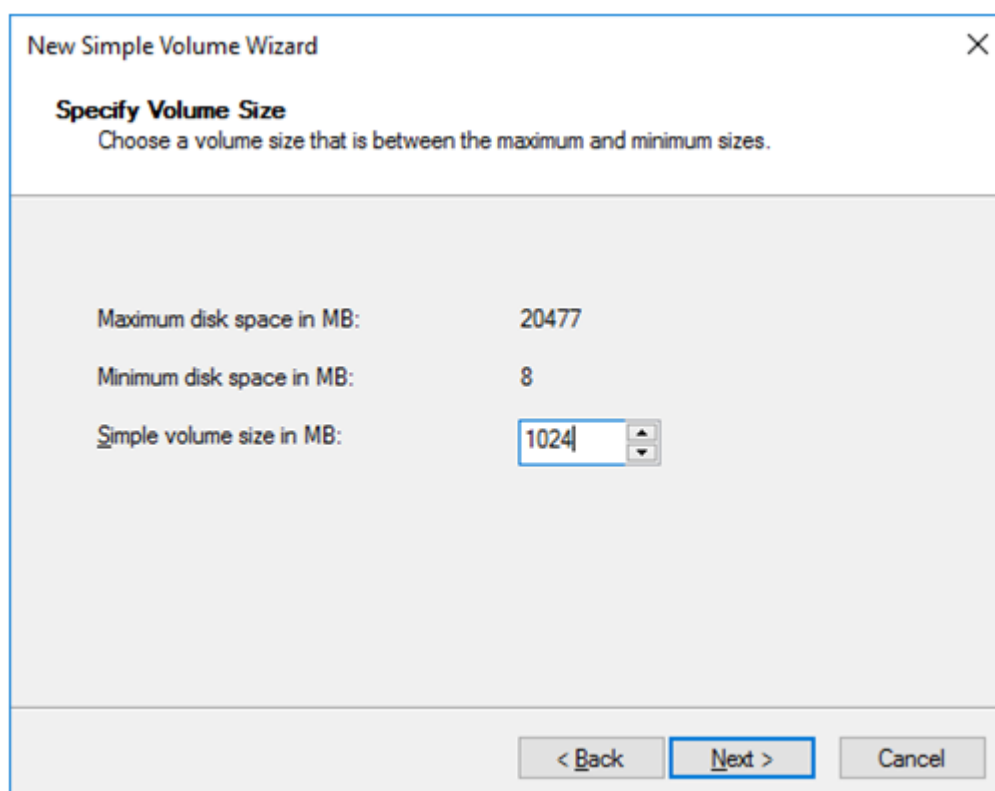
2. Confirm that the added disk is displayed as "Disk 2" in unassigned state under the existing C drive and D drive.



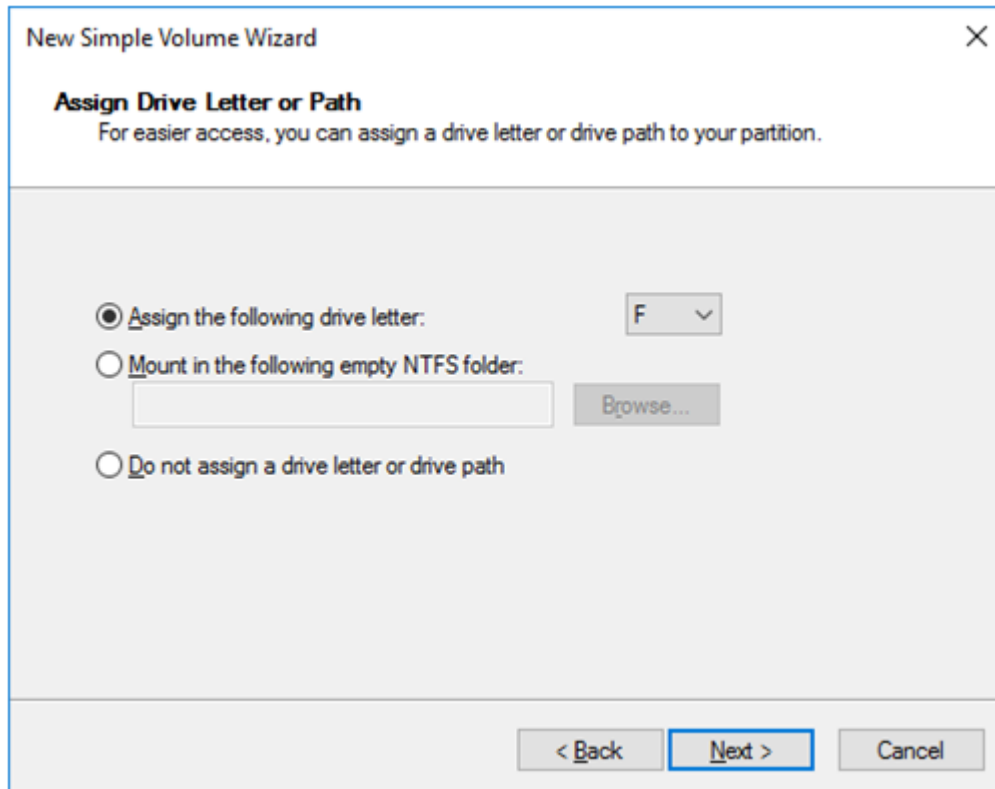
3. Create a cluster partition. Right-click "Disk 2" and select **New Simple Volume**.
4. The **Welcome to the New Simple Volume Wizard** is displayed. Click **Next**.



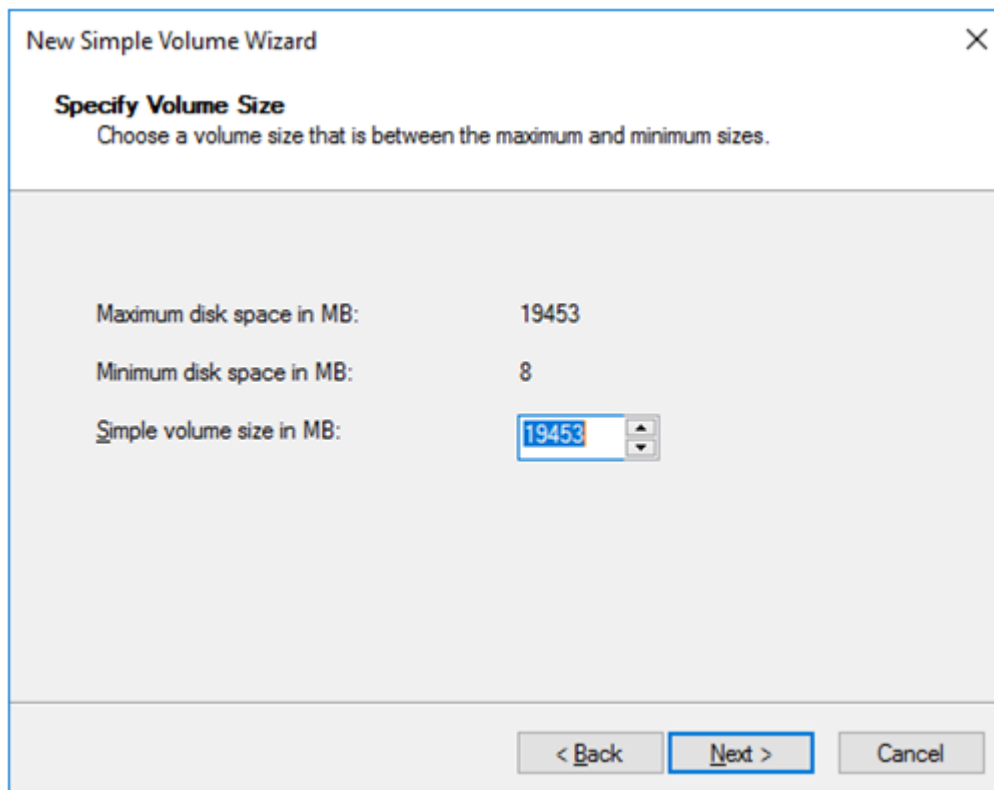
5. The **Specify Volume Size** window is displayed. Allocate 1024 MB (1,073,741,824 bytes) or more to a cluster partition. Click **Next**.



6. The **Assign Drive Letter or Path** window is displayed. Select the F drive for **Assign the following drive letter:**. Use the disk as a raw partition without formatting.



7. Next, create a data partition. Right-click "Disk 2" and select **New Simple Volume**.
8. The **Welcome to the New Simple Volume Wizard** is displayed. Click **Next**.
9. The **Specify Volume Size** window is displayed. Click **Next**.



The screenshot shows the 'New Simple Volume Wizard' window, specifically the 'Specify Volume Size' step. The window title is 'New Simple Volume Wizard' with a close button (X) in the top right corner. Below the title bar, the section is titled 'Specify Volume Size' with the instruction 'Choose a volume size that is between the maximum and minimum sizes.' The main area contains three labels and their corresponding values: 'Maximum disk space in MB:' with the value '19453', 'Minimum disk space in MB:' with the value '8', and 'Simple volume size in MB:' with a text box containing '19453' and a spinner control. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

New Simple Volume Wizard

Specify Volume Size
Choose a volume size that is between the maximum and minimum sizes.

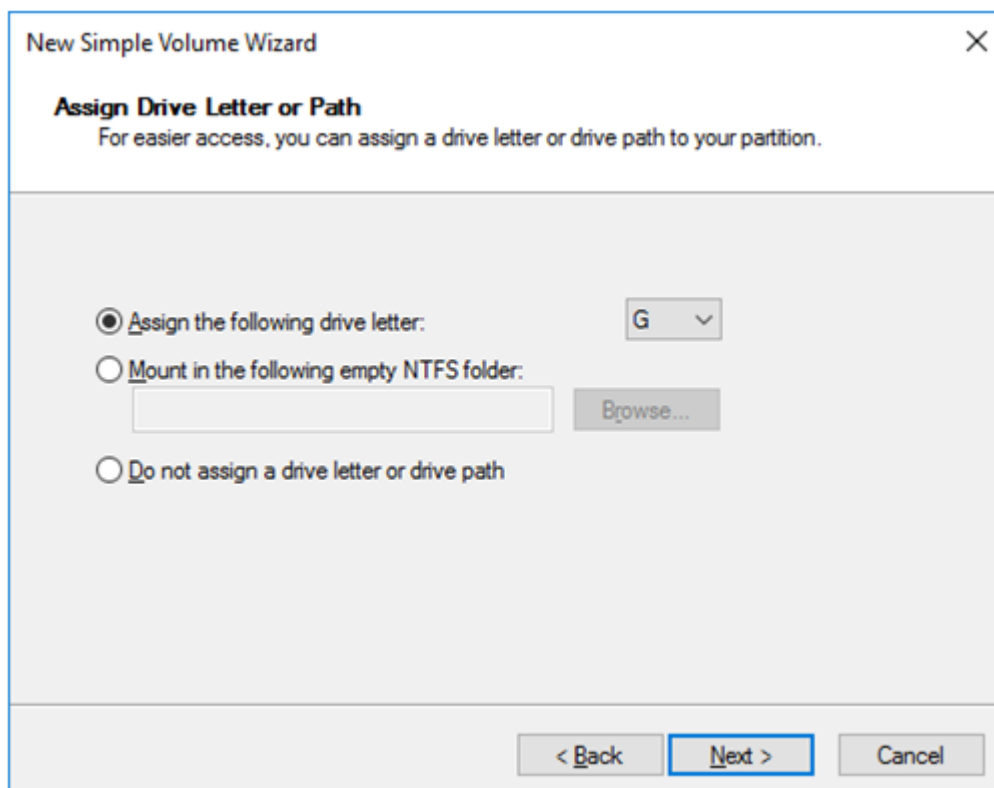
Maximum disk space in MB: 19453

Minimum disk space in MB: 8

Simple volume size in MB: 19453

< Back Next > Cancel

10. The **Assign Drive Letter or Path** window is displayed. Select the G drive for **Assign the following drive letter:** and click Next.



The screenshot shows the 'New Simple Volume Wizard' window, specifically the 'Assign Drive Letter or Path' step. The window title is 'New Simple Volume Wizard' with a close button (X) in the top right corner. Below the title bar, the section is titled 'Assign Drive Letter or Path' with the instruction 'For easier access, you can assign a drive letter or drive path to your partition.' The main area contains three radio button options: 'Assign the following drive letter:' (selected), 'Mount in the following empty NTFS folder:', and 'Do not assign a drive letter or drive path'. The 'Assign the following drive letter:' option has a dropdown menu showing 'G'. The 'Mount in the following empty NTFS folder:' option has a text box and a 'Browse...' button. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

New Simple Volume Wizard

Assign Drive Letter or Path
For easier access, you can assign a drive letter or drive path to your partition.

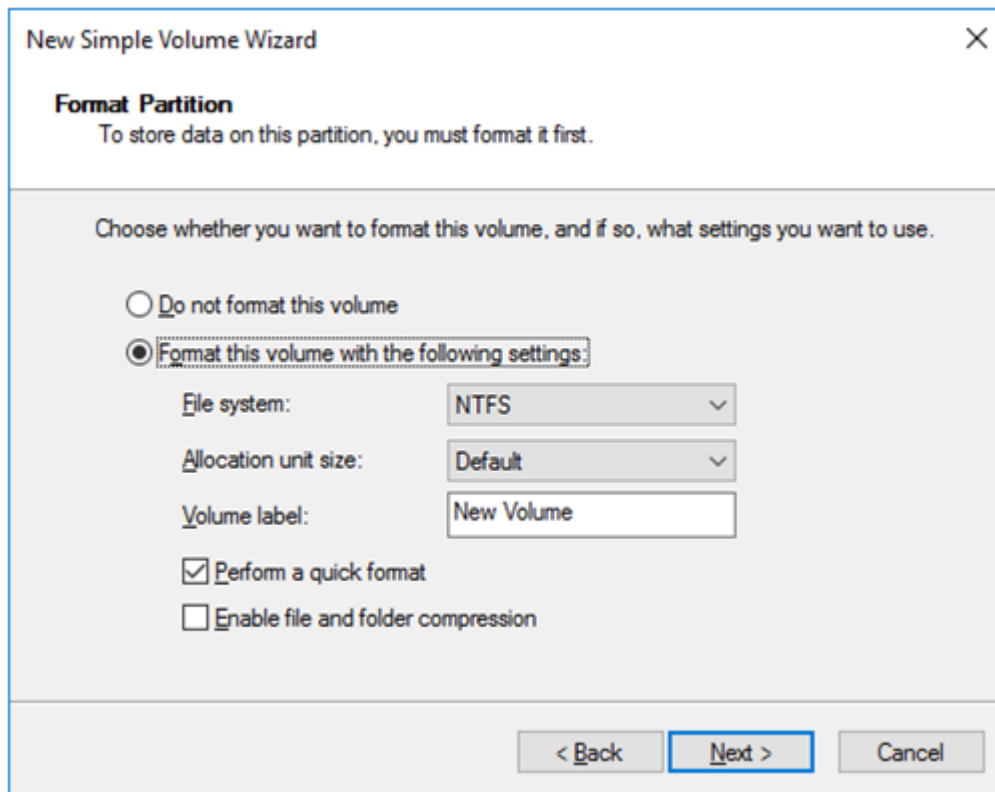
☒ Assign the following drive letter: G

☐ Mount in the following empty NTFS folder: Browse...

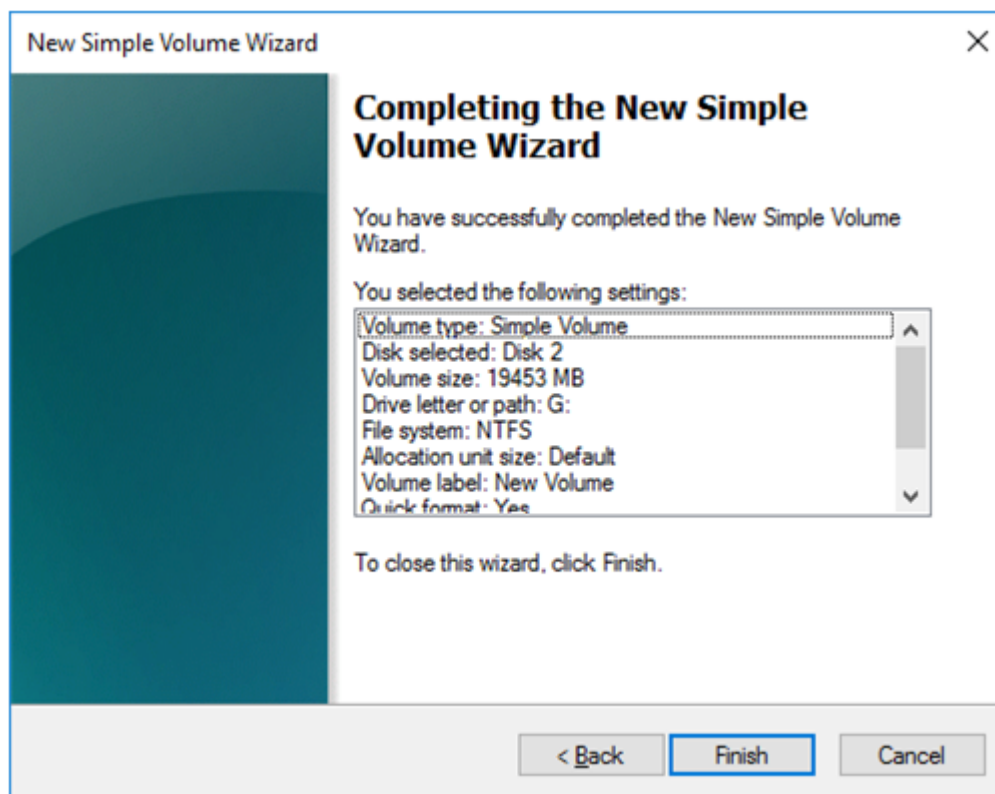
☐ Do not assign a drive letter or drive path

< Back Next > Cancel

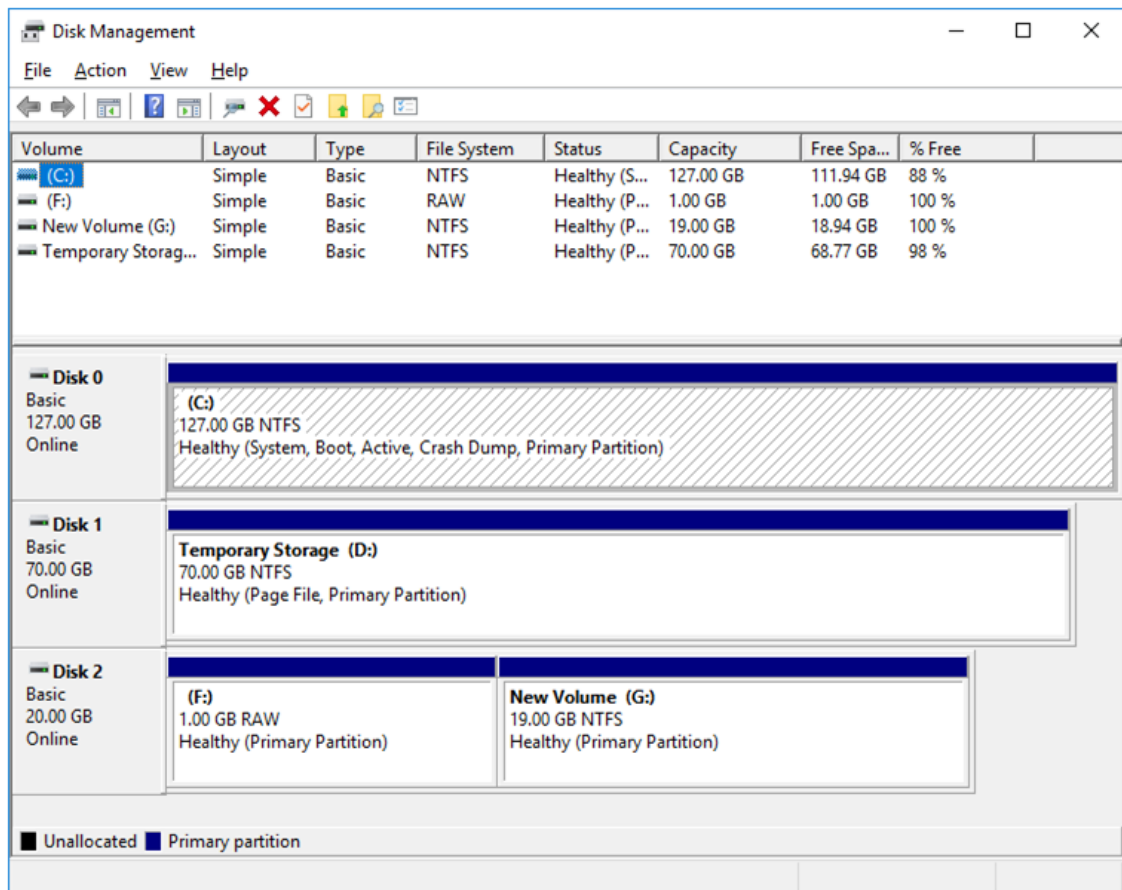
11. The **Format Partition** window is displayed. Confirm that **File System** is **NTFS**.



12. Click **Next**.
13. The **Completing the New Simple Volume Wizard** window is displayed. Check the displayed contents and click **Finish**.



14. Confirm that the added disks are assigned as the F drive and G drive.



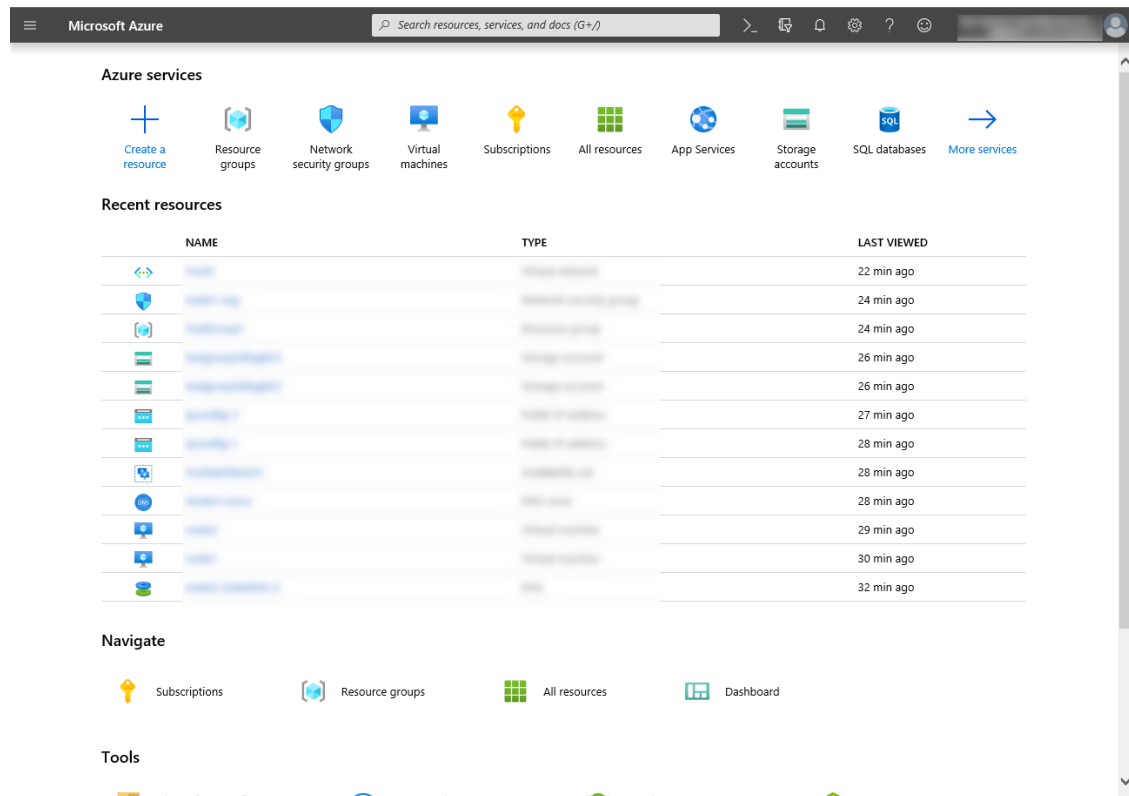
6) Configuring a load balancer

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and add an internal load balancer following the steps below.

For details, see the following websites:

- Load Balancer:
<https://docs.microsoft.com/en-us/azure/load-balancer/>

1. Select **Create a resource** on the upper part of the window.

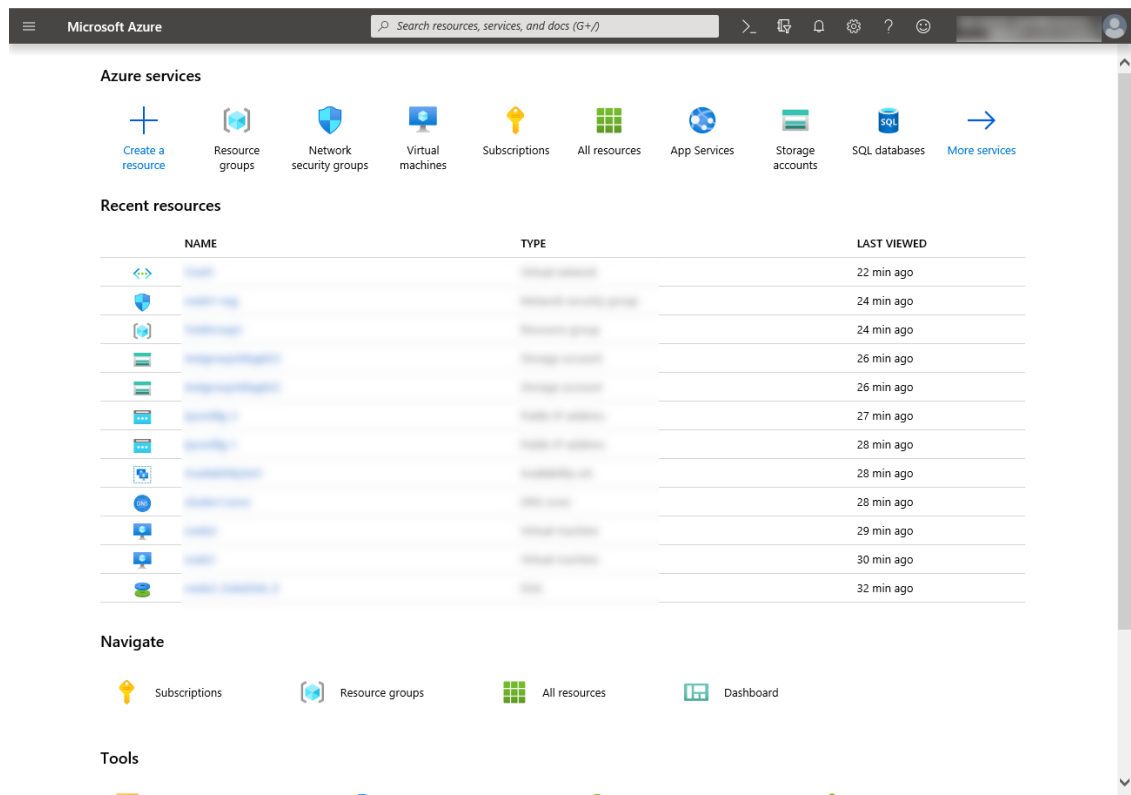


2. Select **Networking** and then **Load balancer**.
3. The **Create load balancer** blade is displayed. Specify **Name**. Select **Internal** for **Type** and **Basic** for **SKU**, respectively.
4. For **Virtual network** and **Subnet**, select the virtual network and subnet created in "2)Creating a virtual network"
5. Specify **Subscription**, **Resource group**, and **Region**, and click **Review+create**. Then click **Create**. Deploying the load balancer starts. This processing takes several minutes.

The screenshot shows the 'Create load balancer' wizard in the Microsoft Azure portal, specifically the 'Basics' tab. The page title is 'Create load balancer'. Below the title, there are tabs for 'Basics', 'Tags', and 'Review + create'. A descriptive paragraph explains that an Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. It uses a hash-based distribution algorithm and can be internet-facing or internal. Below this, the 'Project details' section includes a 'Subscription' dropdown and a 'Resource group' dropdown set to 'TestGroup1'. The 'Instance details' section includes a 'Name' field with 'TestLoadBalancer', a 'Region' dropdown set to '(Asia Pacific) Japan East', a 'Type' radio button set to 'Internal', and a 'SKU' radio button set to 'Basic'. The 'Configure virtual network' section includes a 'Virtual network' dropdown set to 'Vnet1' and a 'Subnet' dropdown set to 'Vnet1-1 (10.5.0.0/24)'. At the bottom, there are buttons for 'Review + create', '< Previous', 'Next : Tags >', and 'Download a template for automation'.

7) Configuring a load balancer (configuring a backend pool)

1. Associate a virtual machine registered to the availability set to the load balancer. After the load balancer has been deployed, select **Resource groups** on the upper part of the window.



2. Select the resource group to which the created load balancer belongs from the resource group list.

3. The summary of the selected resource group is displayed. Select the created load balancer from the item list.

The screenshot shows the Microsoft Azure portal interface for the 'TestGroup1' resource group. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Events, Settings, Cost Management, and Monitoring. The main area displays a table of resources with columns for Name, Type, and Location. The table lists 31 records, including Availability sets, DNS zones, Public IP addresses, Virtual machines, and Network security groups. The 'node-1' VM is highlighted.

Name	Type	Location
AvailabilitySet-1	Availability set	Japan East
AvailabilitySet1	Availability set	Japan East
cluster1.zone	DNS zone	global
ipconfig1	Public IP address	Japan East
ipconfig11	Public IP address	Japan East
ipconfig12	Public IP address	Japan East
ipconfig2	Public IP address	Japan East
node-1	Virtual machine	Japan East
node-1-nsg	Network security group	Japan East
node-1284	Network interface	Japan East
node-1_DataDisk_0	Disk	Japan East
node-1_OsDisk_1_dfa99e02b54a4452ac9964de51616aa3	Disk	Japan East
node-2	Virtual machine	Japan East
node-2-nsg	Network security group	Japan East
node-2410	Network interface	Japan East

4. Select **Backend pools**.

The screenshot shows the Microsoft Azure portal interface for the 'TestLoadBalancer' resource. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Frontend IP configuration, Backend pools, Health probes, Load balancing rules, Inbound NAT rules, Properties, Locks, Export template, Support + troubleshooting, and New support request. The main area displays the configuration details for the load balancer, including Resource group, Location, Subscription, and SKU. The 'Backend pools' section is highlighted in the left sidebar.

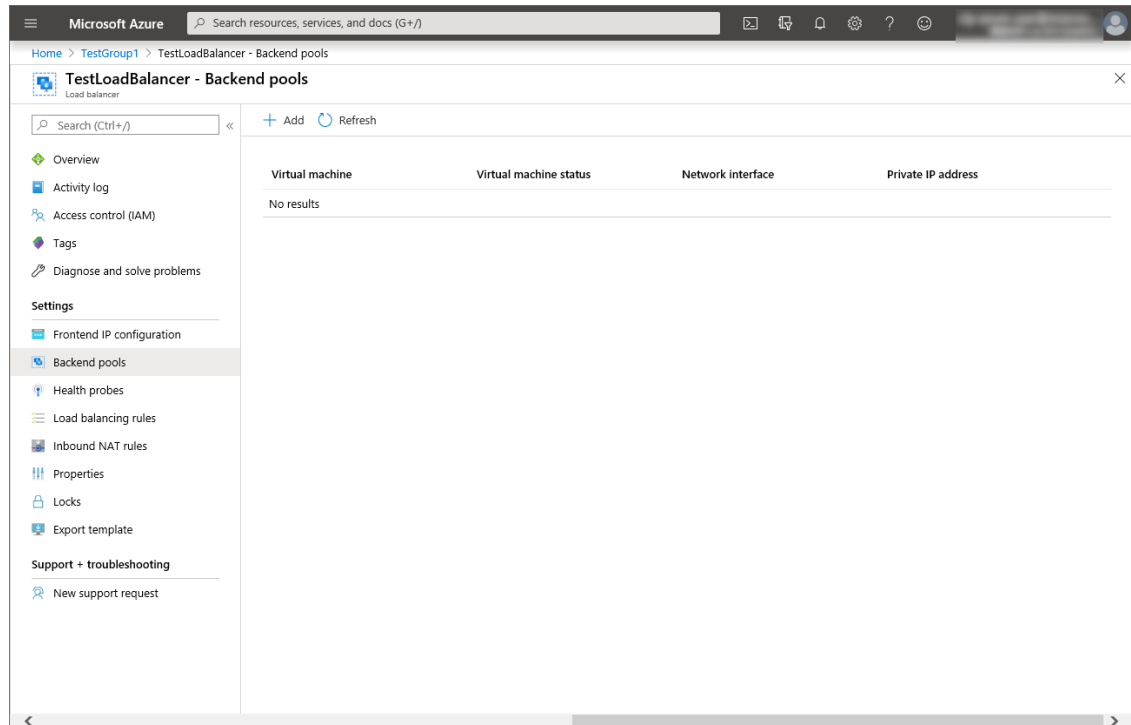
Configure high availability and scalability for your applications
Create highly-available and scalable applications in minutes by using built-in load balancing for cloud services and virtual machines. Azure Load Balancer supports TCP/UDP-based protocols and protocols used for real-time voice and video messaging applications. [Learn more](#)

Balance IPv4 and IPv6 addresses
Native dual-stack endpoints help meet regulatory requirements and address the fast-growing number of devices in mobile and IoT. [View frontend IP configuration](#)

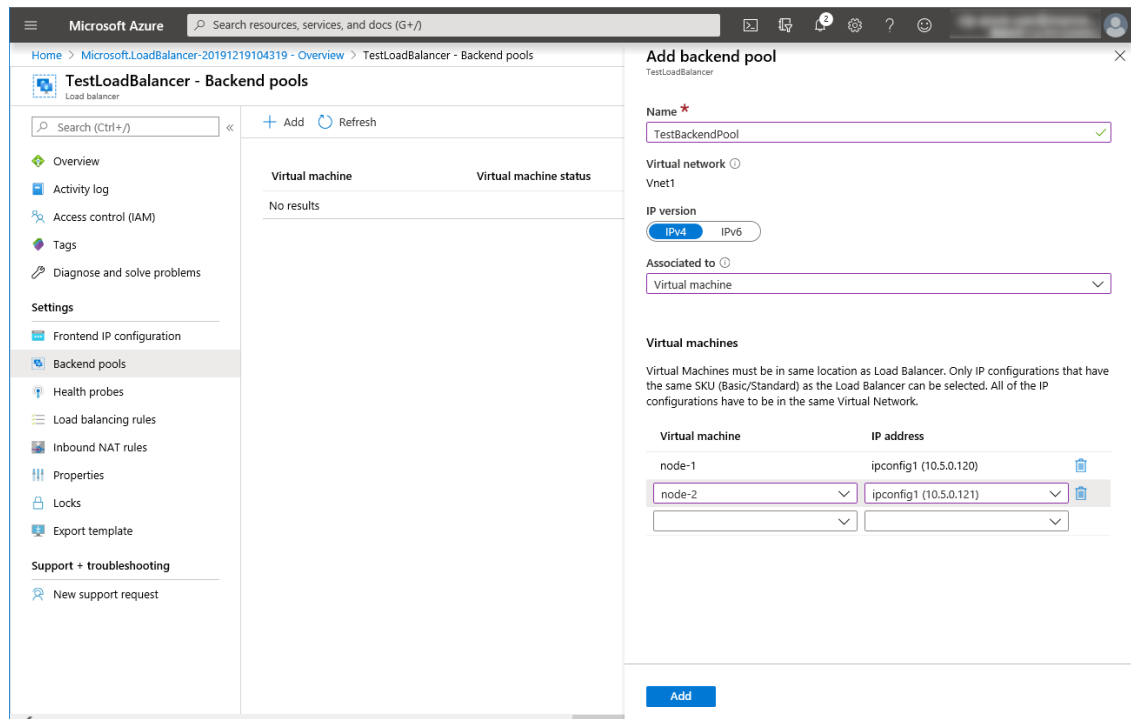
Build highly reliable applications
Load Balancer improves application uptime by routing traffic to healthy nodes. [Learn more](#) [View health probes](#)

Secure your networks
Control network traffic and protect private networks using built-in network address translation (NAT). [View backend pools](#) [View load balancing rules](#)

5. Click **Add**.

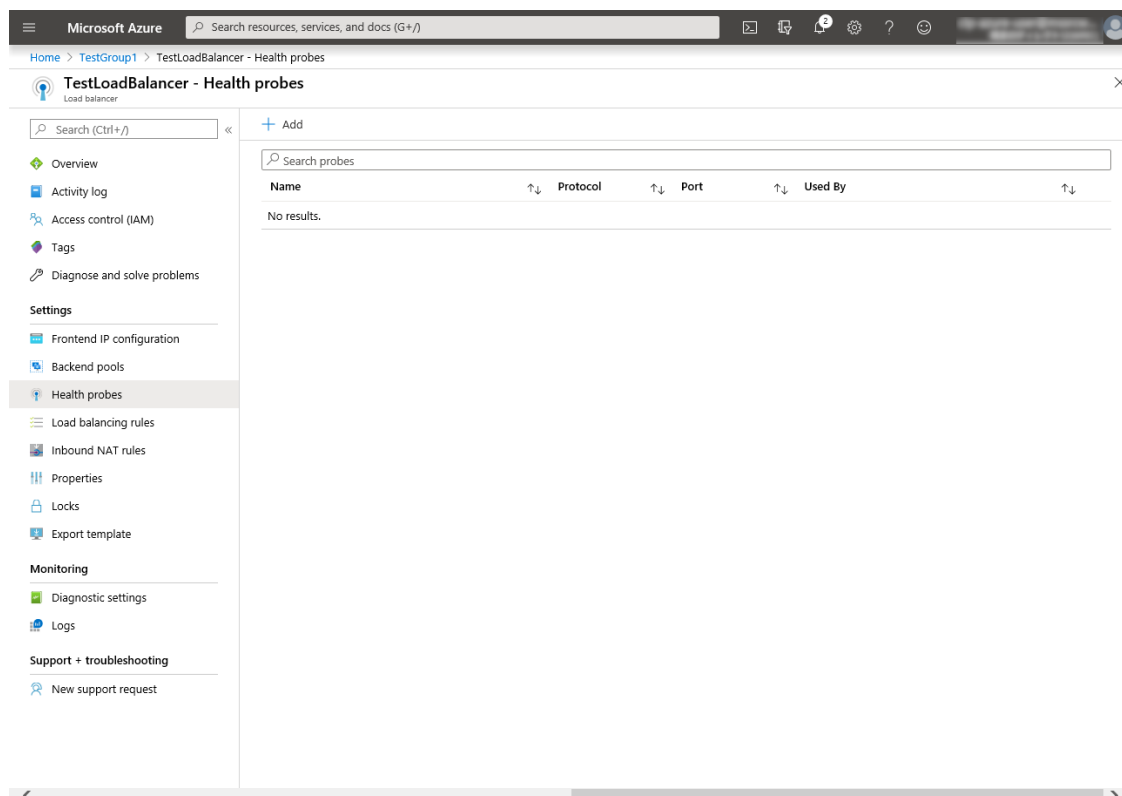


6. The **Add backend pool** blade is displayed. Specify **Name**.
7. Select **Virtual machine** for **Associated to**.
8. Specify **Virtual machine** and **IP address** for the virtual machine you want to associate. Repeat this procedure for the rest of such virtual machines.
9. Then click **Add**.



8) Configuring a load balancer (configuring a health probe)

1. Select **Health probes**.



2. Click **Add**.

3. The **Add health probe** blade is displayed. Specify **Name**.

4. Specify **Protocol** and **Port**, and click **OK**.

Microsoft Azure Search resources, services, and docs (G+/J)

Home > TestLoadBalancer - Health probes > Add health probe

Add health probe

TestLoadBalancer

Name *

Protocol

Port *

Interval * seconds

Unhealthy threshold * consecutive failures

OK

9) Configuring a load balancer (setting the load balancing rules)

1. Select Load balancing rules.

Microsoft Azure Search resources, services, and docs (G+/J)

Home > TestGroup1 > TestLoadBalancer - Load balancing rules

TestLoadBalancer - Load balancing rules

Load balancer

Search (Ctrl+/) « + Add

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Frontend IP configuration

Backend pools

Health probes

Load balancing rules

Inbound NAT rules

Properties

Locks

Export template

Monitoring

Diagnostic settings

Logs

Support + troubleshooting

New support request

Name	Load balancing rule	Backend pool	Health probe
No results.			

2. Click Add.

3. The Add load balancing rule blade is displayed. Specify Name.

4. Specify **Port** and **Backend port**, and click **OK**.

The screenshot shows the 'Add load balancing rule' configuration window in the Microsoft Azure portal. The window is titled 'Add load balancing rule' and has a close button (X) in the top right corner. The breadcrumb navigation shows 'Home > TestGroup1 > TestLoadBalancer - Load balancing rules > Add load balancing rule'. The configuration fields are as follows:

- Name ***: TestLoadBalancingRule (with a green checkmark)
- IP Version ***: ☒ IPv4 ☐ IPv6
- Frontend IP address ***: 10.5.0.200 (LoadBalancerFrontEnd)
- Protocol**: ☒ TCP ☐ UDP
- Port ***: 80
- Backend port ***: 8080 (with a green checkmark)
- Backend pool**: TestBackendPool (2 virtual machines)
- Health probe**: TestHealthProbe (TCP:26001)
- Session persistence**: None
- Idle timeout (minutes)**: 4
- Floating IP (direct server return)**: ☒ Disabled ☐ Enabled

At the bottom left, there is an 'OK' button.

10) **Adjusting the OS startup time, checking the network setting, checking the firewall setting, synchronizing the server time, and disabling the power saving function.**

For each procedure, see "Settings after configuring hardware" in "Determining a system configuration" in the Installation and Configuration Guide.

11) **Installing EXPRESSCLUSTER**

For the installation procedure, see the Installation and Configuration Guide.
After installation is complete, restart the OS.

12) **Registering the EXPRESSCLUSTER license**

For the license registration procedure, see the Installation and Configuration Guide.

6.3 Configuring the EXPRESSCLUSTER settings

For the Cluster WebUI setup and connection procedures, see "Creating the cluster configuration data" in the Installation and Configuration Guide.

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

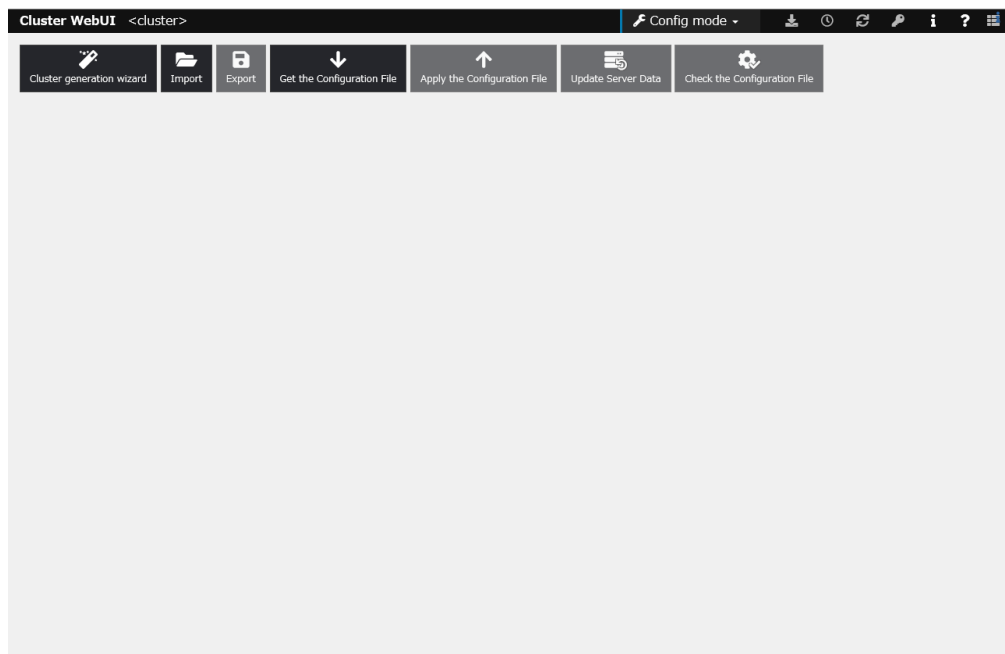
- Mirror disk resource
- Azure probe port resource
- Azure probe port monitor resource
- Azure load balance monitor resource
- PING network partition resolution resource (for NP resolution)

For the settings of other resources and monitor resources, see the Installation and Configuration Guide and the Reference Guide.

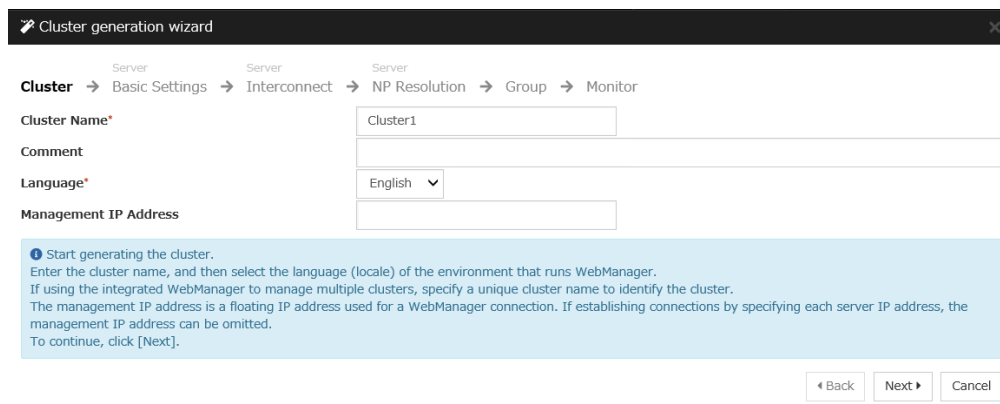
1) Creating a cluster

Start the Cluster generation wizard to create a cluster.

- Creating a cluster
 1. Access Cluster WebUI, and click **Cluster generation wizard**.



2. The **Cluster** window on the **Cluster generation wizard** is displayed.
Enter a desired name in **Cluster Name**.
Select an appropriate language in **Language**. Click **Next**.



Cluster generation wizard

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

Cluster Name*

Comment

Language* English ▾

Management IP Address

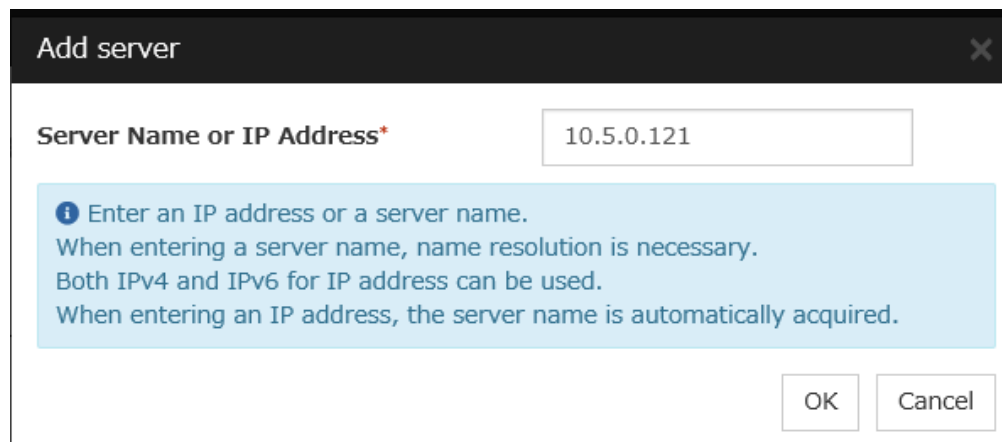
Start generating the cluster.
 Enter the cluster name, and then select the language (locale) of the environment that runs WebManager.
 If using the integrated WebManager to manage multiple clusters, specify a unique cluster name to identify the cluster.
 The management IP address is a floating IP address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

◀ Back Next ▶ Cancel

3. The **Basic Settings** window is displayed.

The instance connected to Cluster WebUI is displayed as a registered master server.

Click **Add** to add the remaining instances (by specifying the private IP address of each instance). Click **Next**.

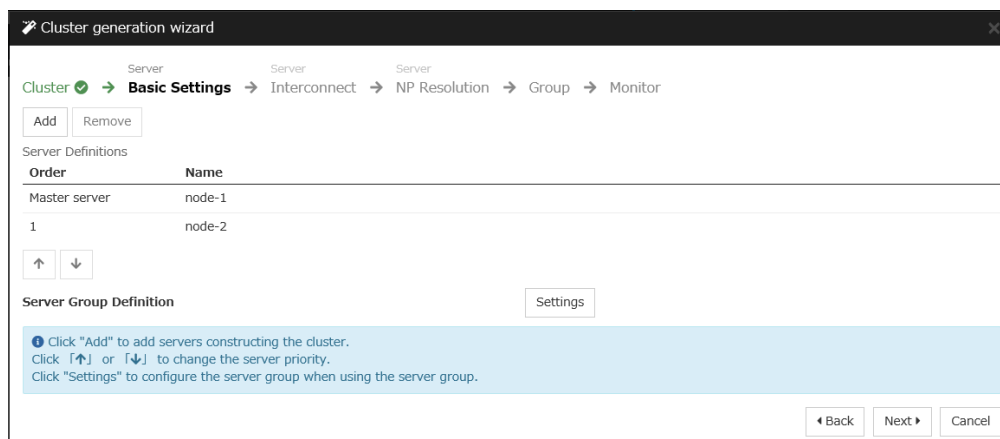


Add server

Server Name or IP Address*

Enter an IP address or a server name.
 When entering a server name, name resolution is necessary.
 Both IPv4 and IPv6 for IP address can be used.
 When entering an IP address, the server name is automatically acquired.

OK Cancel



Cluster generation wizard

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

Add Remove

Server Definitions

Order	Name
Master server	node-1
1	node-2

↑ ↓

Server Group Definition Settings

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

◀ Back Next ▶ Cancel

4. The **Interconnect** window is displayed.

Specify the IP addresses (IP address of each instance) to be used for interconnect. In addition, select mdc1 for **MDC** as a communication path of a mirror disk resource to be created later.

Click **Next**.

Cluster generation wizard

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

Properties Add Remove

Interconnect List

Priority	Type	MDC	node-1	node-2
1	Kernel Mode	mdc1	10.5.0.120	10.5.0.121

↑ ↓

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

Back Next Cancel

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

To execute NP resolution by using a ping, click **Add** to add a line to the NP resolution list. Click a cell of the **Type** column and select **Ping**. Click the cell of the **Ping Target** column and set the IP address of the device to which to send a ping. Be sure to specify the IP address of a server other than cluster servers within the Microsoft Azure virtual network. Click a cell of each server column and select **Use** or **Not use**. Click **Next**.

Cluster generation wizard

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

Properties Add Remove

NP Resolution List

Type	Target	node-1	node-2
Ping	10.5.0.5	Use	Use

Tuning

Configure network partition (NP) resolution function.
 Click "Add" to add NP resolution resource and select the type.
 For "COM" setting, click each server column cell to configure COM port.
 For "DISK" setting, click each server column cell to configure driver letter of the partition for disk heartbeat.
 For "Ping" setting, click Target column cell to configure IP address of Ping destination, and then click each server column cell to configure "Use" or "Do not use".
 For "HTTP" setting, click Target column cell to configure HTTP packet destination, and then click each server column cell to configure "Use" or "Do not use".
 For "Majority" setting, click each server column cell to configure "Use" or "Do not use".
 For "DISK", "Ping", and "HTTP" settings, the detailed settings can be verified and changed by clicking "Properties".
 Click "Tuning" to configure the actions at NP occurrence.

Back Next Cancel

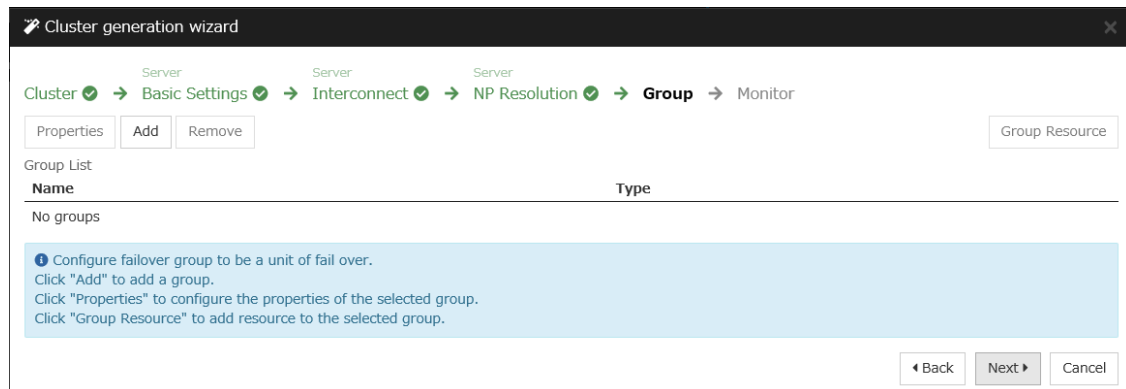
2) **Adding a group resource**

- Defining a group

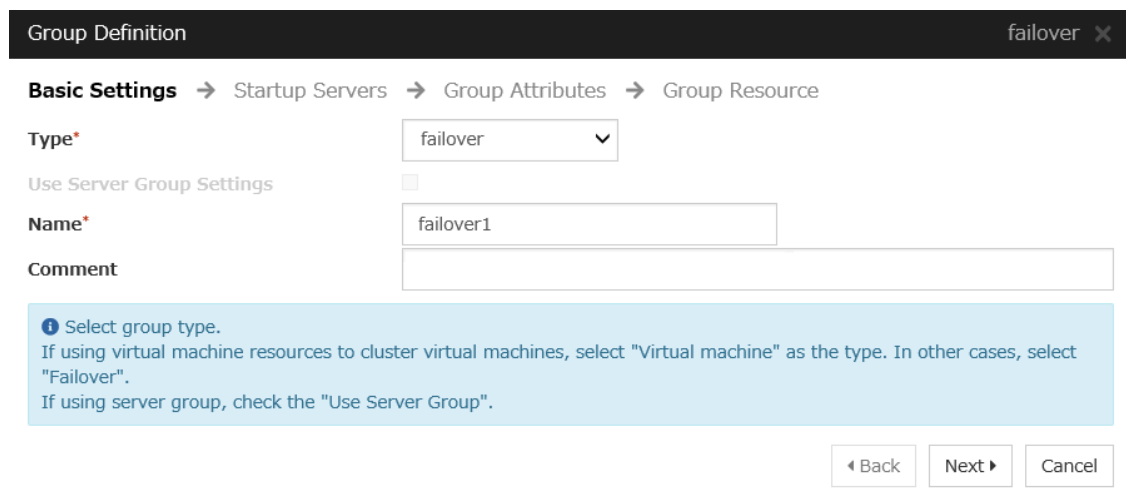
Create a failover group.

1. The **Group List** window is displayed.

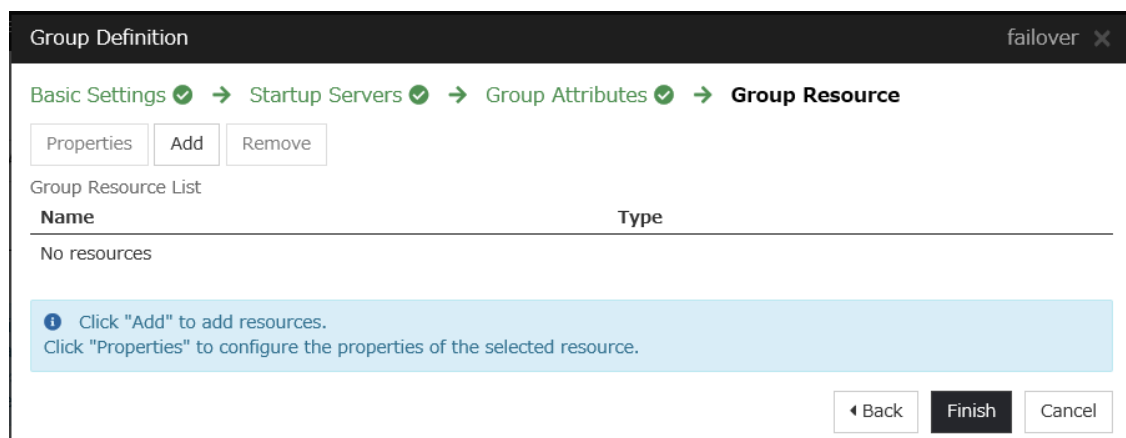
Click **Add**.



2. The **Group Definition** window is displayed.
Specify a failover group name (failover1) for **Name**. Click **Next**.



3. The **Startup Servers** window is displayed.
Click **Next** without specifying anything.
4. The **Group Attributes** window page is displayed.
Click **Next** without specifying anything.
5. The **Group Resource** window is displayed.
On this page, add a group resource following the procedure below.



- Mirror disk resource

Create a mirror disk resource.

For details, see "Understanding mirror disk resources" in "Group resource details" in the Reference Guide.

1. Click **Add** on the **Group Resource List** page.
2. The **Resource Definition of Group | failover1** window is displayed.
Select the group resource type (Mirror disk resource) from the **Type** box and enter the group name (md) in the **Name** box. Click **Next**.

Resource Definition of Group | failover1 md X

Info → Dependency → Recovery Operation → Details

Type* Mirror disk resource ▼

Name* md

Comment

Get License Info

Select the type of group resource and enter its name.

◀ Back Next ▶ Cancel

3. The **Dependency** window is displayed.
Click **Next** without specifying anything.
4. The **Recovery Operation** window is displayed.
Click **Next**.
5. The **Details** window is displayed.
Select a server name in the **Name** column of **Servers that can run the group** and click **Add**.

Resource Definition of Group | failover1 md x

Info → Dependency → Recovery Operation → Details

Mirror Disk No.* 1 ▾
Data Partition Drive Letter*
Cluster Partition Drive Letter*
Cluster Partition Offset Index* 0 ▾
Mirror Disk Connect Select

Servers that can run the group

Name	Data Partition	Cluster Partition
← Add		
→ Remove		

Name
node-1
node-2

Edit

Add Servers that can run the group

Tuning

◀ Back Finish Cancel

6. The **Selection of partition** dialog box is displayed. Click **Connect**, select the data partition and cluster partition created in "5)Configuring virtual machines", and click **OK**.

Selection of partition

Obtain information
Connect

Data Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	10238MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

Cluster Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	10238MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

OK Cancel

7. Perform steps 5 and 6 for node-1 and then node-2 and click **Finish**.

- Azure probe port resource

When EXPRESSCLUSTER is used on Microsoft Azure, EXPRESSCLUSTER provides a mechanism to wait for alive monitoring from a load balancer on a port specific to a node in which operations are running. For details about the Azure probe port resources", see "Understanding Azure probe port resources" in the Reference Guide.

1. Click **Add** on the **Group Resource List** page.
2. The **Resource Definition of Group | failover1** window is displayed. Select the group resource type (Azure probe port resource) from the **Type** box and enter the group name (azurepp1) in the **Name** box. Click **Next**.

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

4. The **Recovery Operation** window is displayed. Click **Next**.
5. For **Probeport**, enter the value specified for **Port** when configuring a load balancer (configuring health probe).

6. Click **Finish**.

3) Adding a monitor resource

- Azure probe port monitor resource

The port monitoring mechanism for alive monitoring is provided for the node in which the Microsoft Azure probe port resource is running.

For details about the Azure probe port monitor resource, see "Understanding Azure probe port monitor resources" in the Reference Guide.

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

- Azure load balance monitor resource

The mechanism to monitor whether the port with the same port number as the probe port is open or not is provided for the node in which the Microsoft Azure probe port resource is not running.

For details about the Azure load balance monitor resource, see "Understanding Azure load balance monitor resources" in the Reference Guide.

Adding one Azure probe port resource creates one Azure load balance monitor resource automatically.

4) Applying the settings and starting the cluster

1. Click **Apply the Configuration File** in the config mode of Cluster WebUI.
A popup message asking "Do you want to perform the operations?" is displayed. Click **OK**.
When the upload ends successfully, a popup message saying "The application finished successfully." is displayed. Click **OK**.
If the upload fails, perform the operations by following the displayed message.
2. Select the **Operation Mode** on the drop down menu of the toolbar in Cluster WebUI to switch to the operation mode. Select **Start Cluster** in the **Status** tab of Cluster WebUI and click.
3. Confirm that a cluster system starts and the status of the cluster is displayed to the Cluster WebUI.
If the cluster system does not start normally, take action according to an error message.

For details, refer to the following:

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

6.4 Verifying the created environment

Verify whether the created environment works properly by generating a (dummy) monitoring error to fail over a failover group.

If the cluster is running normally, the verification procedure is as follows:

1. Start the failover group (failover1) on the active node (node-1). In the Status tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node-1 is **Normal**.
2. Change **Operation Mode** to **Verification Mode** from the Cluster WebUI pull-down menu.
3. In the Status tab on the Cluster WebUI, click the **Enable dummy failure** icon of azureppw1 of Monitors.
4. After the Azure probe port resource (azurepp1) activated three times, the failover group (failover1) becomes abnormal and fails over to node-2. In the Status tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node-2 is **Normal**.

Also, confirm that access to the frontend IP and port of the Azure load balancer is normal after the failover.

Verifying the failover operation in case of a dummy failure is now complete. Verify the operations in case of other failures if necessary.

ERROR MESSAGES

For the error messages related to resources and monitor resources, see the following:

- "Error messages" in the Reference Guide.

NOTES AND RESTRICTIONS

8.1 HA cluster using Azure DNS

8.1.1 Notes on Microsoft Azure

- There is a tendency for the performance difference (performance deterioration rate) to increase in a multi-tenant cloud environment compared to a physical environment or general virtualization environment (non-cloud environment). Therefore, pay careful attention to this point when designing a performance-oriented system.
- Even if a virtual machine is just shut down, its status is **Stopped** and billing continues. Execute **Stop** on the virtual machine setting window of the Microsoft Azure portal to change the virtual machine state to **Stopped (Deallocated)**.
- An availability set can be set only when creating a virtual machine. To move a virtual machine to and from the availability set, it is necessary to create an availability set again.
- 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.

8.1.2 Notes on EXPRESSCLUSTER

Please refer the following for notes for EXPRESSCLUSTER on Azure:

EXPRESSCLUSTER X Getting Started Guide

- "Communication port number" in "Notes and Restrictions"
- "Azure DNS resources" in "Notes and Restrictions"
- "Setting up Azure DNS resources" in "Notes and Restrictions"

EXPRESSCLUSTER X Reference Guide

- "Notes on Azure DNS resources"
- "Notes on Azure DNS monitor resources"

Virtual machines are paused for up to 30 seconds for Azure memory preserving maintenance.

Please refer the following for details about memory preserving maintenance.

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/maintenance-and-updates>

Therefore, it is recommended to set **Heartbeat Timeout** parameter on **Timeout** tab in **Cluster Properties** more than 30 sec.

In addition to **Heartbeat Timeout**, please also note the following.

- Please set **Heartbeat Timeout** parameter less than OS reboot time.

Please refer the following about the above:

EXPRESSCLUSTER X Getting Started Guide

- "Adjusting OS startup time" in "Notes and Restrictions"

EXPRESSCLUSTER X Reference Guide

- "Timeout tab"

8.2 HA cluster using a load balancer

8.2.1 Notes on Microsoft Azure

- There is a tendency for the performance difference (performance deterioration rate) to increase in a multi-tenant cloud environment compared to a physical environment or general virtualization environment (non-cloud environment). Therefore, pay careful attention to this point when designing a performance-oriented system.
- Even if a virtual machine is just shut down, its status is **Stopped** and billing continues. Execute **Stop** on the virtual machine setting window of the Microsoft Azure portal to change the virtual machine state to **Stopped (Deallocated)**.
- An availability set can be set only when creating a virtual machine. To move a virtual machine to and from the availability set, it is necessary to create an availability set again.

8.2.2 Notes on EXPRESSCLUSTER

Please refer the following for notes for EXPRESSCLUSTER on Azure:

EXPRESSCLUSTER X Getting Started Guide

- "Communication port number" in "Notes and Restrictions"
- "Azure probe port resources" in "Notes and Restrictions"
- "Setting up Azure probe port resources" in "Notes and Restrictions"
- "Setting up Azure load balance monitor resources" in "Notes and Restrictions"

EXPRESSCLUSTER X Reference Guide

- "Notes on Azure probe port resources"
- "Notes on Azure probe port monitor resources"
- "Note on Azure load balance monitor resources"

Virtual machines are paused for up to 30 seconds for Azure memory preserving maintenance.
Please refer the following for details about memory preserving maintenance.

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/maintenance-and-updates>

Therefore, it is recommended to set **Heartbeat Timeout** parameter on **Timeout** tab in **Cluster Properties** more than 30 sec.

In addition to **Heartbeat Timeout**, please also note the following.

- Please set **Heartbeat Timeout** parameter less than OS reboot time.

Please refer the following about the above:

EXPRESSCLUSTER X Getting Started Guide

- "Adjusting OS startup time" in "Notes and Restrictions"

EXPRESSCLUSTER X Reference Guide

- "Timeout tab"

LEGAL NOTICE

9.1 Disclaimer

- Information in this document is subject to change without notice.
- NEC Corporation is not liable for technical or editorial errors or omissions in the information in this document. To obtain the benefits of the product, it is the customer's responsibility to install and use the product in accordance with this document.
- The copyright of the contents described in this document belongs to NEC Corporation. No part of this document may be reproduced or transmitted in any form by any means, electronic or mechanical, for any purpose, without the express written permission of NEC Corporation.

9.2 Trademark Information

- EXPRESSCLUSTER® is a registered trademark of NEC Corporation.
- Microsoft, Windows, Microsoft Azure, and Azure DNS are registered trademarks of Microsoft Corporation in the United States and other countries.
- Other product names and slogans written in this manual are trademarks or registered trademarks of their respective companies.

REVISION HISTORY

Edition	Revised Date	Description
1st	Apr 08, 2022	New Guide
2nd	Jul 29, 2022	Corrected typographical errors.
3rd	Feb 17, 2023	Corrected typographical errors.

© Copyright NEC Corporation 2022. All rights reserved.