



EXPRESSCLUSTER X 5.2
HA Cluster Configuration Guide for Microsoft Azure
(Linux)
Release 2

NEC Corporation

Nov 29, 2024

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	27
3.1	HA cluster using Azure DNS	27
3.2	HA cluster using a load balancer	29
4	Cluster Creation Procedure (for an HA Cluster Using Azure DNS)	31
4.1	Creation example	31
4.2	Configuring Microsoft Azure	35
4.3	Configuring the EXPRESSCLUSTER settings	57
4.4	Verifying the created environment	73
5	Cluster Creation Procedure (for an HA Cluster Using a Public Load Balancer)	75
5.1	Creation example	75
5.2	Configuring Microsoft Azure	80
5.3	Configuring the EXPRESSCLUSTER settings	106
5.4	Verifying the created environment	122
6	Cluster Creation Procedure (for an HA Cluster Using an Internal Load Balancer)	123
6.1	Creation example	123
6.2	Configuring Microsoft Azure	127
6.3	Configuring the EXPRESSCLUSTER settings	151
6.4	Verifying the created environment	159
7	Error Messages	161
8	Notes	163
9	Legal Notice	165

9.1	Disclaimer	165
9.2	Trademark Information	166
10	Revision History	167

1.1 Who Should Use This Guide

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

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

1.2 Scope of application

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

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

1.3 How This Guide is Organized

- *2. Overview*: Describes the functional overview.
- *3. Operating Environments*: Describes the tested operating environment of this function.
- *4. Cluster Creation Procedure (for an HA Cluster 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 a 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*: 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 five guides. The title and purpose of each guide is described below:

EXPRESSCLUSTER X Getting Started Guide

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

EXPRESSCLUSTER X Installation and Configuration Guide

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

EXPRESSCLUSTER X Reference Guide

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

EXPRESSCLUSTER X Maintenance Guide

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

EXPRESSCLUSTER X Hardware Feature Guide

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

1.5 Conventions

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

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

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

See also:

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

The following conventions are used in this guide.

Convention	Usage	Example
Bold	Indicates graphical objects, such as text boxes, list boxes, menu selections, buttons, labels, icons, etc.	Click Start. Properties dialog box
Angled bracket within the command line	Indicates that the value specified inside of the angled bracket can be omitted.	<code>clpstat -s[-h <i>host_name</i>]</code>
#	Prompt to indicate that a Linux user has logged on as root user.	<code># clpstat</code>
Monospace	Indicates path names, commands, system output (message, prompt, etc.), directory, file names, functions and parameters.	<code>/Linux</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.

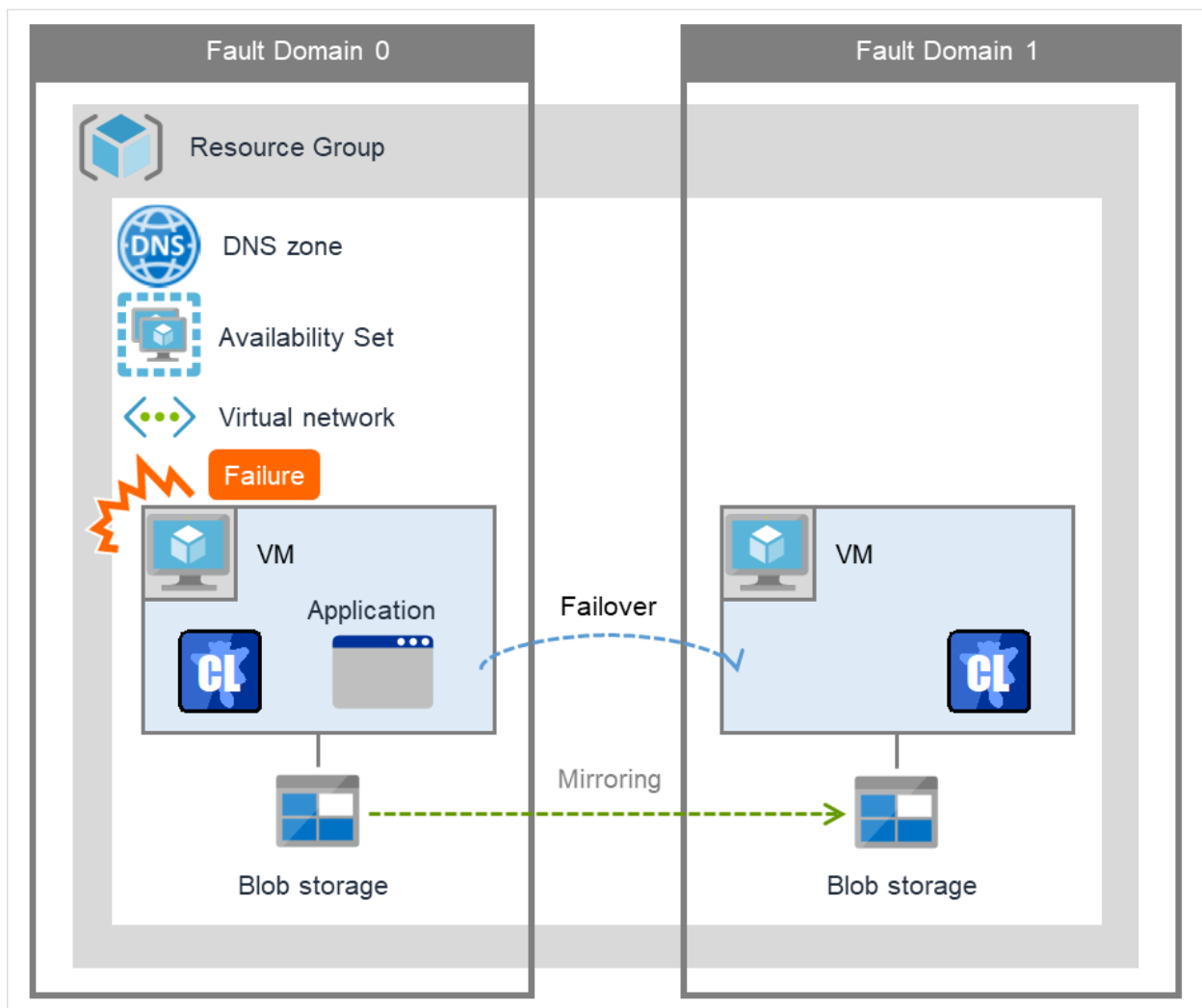


Fig. 2.1: HA Cluster on a Cloud Service (Using Azure DNS)

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 Linux virtual machines:

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/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 (Azure DNS needs to be installed)	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 IP address(private IP address) (Use internal load balancer)	Azure probe port resource
Accessing the cluster by using a virtual IP address(private IP address) and applications to be clustered is Always On configuration (Use internal load balancer and configure Direct Server Return (DSR))	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/>

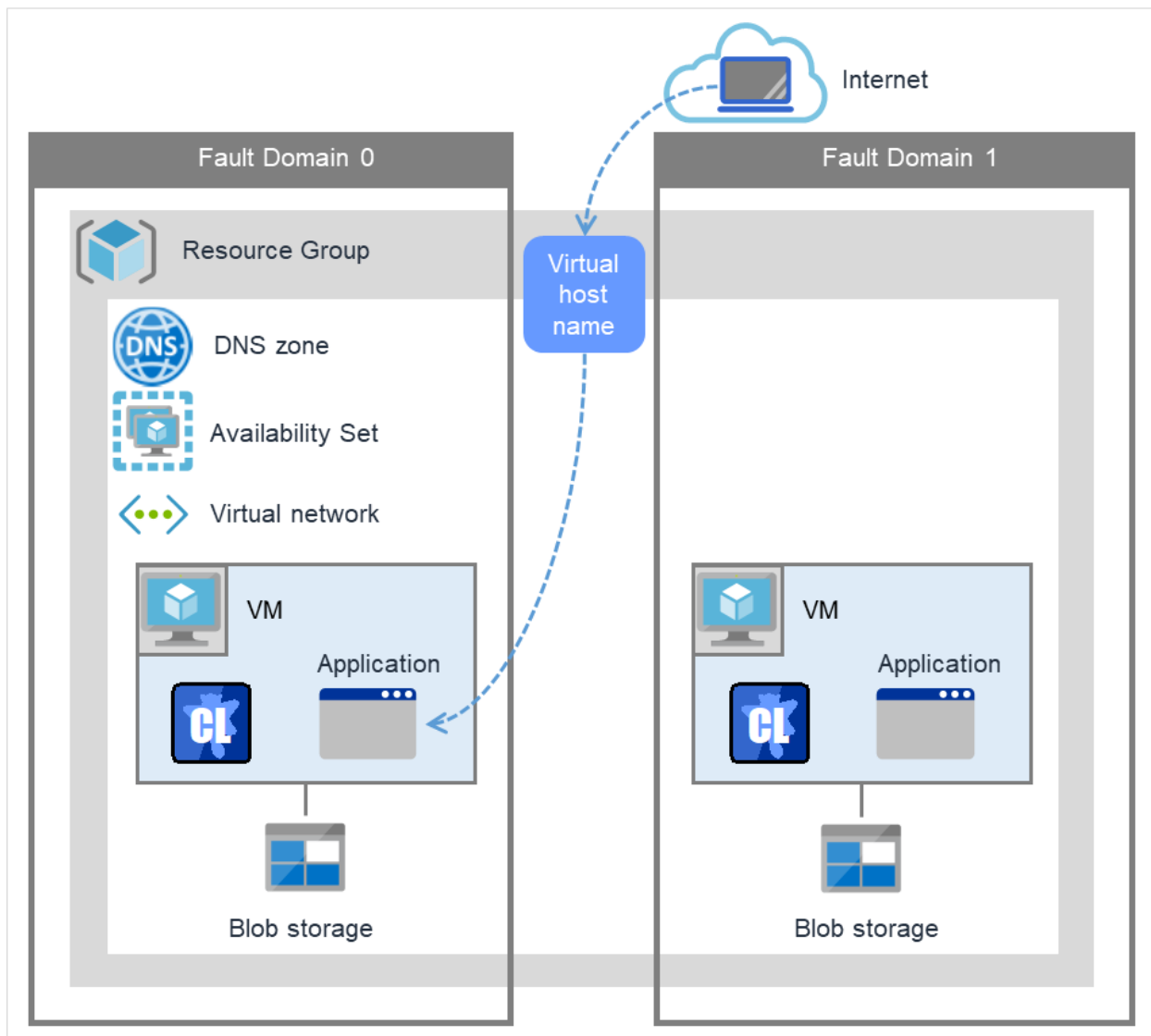


Fig. 2.2: HA Cluster Using Azure DNS

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 a 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 a 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 a 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

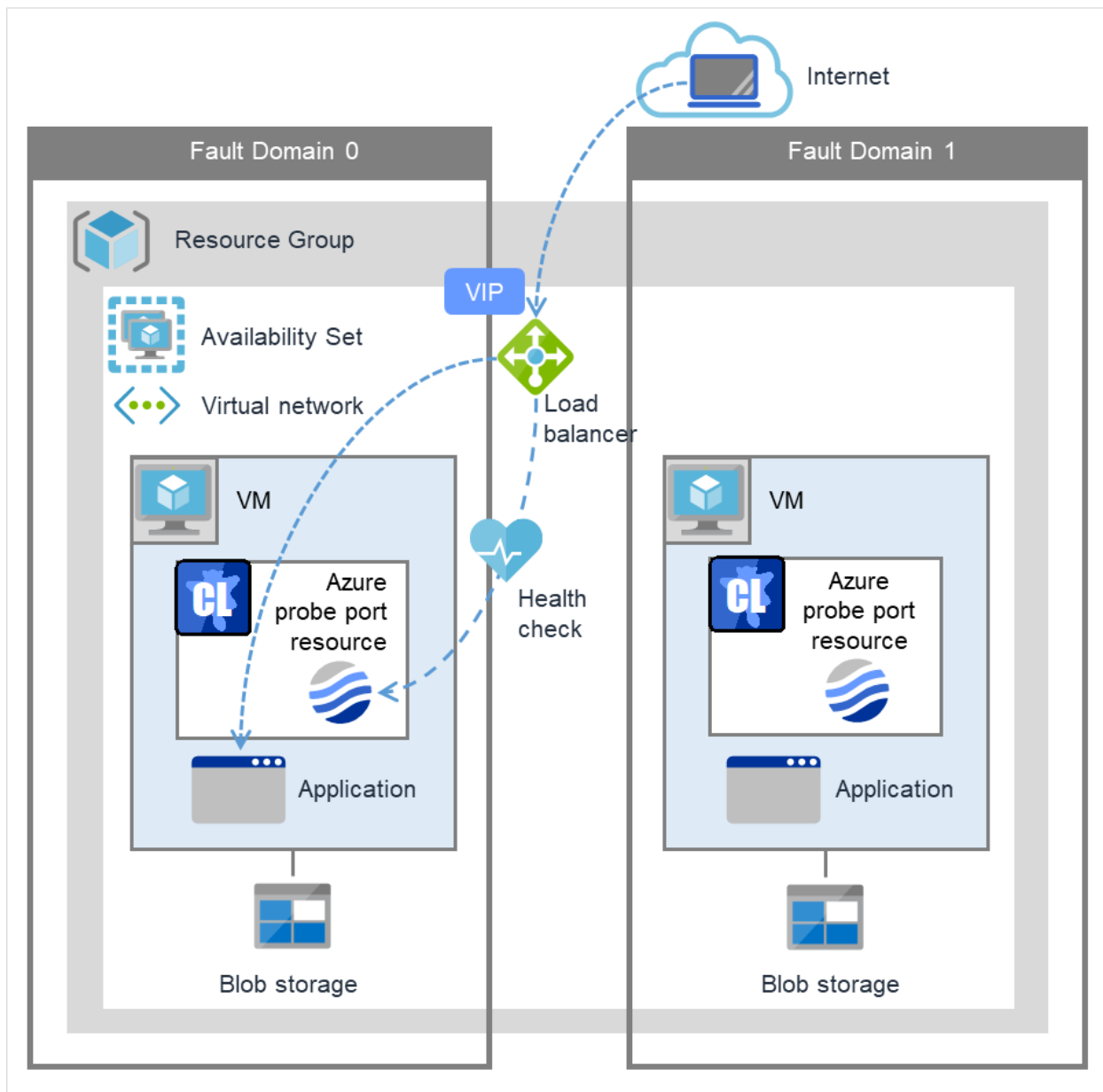


Fig. 2.3: HA Cluster Using a Public Load Balancer

A client application can connect a virtual machine on an availability set in a Microsoft Azure environment to a cluster node by using 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 a 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 a 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.

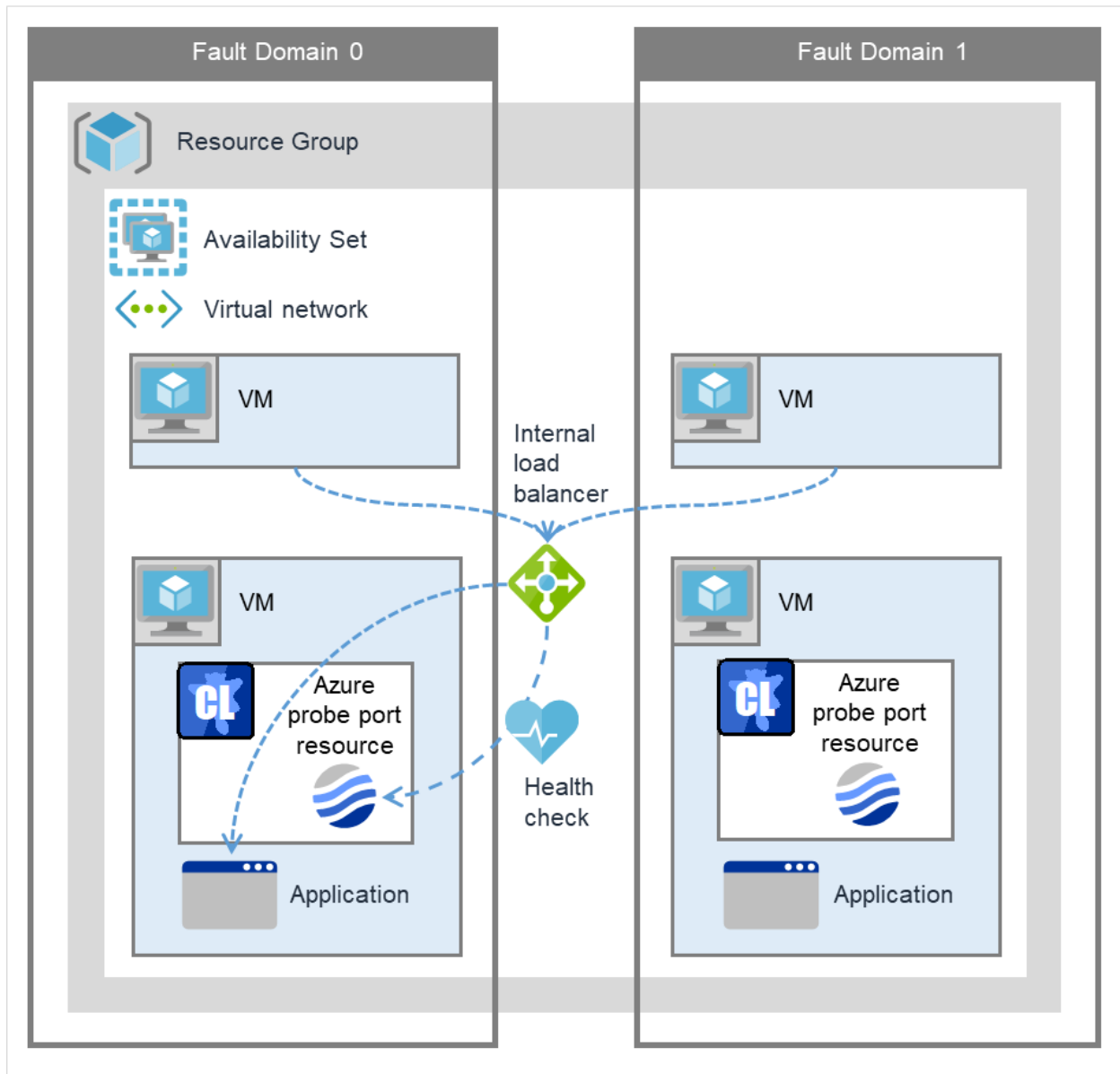


Fig. 2.4: HA Cluster Using the Internal Load Balancer

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 a 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 a 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 a 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 in the following table are used as ping devices for Microsoft Azure.

(*) 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:

- "Network partition resolution resources details" 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
Creating a shared disk type cluster	✓	✓
Creating a mirror disk type cluster	✓	✓
Creating a hybrid disk type cluster	✓	✓
Using the management group	✓	n/a
Using the floating IP resource	✓	n/a
Using the virtual IP resource	✓	n/a
Using the 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 18 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.

Continued on next page

Table 2.7 – continued from previous page

Step No.	Procedure	On-premise	Microsoft Azure
7	Setting up the DNS server	See the manual provided with an OS or DNS server such as Red Hat Enterprise Linux 7 Network Guide.	Not required
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 root file system	See "Settings after configuring hardware" in Determining a system configuration in the Installation and Configuration Guide.	Same as "On-premise"
12	Checking the firewall setting	See "Settings after configuring hardware" in Determining a system configuration in the Installation and Configuration Guide.	Same as "On-premise"
13	Synchronizing the server time	See "Settings after configuring hardware" in Determining a system configuration in the Installation and Configuration Guide.	Same as "On-premise"

Continued on next page

Table 2.7 – continued from previous page

Step No.	Procedure	On-premise	Microsoft Azure
14	Checking the SELinux setting	See "Settings after configuring hardware" in Determining a system configuration in the Installation and Configuration Guide.	Same as "On-premise"
15	Installing the Azure CLI	Not required	See "4.2. <i>Configuring Microsoft Azure</i> " in this guide.
16	Registering the service principal	Not required	See "4.2. <i>Configuring Microsoft Azure</i> " in this guide.
17	Installing EXPRESSCLUSTER	See "Installing EXPRESSCLUSTER" in the Installation and Configuration Guide.	Same as "On-premise"

- After Installing EXPRESSCLUSTER

Step No.	Procedure	On-premise	Microsoft Azure
18	Registering the EXPRESSCLUSTER license	See Registering the license in the Installation and Configuration Guide.	Same as "On-premise"
19	Creating a cluster: Setting the heartbeat method	See "Creating the configuration data of a 2-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.
20	Creating a cluster: Setting the NP resolution processing	The network partition resolution resource is used. See the following: "Creating the configuration data of a 2-node cluster" in Creating the cluster configuration data in the Installation and Configuration Guide. "Network partition resolution resources details" in the Reference Guide.	See "4.3. <i>Configuring the EXPRESSCLUSTER settings</i> " in this guide.

Continued on next page

Table 2.8 – continued from previous page

Step No.	Procedure	On-premise	Microsoft Azure
21	Creating a cluster: Creating a failover group and monitor resource	See "Creating the configuration data of a 2-node cluster" in Creating the cluster configuration data in the Installation and Configuration Guide.	In addition 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. <i>"4.3. 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 16 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: <i>"5.2. Configuring Microsoft Azure"</i> in this guide <i>"6.2. 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: <i>"5.2. Configuring Microsoft Azure"</i> in this guide <i>"6.2. 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
3	Creating a virtual machine	Not required	See either of the following depending on the load balancer to use: <i>"5.2. Configuring Microsoft Azure"</i> in this guide <i>"6.2. Configuring Microsoft Azure"</i> in this guide
4	Setting a private IP address	Not required	See either of the following depending on the load balancer to use: <i>"5.2. Configuring Microsoft Azure"</i> in this guide <i>"6.2. 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: <i>"5.2. Configuring Microsoft Azure"</i> in this guide <i>"6.2. 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: <i>"5.2. Configuring Microsoft Azure"</i> in this guide <i>"6.2. 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
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
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 root file system	See "Settings after configuring hardware" in Determining a system configuration in the Installation and Configuration Guide.	Same as "On-premise"
12	Checking the firewall setting	See "Settings after configuring hardware" in Determining a system configuration in the Installation and Configuration Guide.	Same as "On-premise"
13	Synchronizing the server time	See "Settings after configuring hardware" in Determining a system configuration in the Installation and Configuration Guide.	Same as "On-premise"
14	Checking the SELinux setting	See "Settings after configuring hardware" in Determining a system configuration in the Installation and Configuration Guide.	Same as "On-premise"

Continued on next page

Table 2.9 – continued from previous page

Step No.	Procedure	On-premise	Microsoft Azure
15	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
16	Registering the EXPRESSCLUSTER license	See Registering the license in the Installation and Configuration Guide.	Same as "On-premise"
17	Creating a cluster: Setting the heartbeat method	See "Creating the configuration data of a 2-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.
18	Creating a cluster: Setting the NP resolution processing	The network partition resolution resource is used. See the following: "Creating the configuration data of a 2-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.

Continued on next page

Table 2.10 – continued from previous page

Step No.	Procedure	On-premise	Microsoft Azure
19	Creating a cluster: Creating a failover group and monitor resource	See "Creating the configuration data of a 2-node cluster" in Creating the cluster configuration data in the Installation and Configuration Guide.	<p>See the following in addition to the description of "On-premise."</p> <p>"Understanding Azure probe port resources" in the Reference Guide.</p> <p>"Understanding Azure probe port monitor resources" in the Reference Guide.</p> <p>"Understanding Azure load balance monitor resources" in the Reference Guide.</p> <p>See either of the following depending on the load balancer to use:</p> <p>See "5.3. <i>Configuring the EXPRESSCLUSTER settings</i>" in this guide.</p> <p>See "6.3. <i>Configuring the EXPRESSCLUSTER settings</i>" in this guide.</p>

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, 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, Microsoft Azure portal, and Azure CLI, please replace it as appropriate.

x86_64

OS	CentOS 7.6
EXPRESSCLUSTER	EXPRESSCLUSTER X 4.2 for Linux (Internal version: 4.2.0-1)
Microsoft Azure deployment model	Resource Manager
Region	(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	Azure CLI 2.0
Python	2.7

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

Since Python 2.7 is required when using 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>

Install the Azure classic CLI:

<https://docs.microsoft.com/en-us/cli/azure/install-classic-cli>

Python is bundled with Linux OS.

Since Azure CLI 1.0 (Azure classic CLI) running on Python 2.6 has been unrecommended, install Python by using the package manager of each distribution (e.g. APT, yum, and zipper) if Python 2.7 is not bundled.

Azure DNS must be installed because the 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

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, Microsoft Azure portal, and Azure CLI, please replace it as appropriate.

x86_64

OS	CentOS 7.6
EXPRESSCLUSTER	EXPRESSCLUSTER X 4.2 for Linux (Internal version: 4.2.0-1)
Microsoft Azure deployment model	Resource Manager
Region	(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 node1 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 node1 and node2)

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	

Continued on next page

Table 4.1 – continued from previous page

Setting item	Setting value
- Name	cluster1.zone
- Resource group	TestGroup1
- Record set	test-record1

- Microsoft Azure settings (specific to each of node1 and node2)

Setting item	Setting value	
	node1	node2
Virtual machine setting		
- Disk type	Standard HDD	Standard HDD
- User name	testlogin	testlogin
- Password	PassWord_123	PassWord_123
- Resource group	TestGroup1	TestGroup1
- Region	(Asia Pacific) Japan East	(Asia Pacific) Japan East
Network security group setting		
- Name	node1-nsg	node2-nsg
Availability set setting		
- Name	AvailabilitySet1	AvailabilitySet1
- Update domains	5	5
- Fault domains	2	2
Diagnostics storage account setting		
- Name	Automatically generated	Automatically generated

Continued on next page

Table 4.2 – continued from previous page

Setting item	Setting value	
	node1	node2
– Performance	Standard	Standard
– Replication	Locally-redundant storage (LRS)	Locally-redundant storage (LRS)
IP configuration setting		
– IP address	10.5.0.110	10.5.0.111
Disk setting		
– Name	node1_DataDisk_0	node2_DataDisk_0
– Source type	None (empty disk)	None (empty disk)
– Account type	Standard HDD	Standard HDD
– Size	20	20

- EXPRESSCLUSTER settings (cluster properties)

Setting item	Setting value	
	node1	node2
– Cluster Name	Cluster1	Cluster1
– Server Name	node1	node2
– Timeout Tab: Heartbeat timeout	120	120

- EXPRESSCLUSTER settings (failover group)

Resource name	Setting item	Setting value
Mirror disk resource	Name	md
	Details Tab: Mount Point	/mnt/md
	Details Tab: Data Partition Device Name	/dev/sdc2
	Details Tab: Cluster Partition Device Name	/dev/sdc1
	Details Tab: File System	ext4

Continued on next page

Table 4.4 – continued from previous page

Resource name	Setting item	Setting value
	Mirror Tab: Execute the initial mirror construction	On
	Mirror Tab: Execute initial mkfs	On
Azure DNS resource	Name	azuredns1
	Record Set Name	test-record1
	Zone Name	cluster1.zone
	IP Address	(node1) 10.5.0.110 (node2) 10.5.0.111
	Resource Group Name	TestGroup1
	User URI	xxxxxxxx-xxxx-xxxx-xxxx- xxxxxxxxxxxx
	Tenant ID	xxxxxxxx-xxxx-xxxx-xxxx- xxxxxxxxxxxx
	File Path of Service Principal	/home/testlogin/tmpbyJlck.pem
	Azure CLI File Path	/usr/bin/az

- EXPRESSCLUSTER settings (monitor resource)

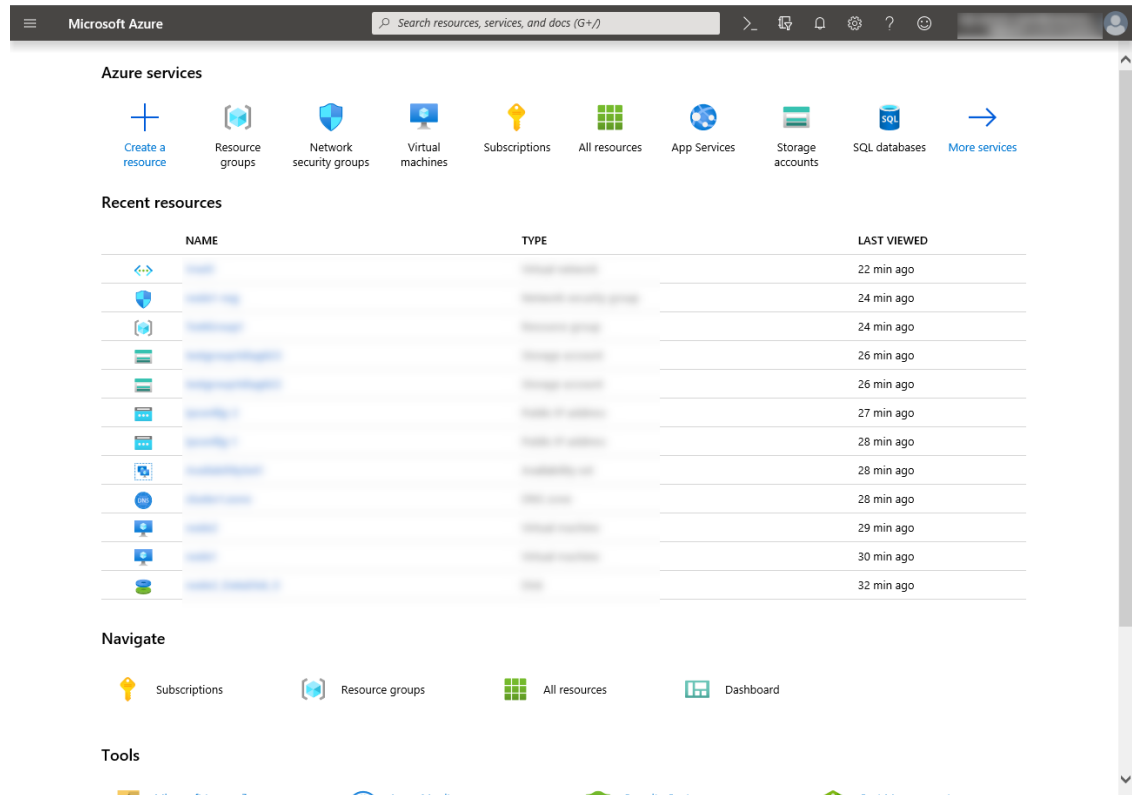
Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	Name	mdw1
Azure DNS monitor resource	Name	azuredns1
Custom monitor resource	Name	genw1
	Script created with this product	On
	Monitor Type	Synchronous
	Normal Return Value	0
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
IP monitor resource	Name	ipw1
	Server to monitor	node1
	IP Address	10.5.0.111
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
IP monitor resource	Name	ipw2
	Server to monitor	node2
	IP Address	10.5.0.110
	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.

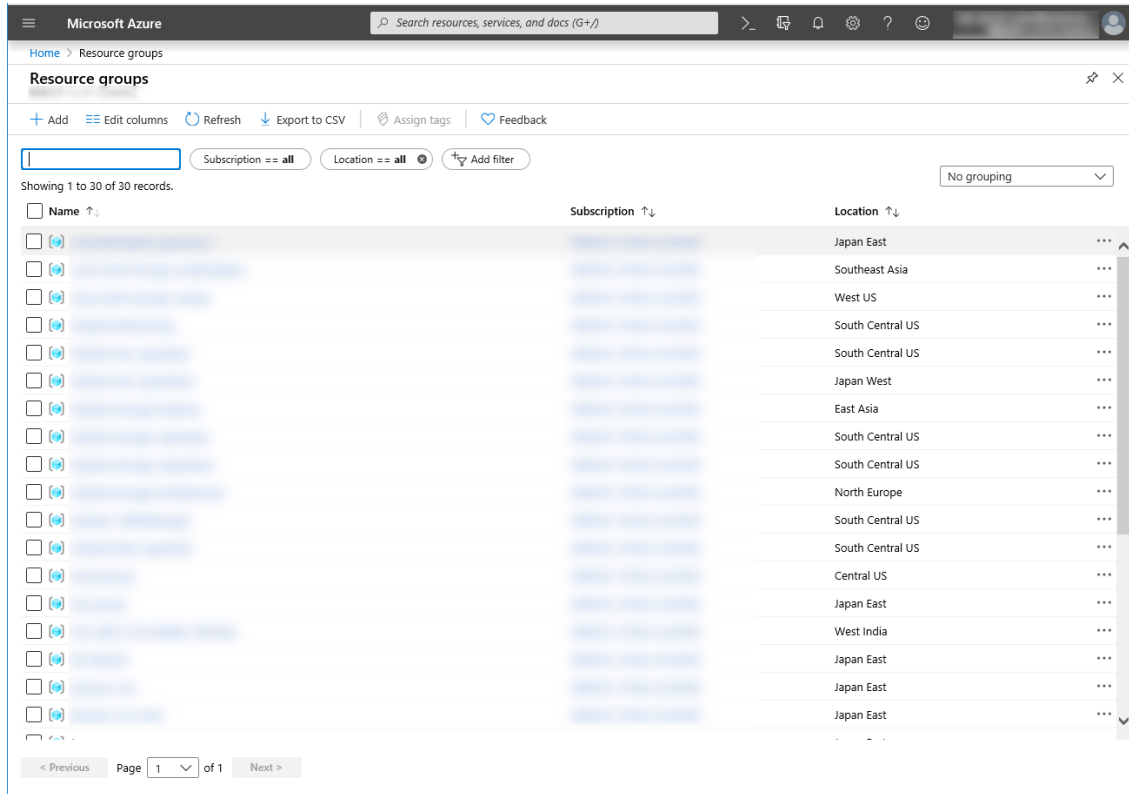
1. Select the **Resource groups** icon on the upper part of the window. If there are existing resource groups, they are displayed in a list.



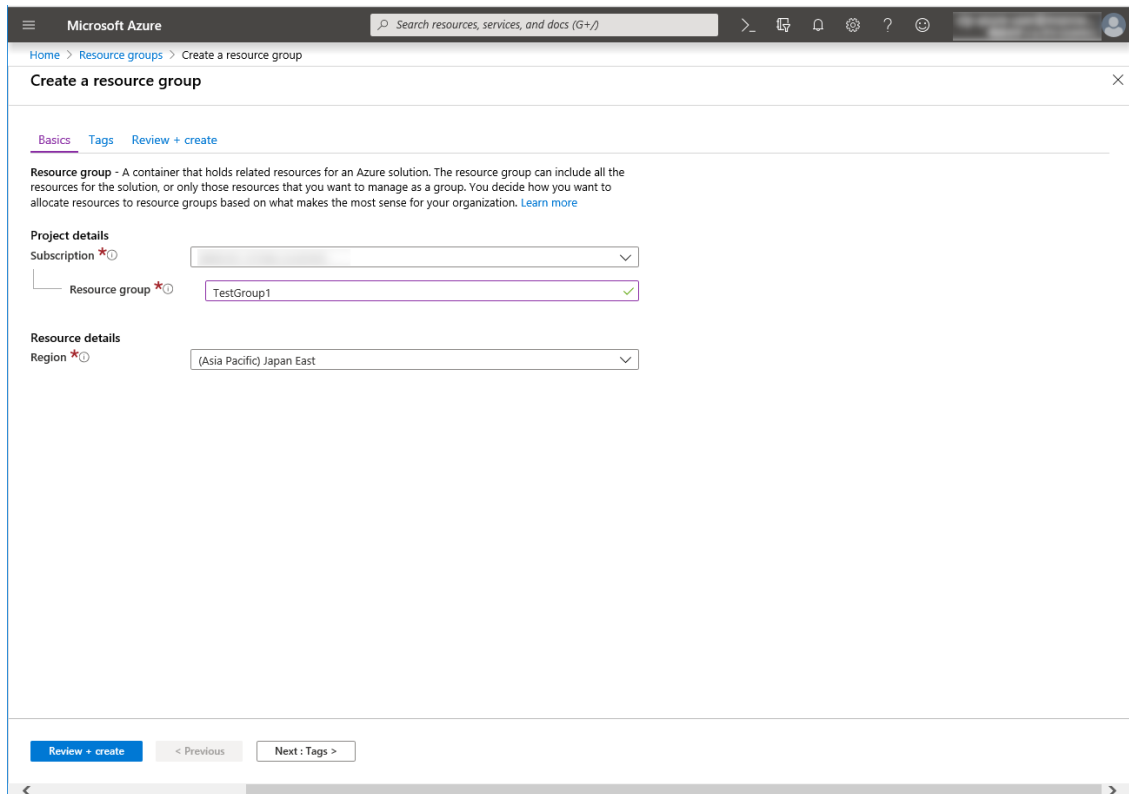
2. Select **+Add** on the upper part of the window.

EXPRESSCLUSTER X 5.2

HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



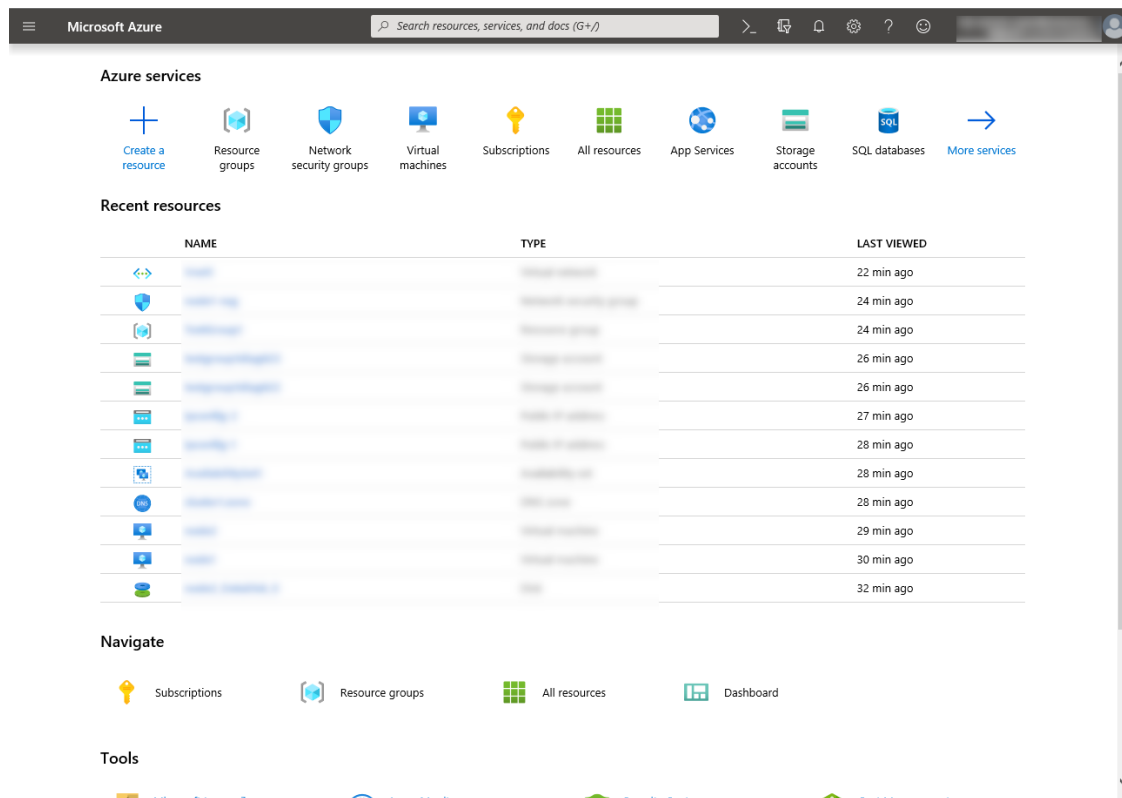
3. Specify **Subscription**, **Resource group**, and **Region**, and click **Review+Create**.



2) **Creating a virtual network**

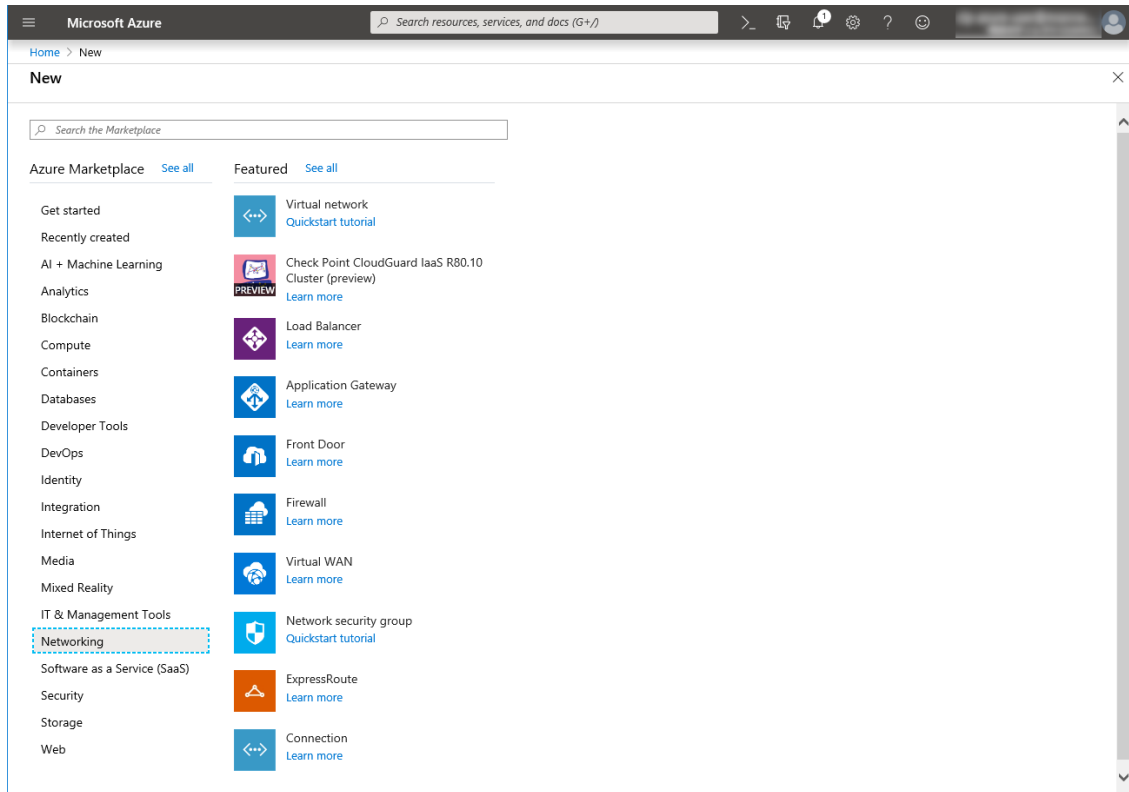
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create a virtual network following the steps below.

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

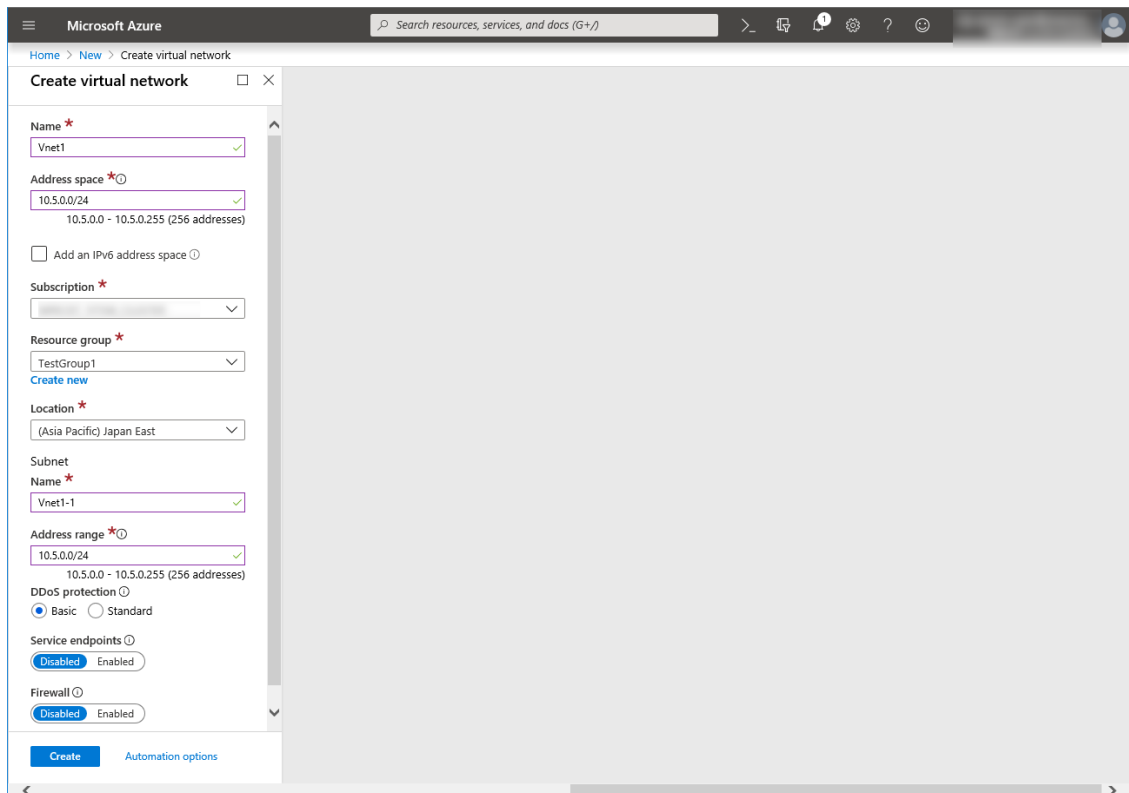


2. Select **Networking** and then **Virtual network**.

EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



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

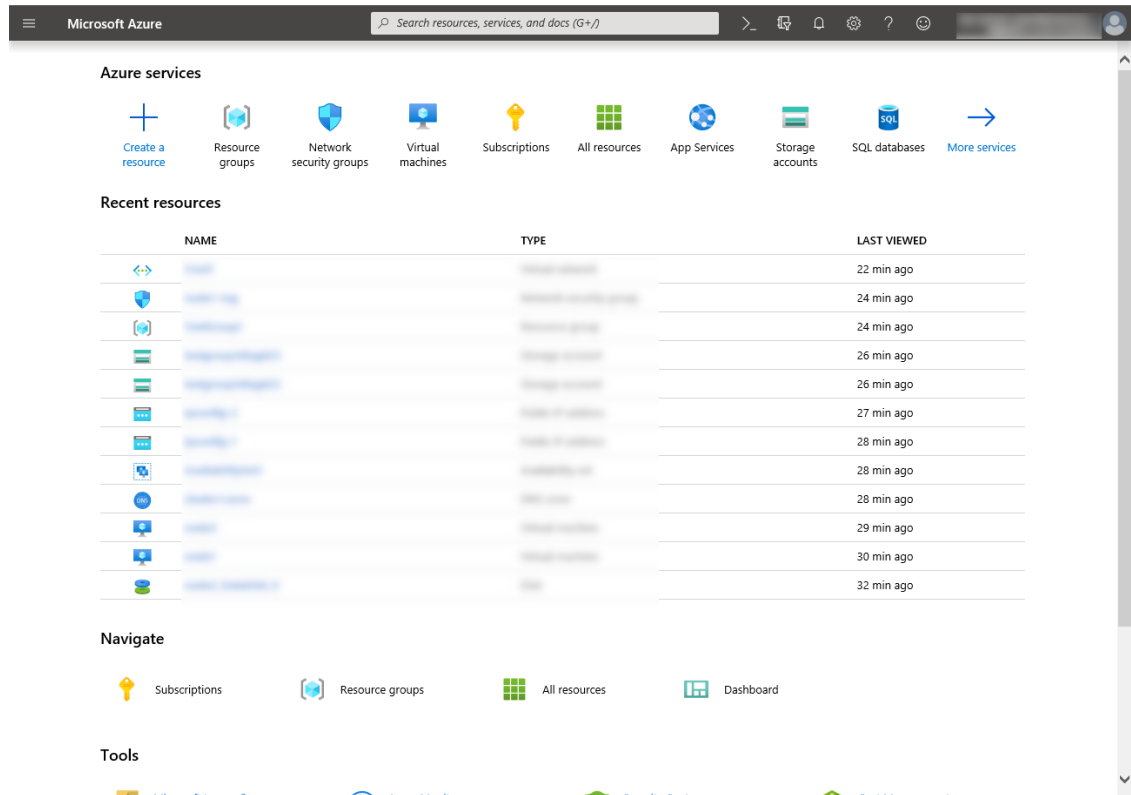


3) Creating a virtual machine

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

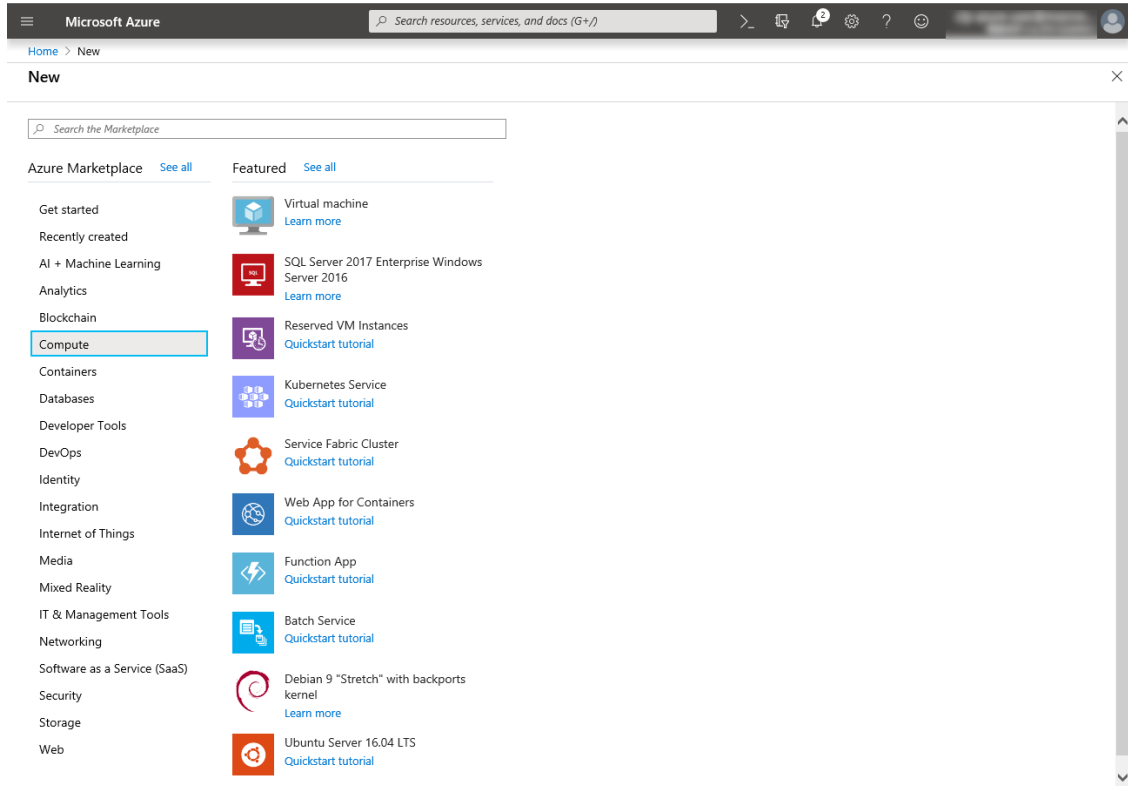
Create as many virtual machines as required to create a cluster. Create node1 and then node2.

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

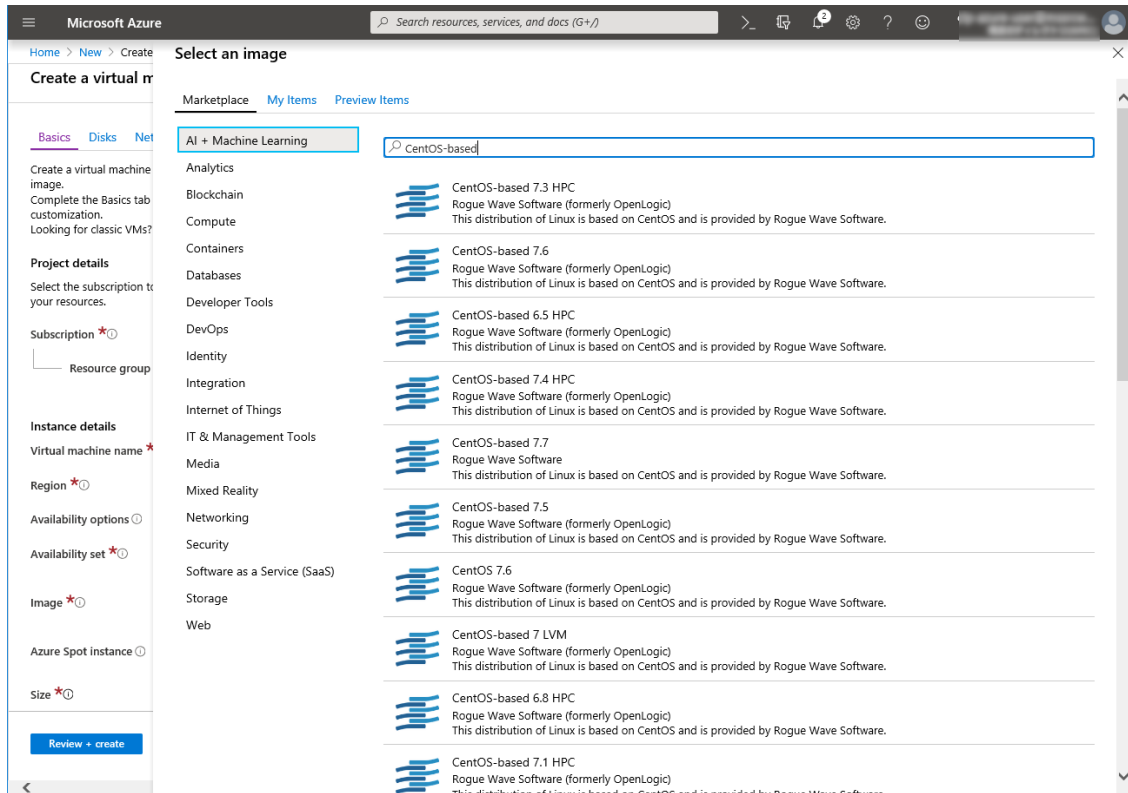


2. Select **Compute** and then **See all**.

EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



3. Select CentOS-based 7.6.

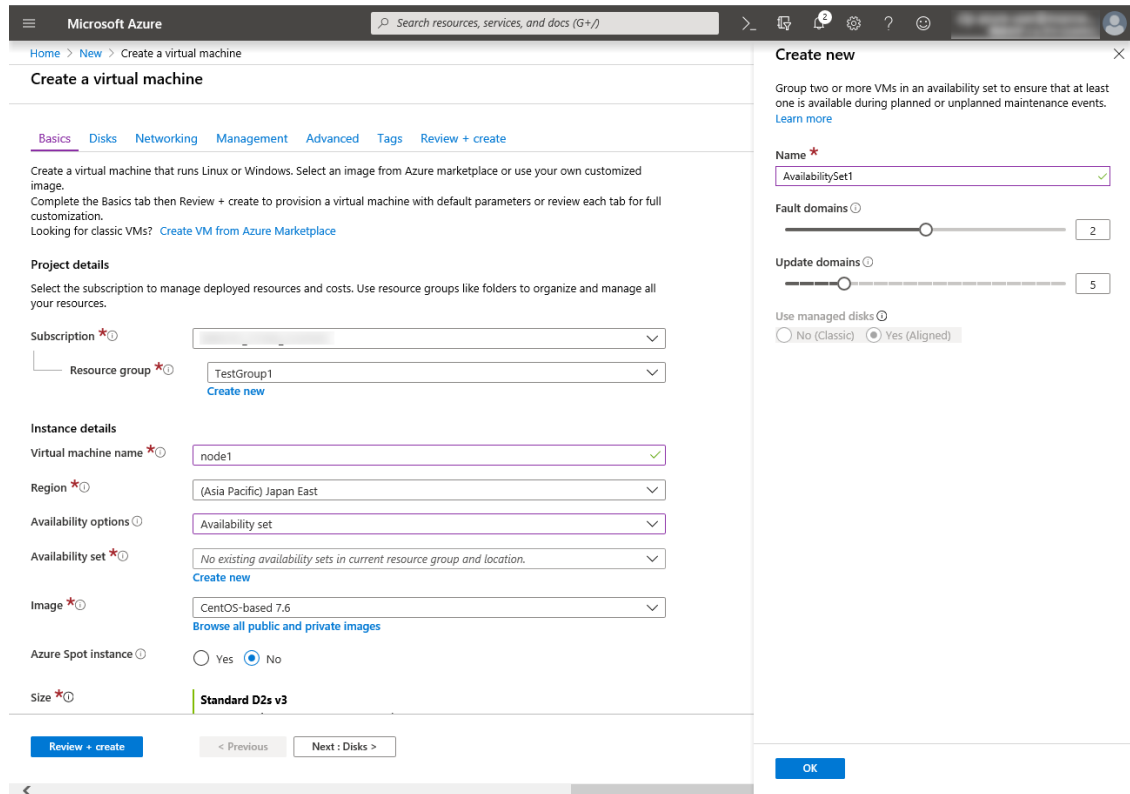


4. Click Create.

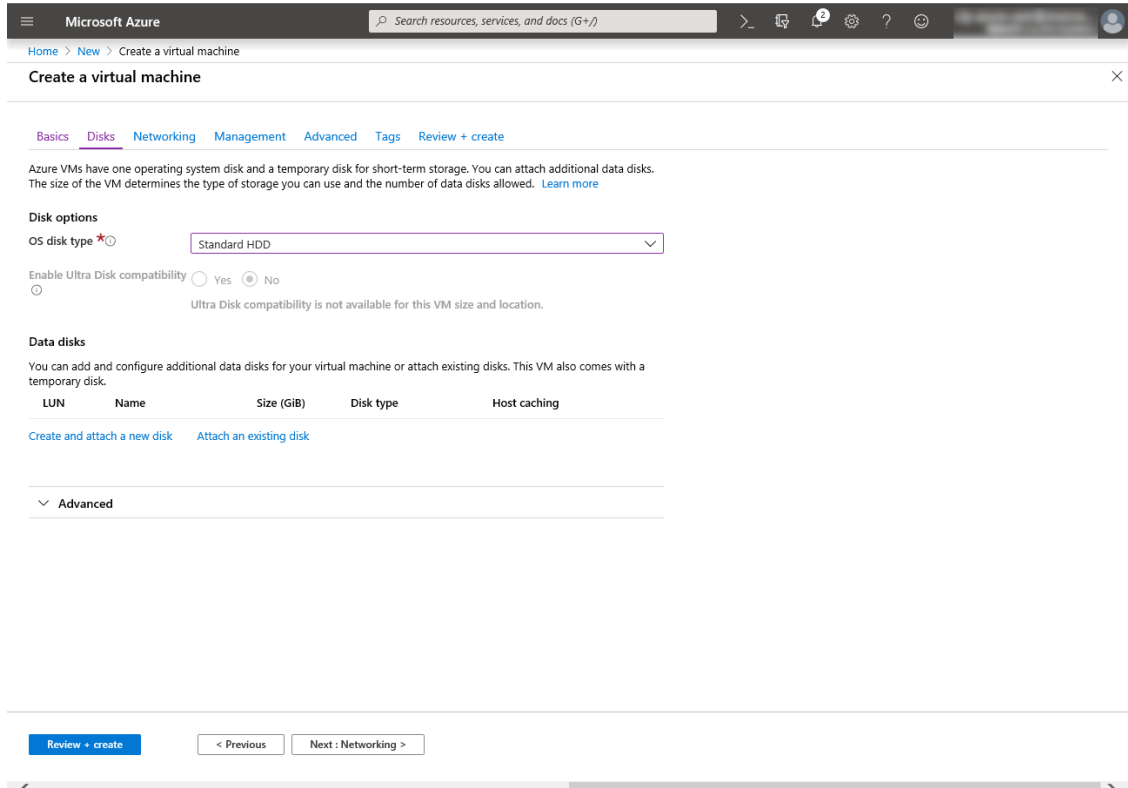
- When the **Basics** tab appears, specify the settings of **Subscription**, **Resource group**, **Virtual machine name**, **Region**, **Image**, **Size**, **Username**, **Password**, and **Confirm password**.
Select **Availability set** from **Availability options**, and click **Create new** under the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

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal, specifically the 'Basics' tab. The page title is 'Create a virtual machine' and the breadcrumb is 'Home > New > Create a virtual machine'. The 'Basics' tab is selected, with other tabs like 'Disks', 'Networking', 'Management', 'Advanced', 'Tags', and 'Review + create' visible. The instructions state: 'Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Looking for classic VMs? Create VM from Azure Marketplace'. The 'Project details' section asks to 'Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.' The 'Subscription' dropdown is empty, and the 'Resource group' dropdown is set to 'TestGroup1' with a 'Create new' link below it. The 'Instance details' section includes: 'Virtual machine name' set to 'node1'; 'Region' set to '(Asia Pacific) Japan East'; 'Availability options' set to 'Availability set'; 'Availability set' set to 'No existing availability sets in current resource group and location.' with a 'Create new' link; 'Image' set to 'CentOS-based 7.6' with a 'Browse all public and private images' link; 'Azure Spot instance' with 'No' selected; and 'Size' set to 'Standard D2s v3'. At the bottom, there are buttons for 'Review + create', '< Previous', and 'Next : Disks >'. The page is scrollable, as indicated by the scrollbar on the right.

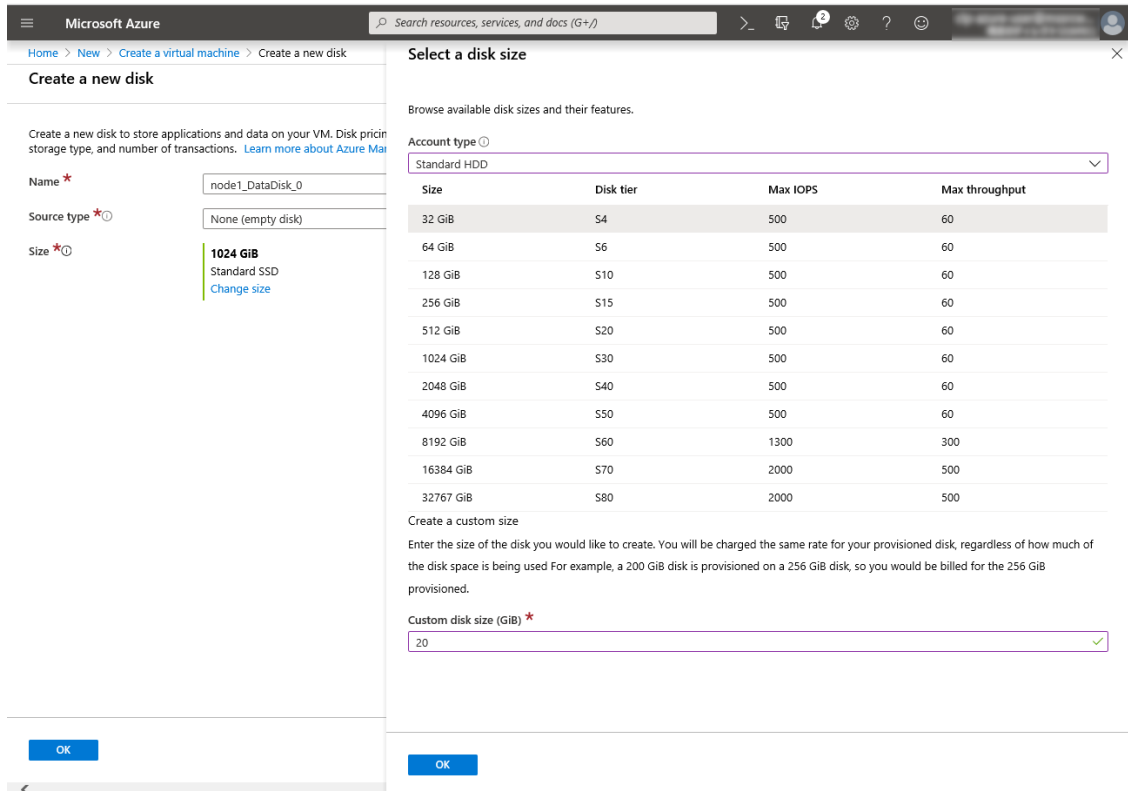
EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



6. Click **Change size** to display **Select a VM size**.
From the list, choose a size (**Standard - A1** in this guide) suitable for your virtual machine and click **Select**.
Regarding the **Virtual machine name**, node1 is for node1, and node2 is for node2.
Click **Next: Disks >**
7. 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**.



8. **Create a new disk** appears. Specify the settings of **Name**, **Source type**, and **Size**. Then click **OK**. Click **Next: Networking >**

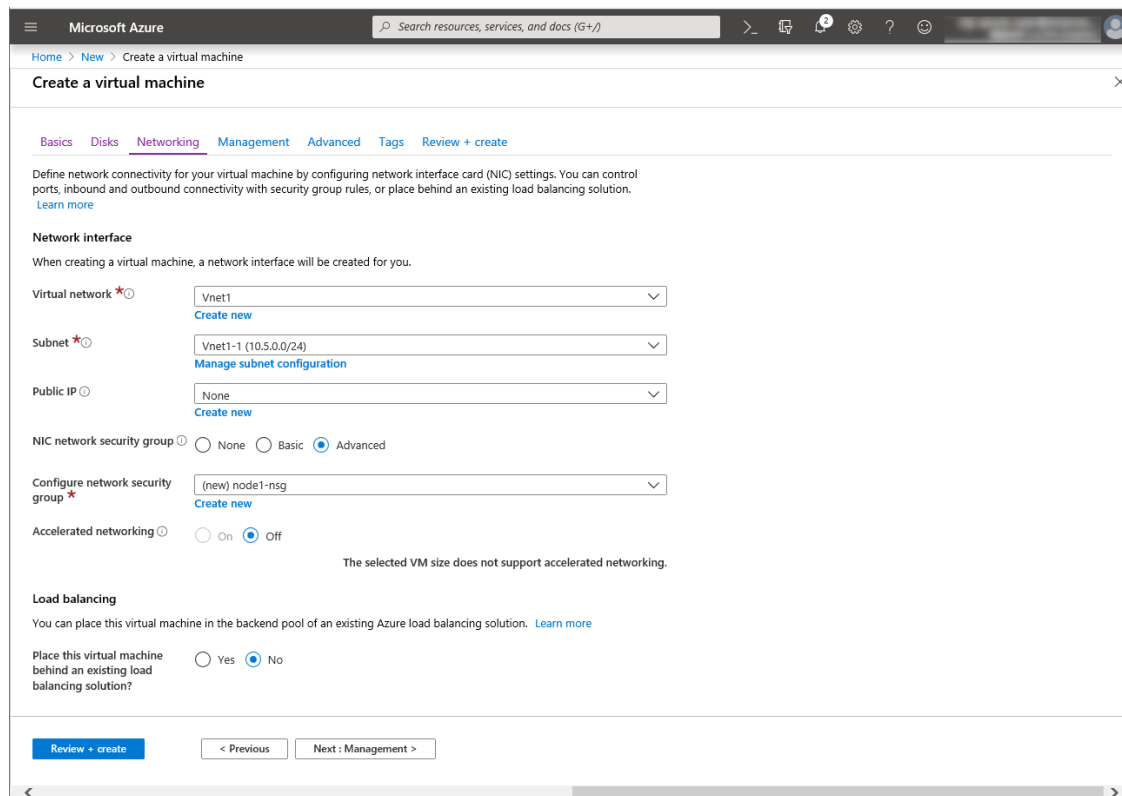


9. The **Networking** tab appears.

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

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

Click **Next: Management >**.

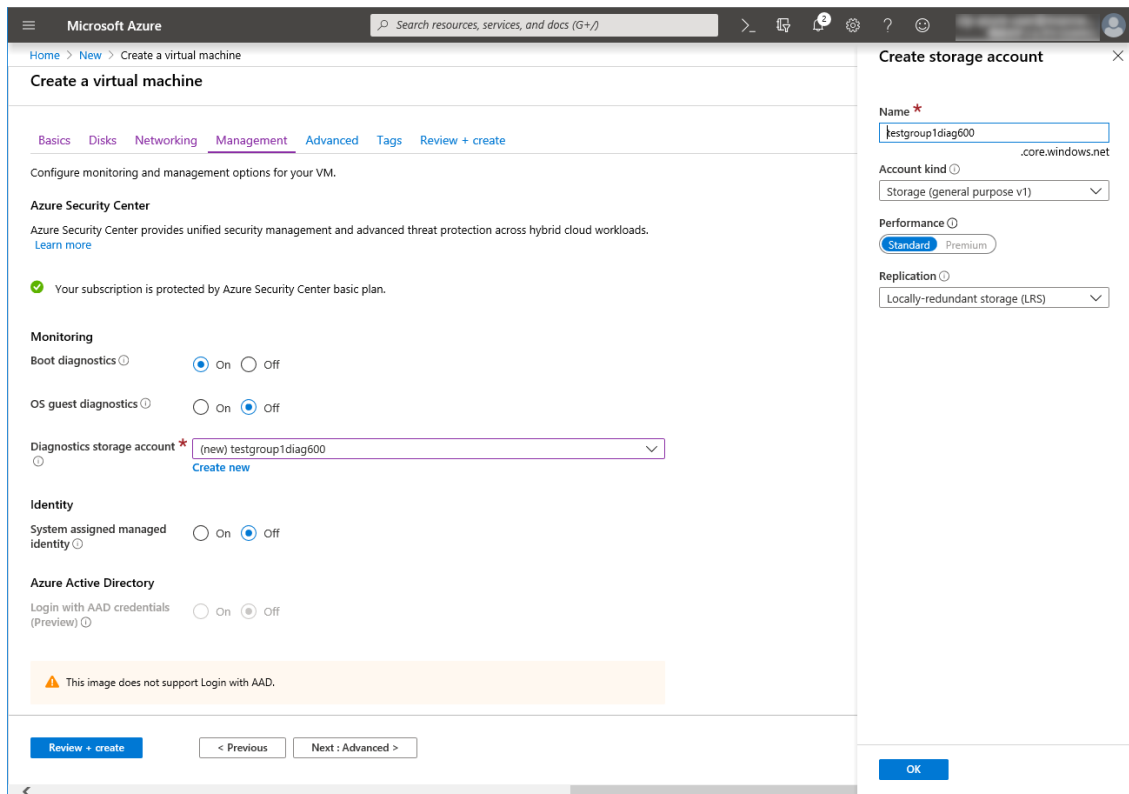
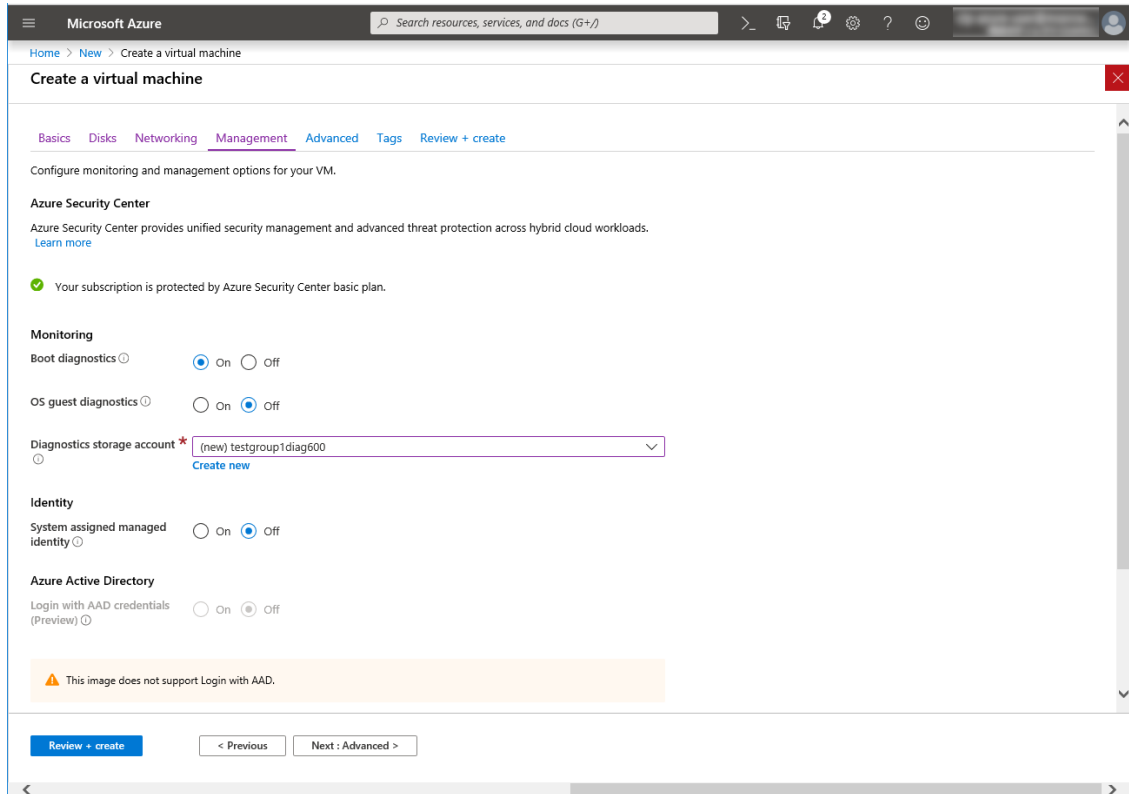


10. The **Management** tab appears.

Click **Create new** under the **Diagnostics storage account** field to display **Create storage account**. Specify the settings of **Name**, **Account kind**, and **Replication**. Then click **OK**.

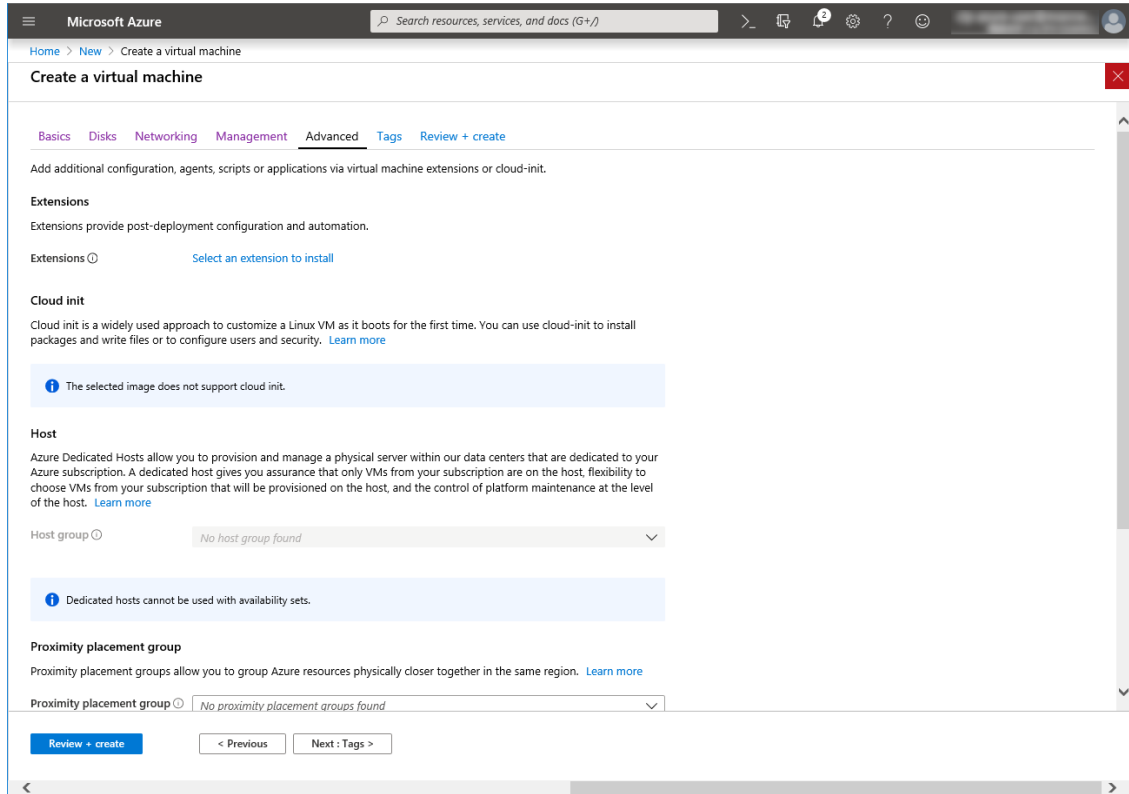
In the **Diagnostics storage account** field, the default value is automatically generated and entered.

Click **Next: Details >**.

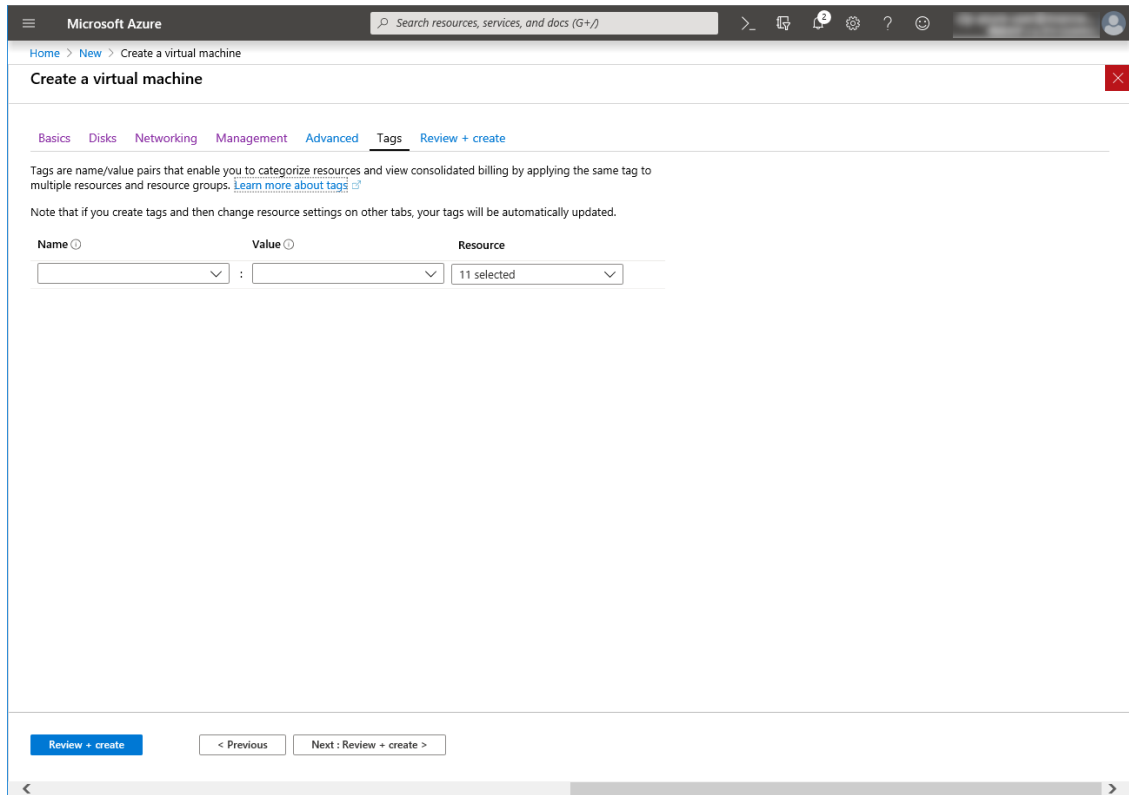


11. Click **Next: Tags >**.

EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2

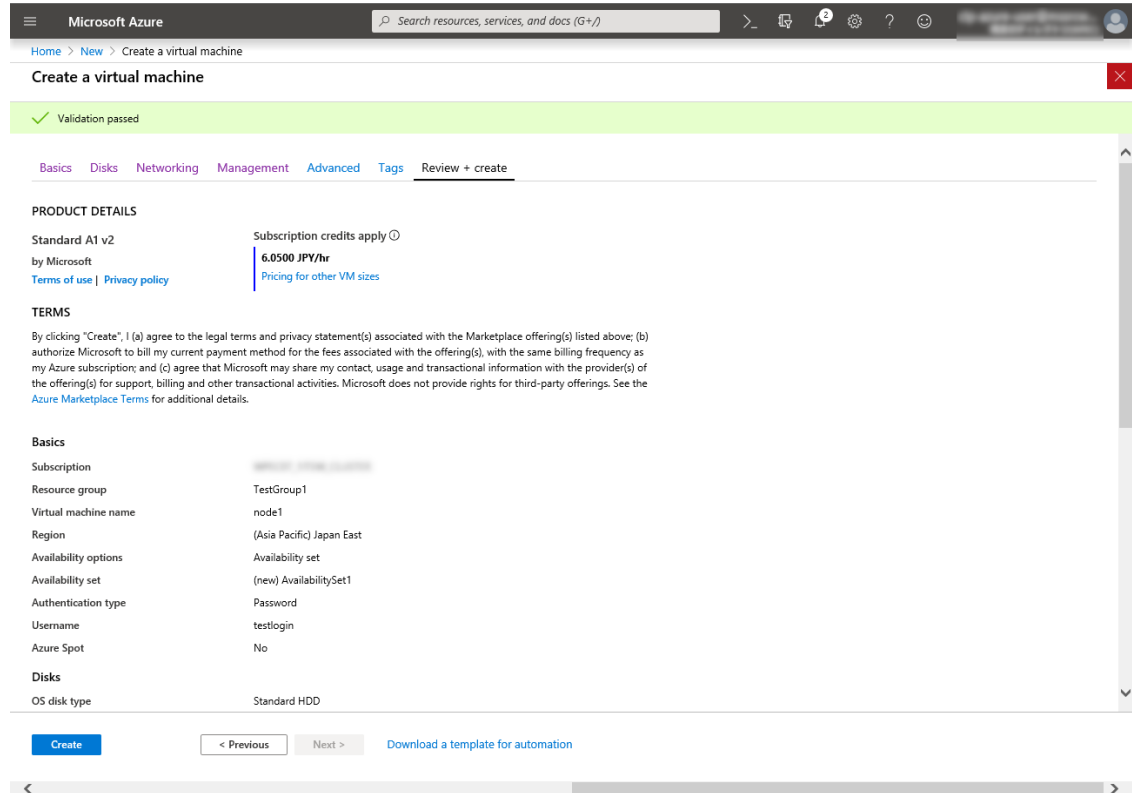


12. Click **Next: Review + create >**.



13. The **Review + create** tab appears. Check the contents. If there is no problem, click **Create**. The deploy-

ment starts and takes several minutes.

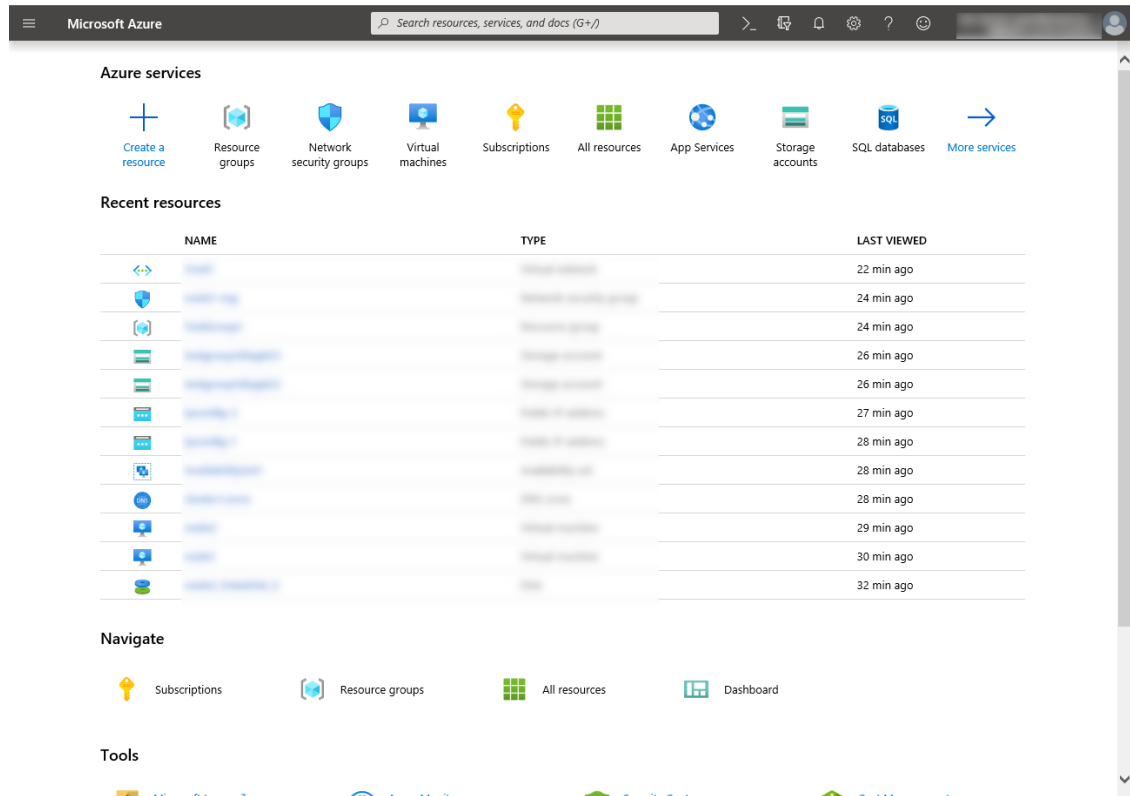


4) Setting a private IP address

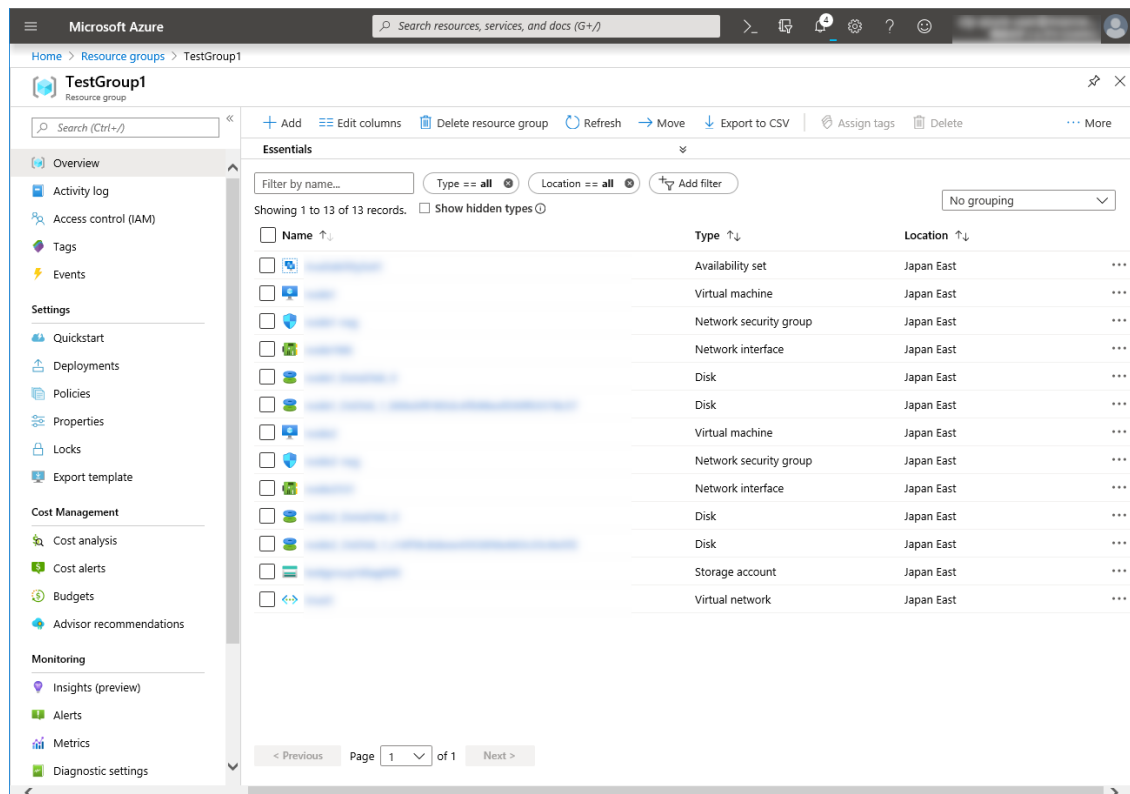
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and change the private IP address setting following the steps below. Since an IP address is initially set to be assigned dynamically, change the setting so that an IP address is assigned statically. Change the settings of node1 and then node2.

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

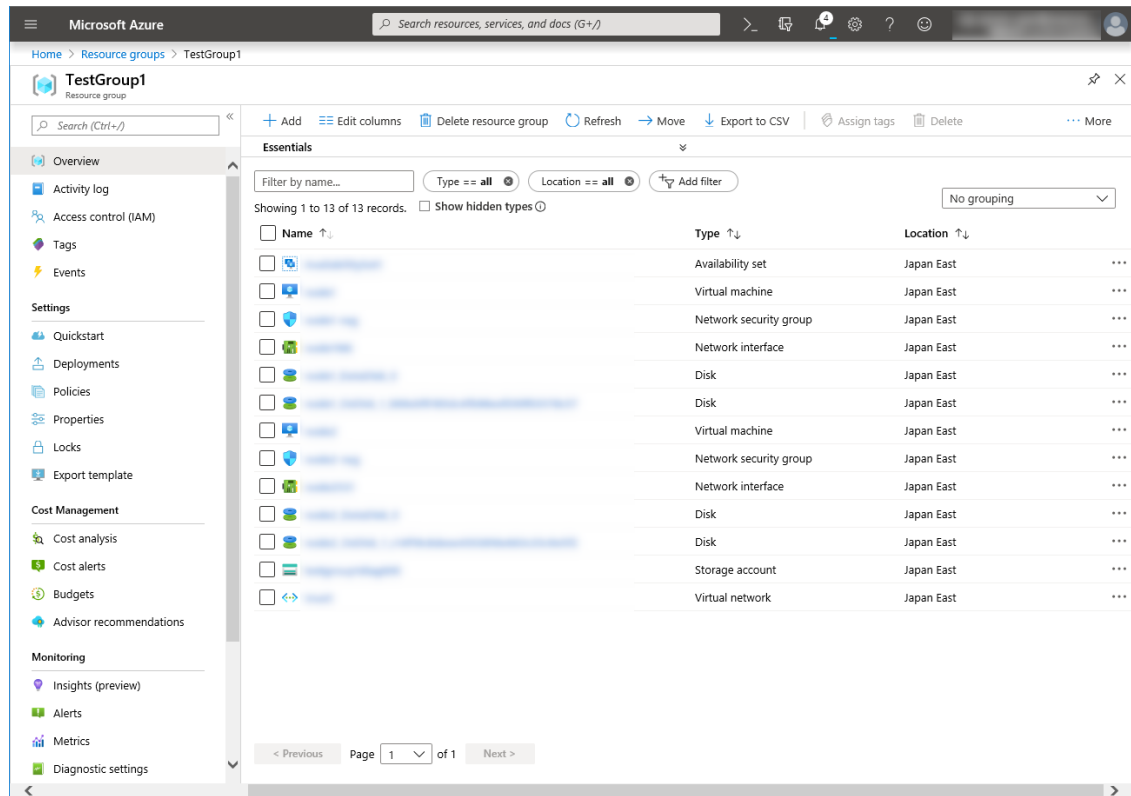
EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



2. Select TestGroup1 from the resource group list.
3. The summary of TestGroup1 is displayed. Select virtual machine node1 or node2 from the item list.

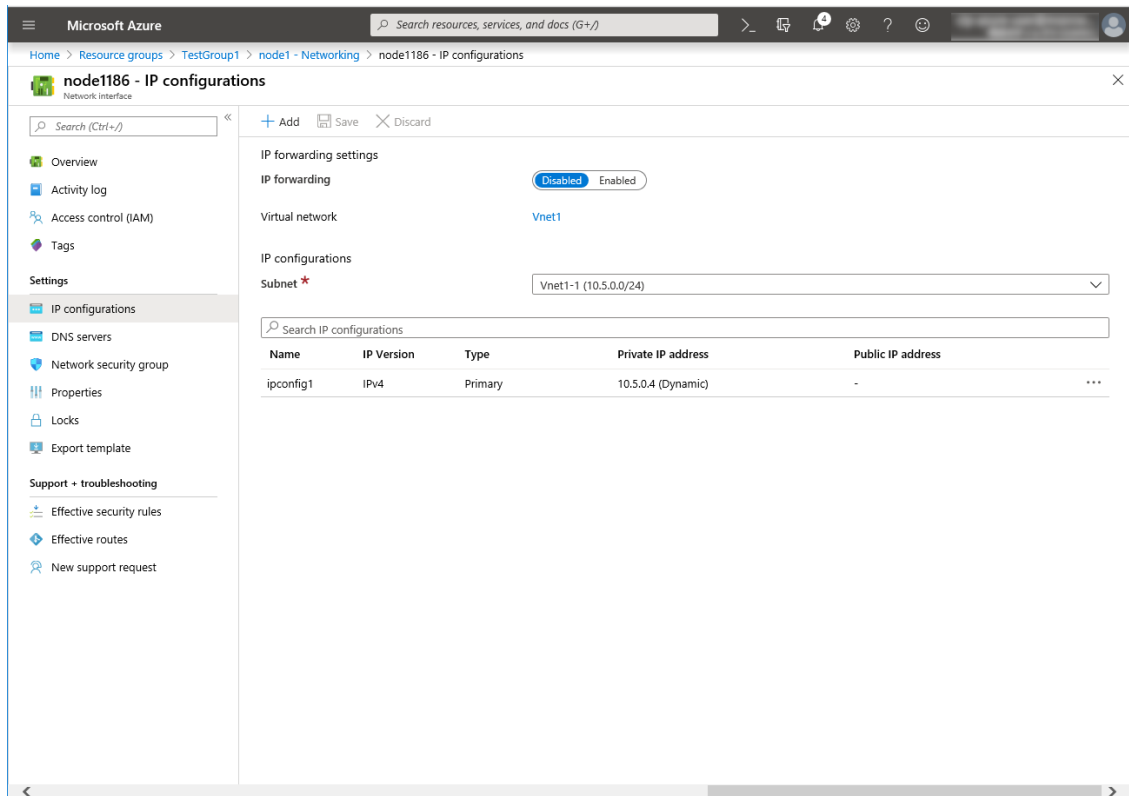


4. Select Networking.

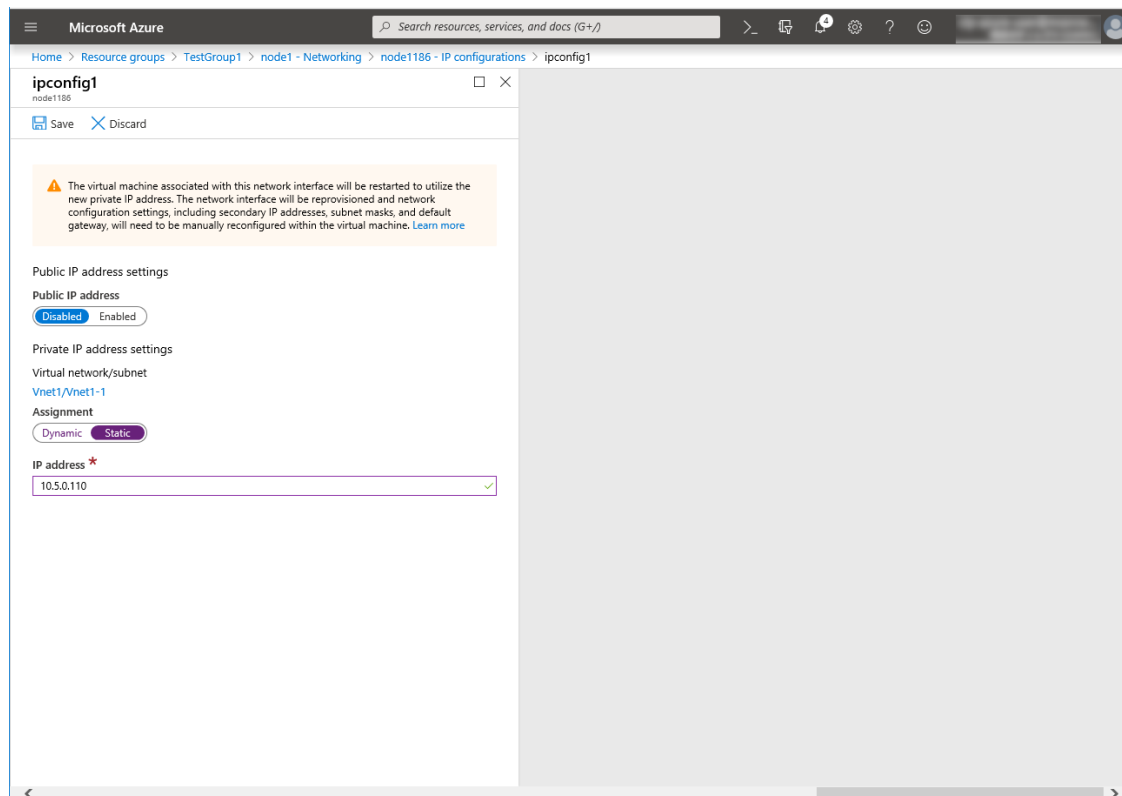


5. Select a network interface displayed in the list. The network interface name is generated automatically.
6. Select **IP configurations**.

EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



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 node1 is 10.5.0.110. The IP address of node2 is 10.5.0.111.



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

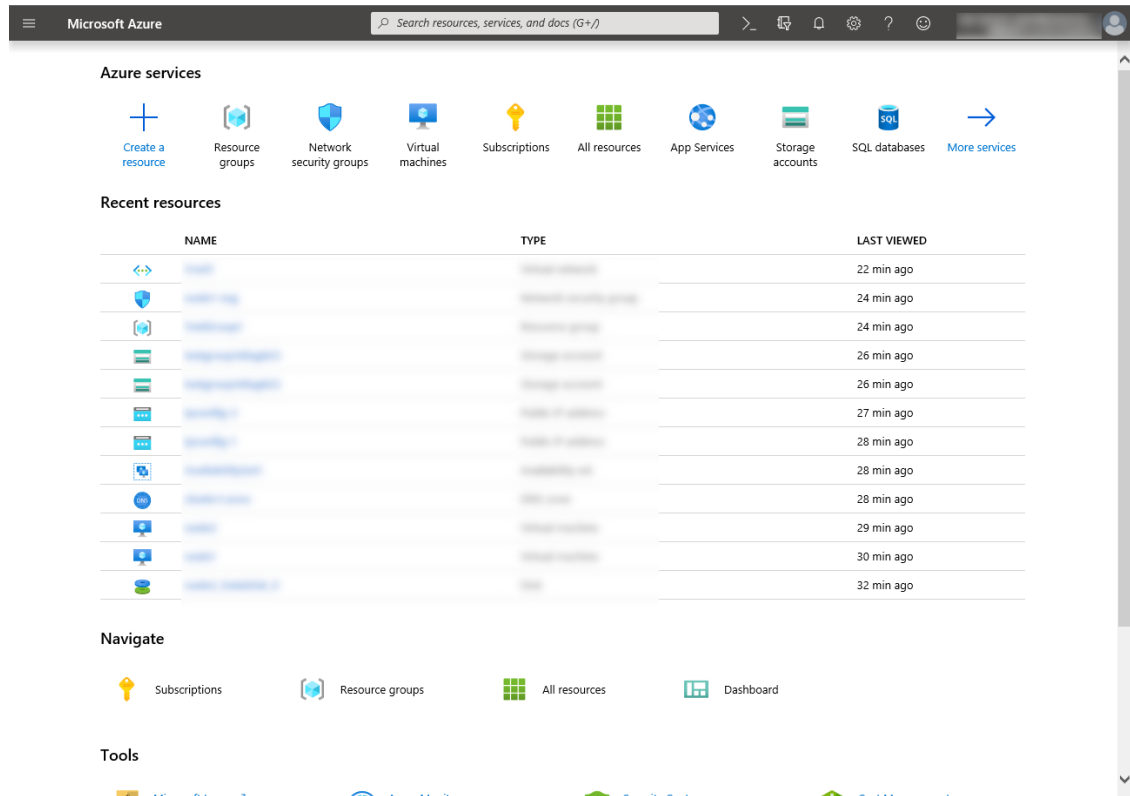
5) Creating a DNS zone

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

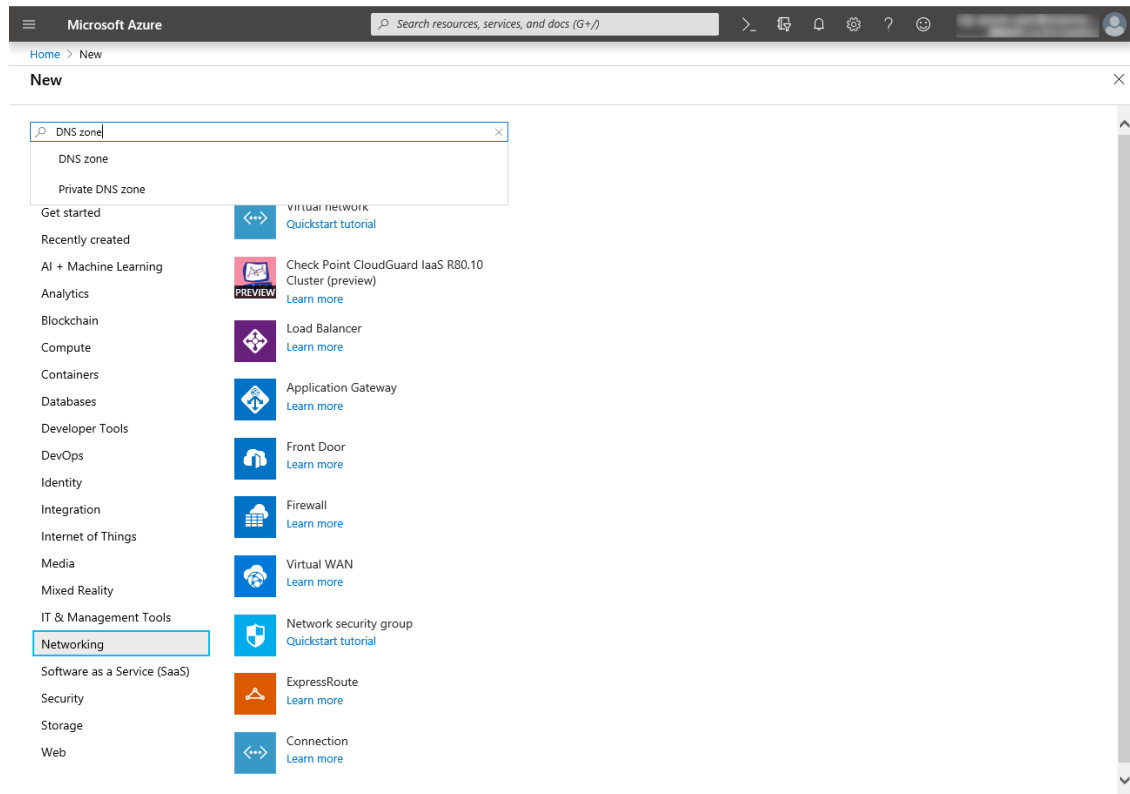
1. Select the **Create a resource** icon on the upper part of the window.

EXPRESSCLUSTER X 5.2

HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



2. Select **Networking** and then **See all**. Search for **DNS zone**.



3. **Create DNS zone** is displayed. Specify **Subscription**, **Resource group**, and **Name**, and click **Re-**

view+create. Then click **Create**.

The screenshot shows the 'Create DNS zone' wizard in the Microsoft Azure portal. The 'Basics' tab is selected, and the form contains the following fields:

- Subscription ***: A dropdown menu.
- Resource group ***: A dropdown menu with 'TestGroup1' selected and a 'Create new' link below it.
- Instance details** section:
 - Name ***: A text input field containing 'cluster1.zone'.
 - Resource group location**: A dropdown menu with '(Asia Pacific) Japan East' selected.

At the bottom of the form, there is a 'Review + create' button, a '< Previous' button, a 'Next : Tags >' button, and a 'Download a template for automation' link.

6) Configuring virtual machines

Log in to the created node1 and node2 and specify the settings following the procedure below.

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

Secure an area in the added disk by using the fdisk command and then create a file system.

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. Check the partition list. In the following example, the last line shows the added disk.

```
$ cat /proc/partitions
major minor #blocks name

 2         0          4 fd0
 8         0    31457280 sda
 8         1     512000 sda1
 8         2    30944256 sda2
 8        16    73400320 sdb
 8        17    73398272 sdb1
 8        32    20971520 sdc
```

2. Create a cluster partition and data partition in the added disk by using the fdisk command. Allocate 1 GB (1*1024*1024*1024 bytes) or more to a cluster partition. (If the size is specified as just 1 GB, the actual size will be larger than 1 GB depending on the disk geometry difference. This is not a problem.) Also, do not create a file system in a cluster partition.
3. If you select **Execute initial mkfs** when creating the cluster configuration data by using Cluster WebUI,

EXPRESSCLUSTER creates a file system automatically. Note that existing data in the partition will be lost.

- 7) **Adjusting the OS startup time, checking the network setting, checking the root file system, checking the firewall setting, synchronizing the server time, and checking the SELinux setting.**

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 an npm package is described.

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

Install the Azure CLI:

<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli>

Log in to the created node1 and node2 and install the Azure CLI following the procedure below.

Be sure to use the following installation procedure. If the Azure CLI is installed in other ways, Azure DNS resource will not work properly.

```
$ sudo yum check-update; sudo yum install -y gcc libffi-devel python3-devel  
↪openssl-devel  
$ curl -L https://aka.ms/InstallAzureCli | bash -  
$ exec -l $SHELL
```

9) **Creating a service principal**

Create a service principal using the Azure CLI.

Azure DNS resource 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>

Create an Azure service principal with Azure CLI:

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

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 it is necessary to set them in the Azure DNS resource settings of Cluster WebUI. In the following example, a service principal is created in /home/testlogin/tmpbyJ1cK.pem. The valid period of certificates is set to 10 years.

```
$ az ad sp create-for-rbac --display-name azure-test --create-cert_
↪--years 10 --role Contributor --scopes <Scopes the service_
↪principal's role assignment applies>
{
  "appId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "displayName": "azure-test",
  "fileWithCertAndPrivateKey": "/home/testlogin/tmpbyJ1cK.pem",
  "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 <appId_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": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
      "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, will fail 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)

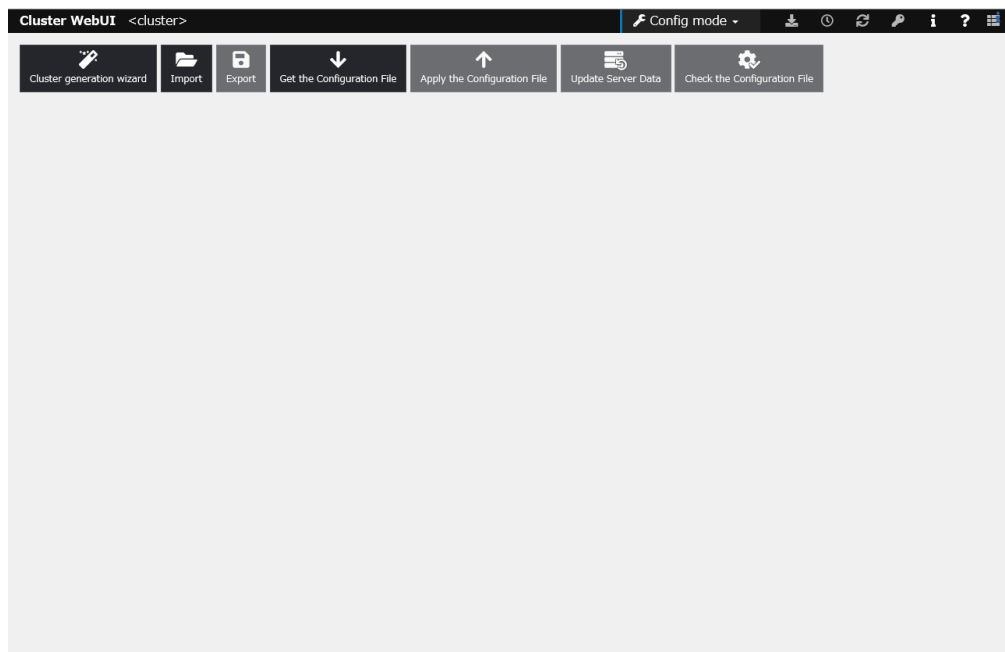
For the settings of other resources and monitor resources, see the Installation and Configuration Guide and the Reference Guide.

1) Creating a cluster

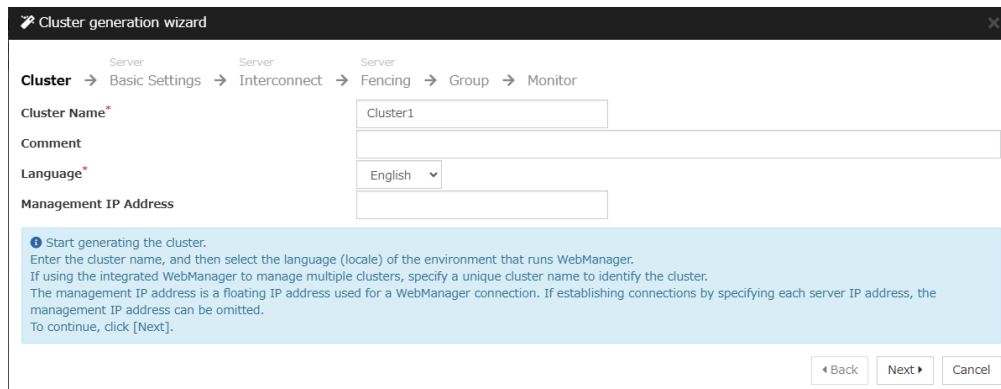
Start the Cluster generation wizard to create a cluster.

- Creating a cluster

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

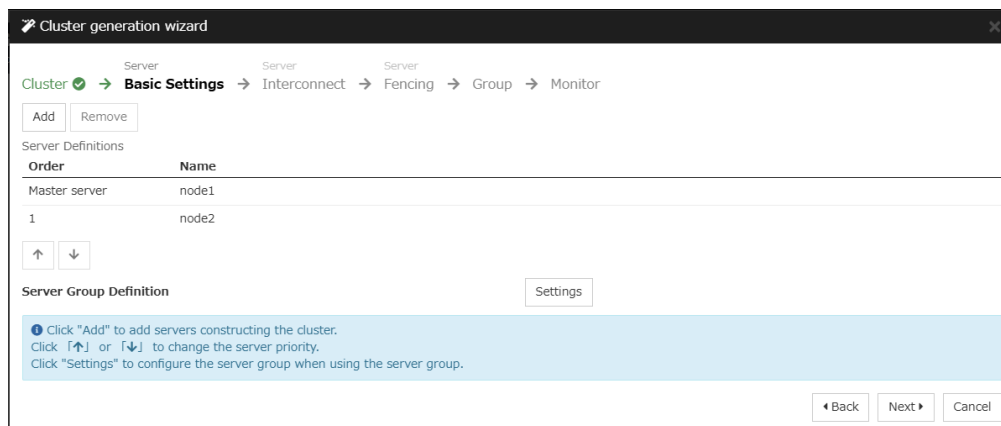
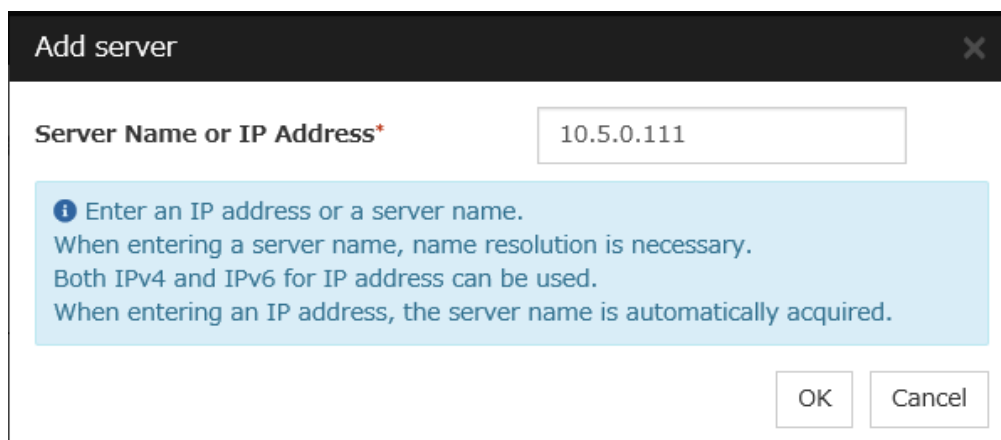


2. **Cluster of Cluster generation wizard** is displayed.
Enter a desired name in **Cluster Name**.
Select an appropriate language in **Language**. Click **Next**.



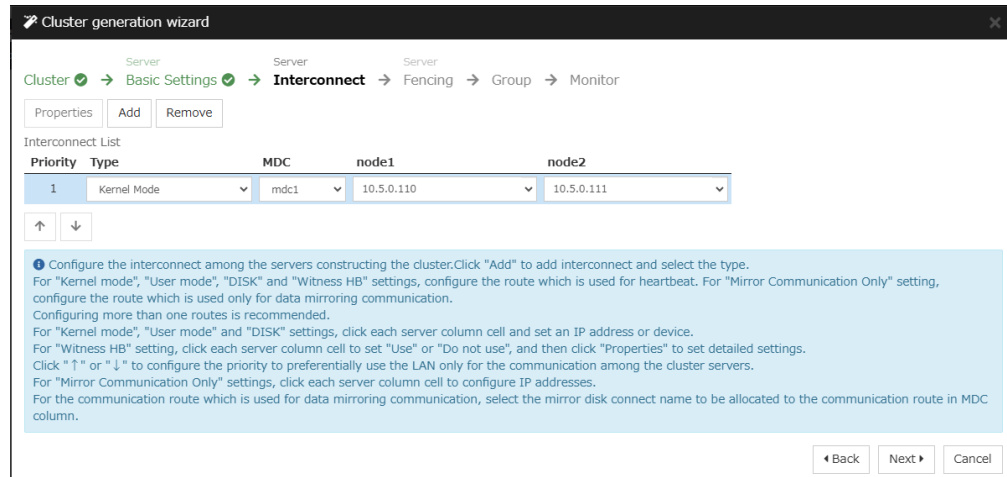
3. **Basic Settings** is displayed.

The instance connected to Cluster WebUI is displayed as a registered master server. Click **Add** to add the remaining instances (by specifying the private IP address of each instance). Click **Next**.



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

Specify the IP addresses (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**.

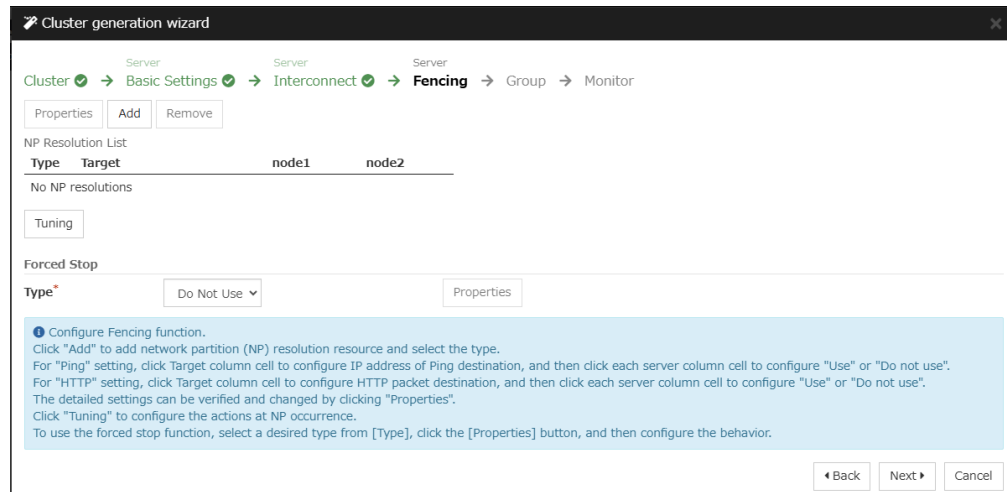


5. The **Fencing** window is displayed.

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**.



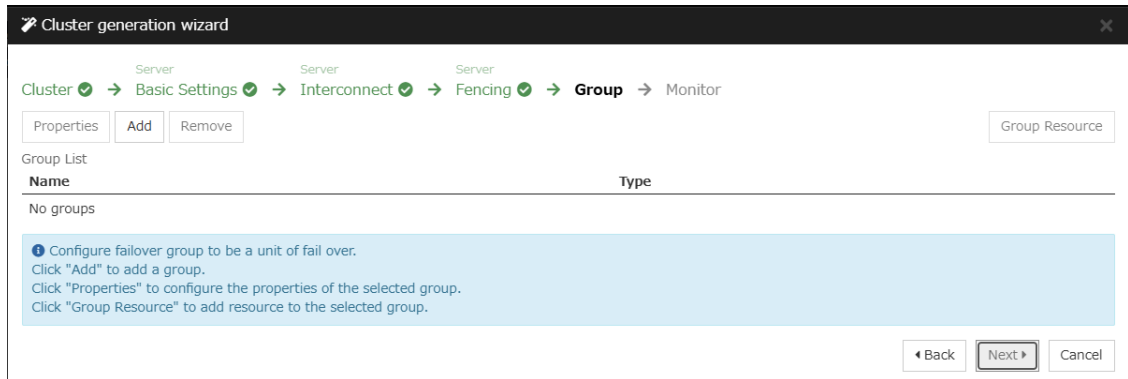
2) Adding a group resource

- Defining a group

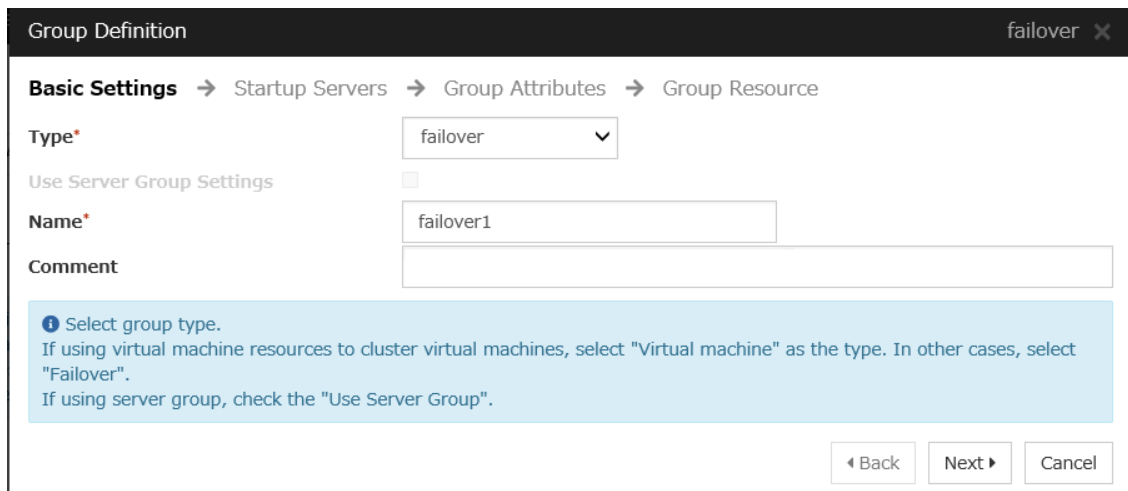
Create a failover group.

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

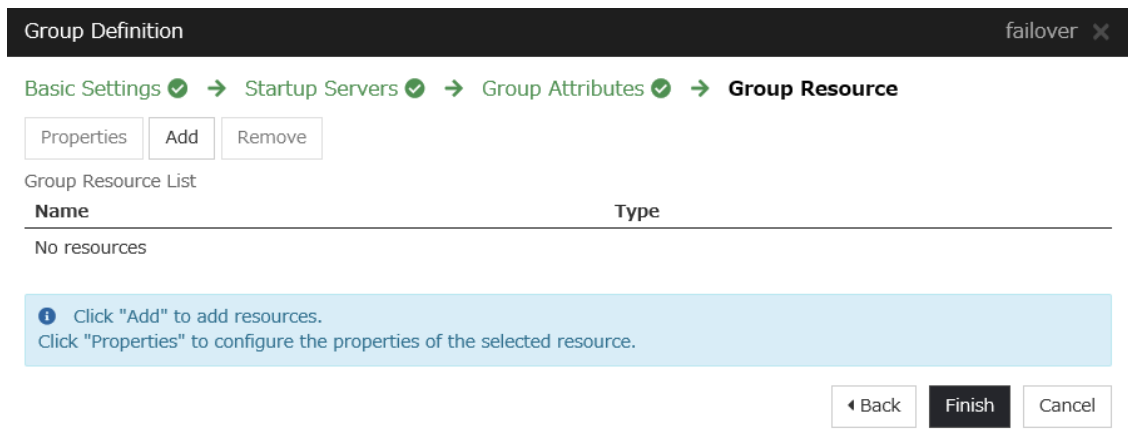
Click **Add**.



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. **Group Resource List** 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 X

Info → Dependency → Recovery Operation → Details

Type*

Name*

Comment

i 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.
Enter the device name of the partition created in "6. Configuring virtual machines" in **Data Partition Device Name** and **Cluster Partition Device Name**. Specify **Mount Point** and **File System**. Click **Finish** to finish setting.

Resource Definition of Group | failover1 md X

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

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

Mirror Partition Device Name*

Mount Point*

Data Partition Device Name*

Cluster Partition Device Name*

File System*

Mirror Disk Connect

- 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**.

Resource Definition of Group | failover1 azuredns X

Info → Dependency → Recovery Operation → Details

Type* Azure DNS resource ▼

Name* azuredns1

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. 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, Thumbprint 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.
Only when using Azure CLI 1.0 (Azure classic CLI), enter **Thumbprint of Service Principal**.
For **User URI** and **Tenant ID**, specify respectively the appID and the tenant you wrote down at "9. **Creating a service principal**".

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 "Understanding Azure DNS monitor resources" in the "Reference Guide".

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

- Custom monitor resource

Sets a script to monitor whether communication with the Microsoft Azure Service Management API is possible, and also to monitor 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*

Name*

Comment

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

- 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* sec

Timeout* sec

Do Not Retry at Timeout Occurrence

Do Not Execute Recovery Action at Timeout Occurrence

Retry Count* time

Wait Time to Start Monitoring* sec

Monitor Timing

Always

Active

Target Resource

Nice Value

Choose servers that execute monitoring

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

```
#!/bin/sh
<EXPRESSCLUSTER-installation-path>/bin/clpazure_port_checker -h_
↪management.core.windows.net -p 443
exit $?
```

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.sh Edit View Replace

Monitor Type Synchronous
 Asynchronous

Wait a period of time for Application/Script monitor to start 0 sec

Log Output Path

Rotate Log

Rotation Size 1000000 byte

Normal Return Value* 0

Wait for activation monitoring to stop before stopping the cluster

◀ 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

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 X

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

Type* IP monitor

Name* ipw1

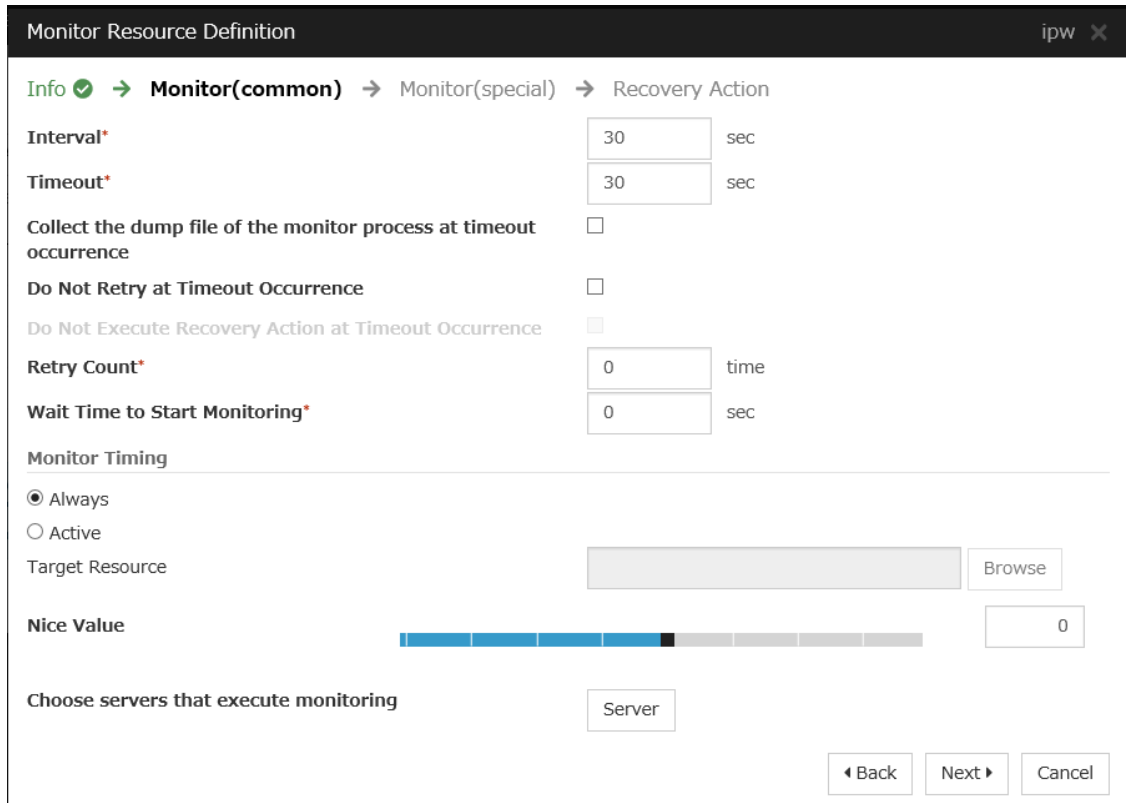
Comment

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**.

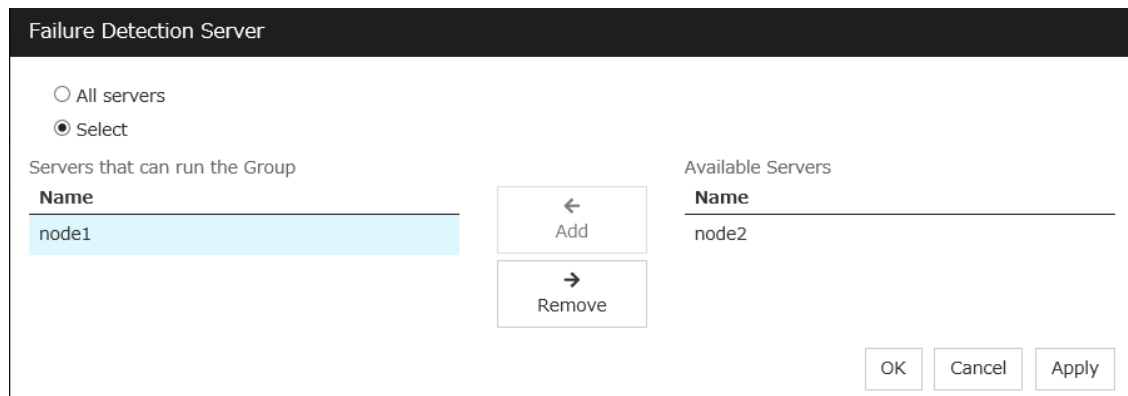


The 'Monitor Resource Definition' dialog box is shown with the following settings:

- Interval*: 30 sec
- Timeout*: 30 sec
- Collect the dump file of the monitor process at timeout occurrence:
- Do Not Retry at Timeout Occurrence:
- Do Not Execute Recovery Action at Timeout Occurrence:
- Retry Count*: 0 time
- Wait Time to Start Monitoring*: 0 sec
- Monitor Timing: Always, Active
- Target Resource: [Empty field] Browse
- Nice Value: [Slider bar] 0
- Choose servers that execute monitoring: [Server]

Buttons: ◀ Back, Next ▶, Cancel

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

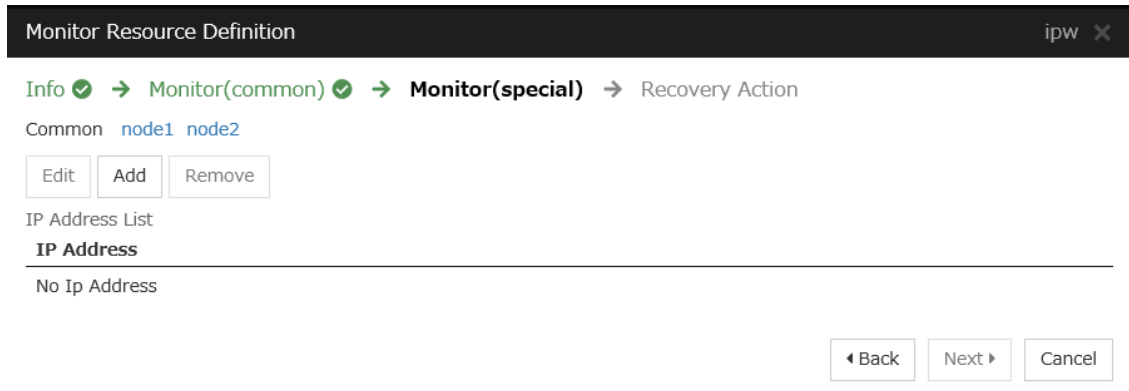


The 'Failure Detection Server' dialog box is shown with the following settings:

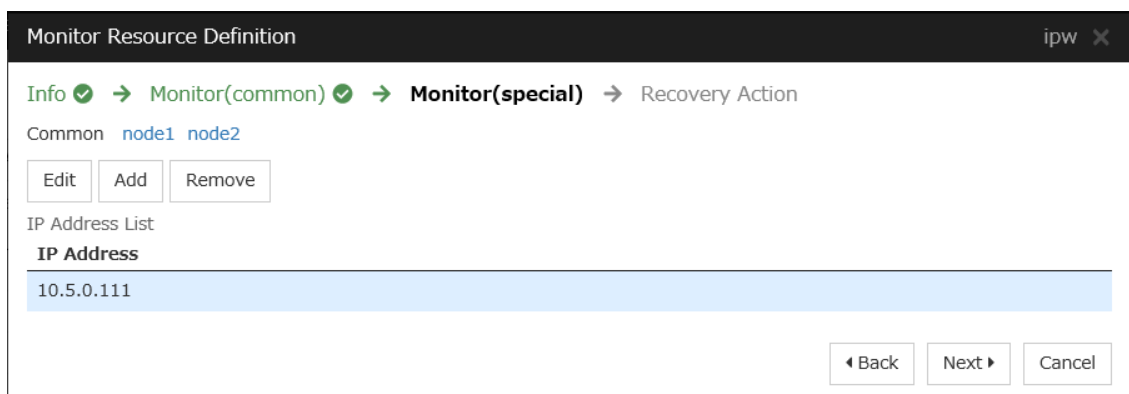
- All servers
- Select
- Servers that can run the Group:
 - Name: node1
- Available Servers:
 - Name: node2
- Buttons: Add, Remove
- Buttons: OK, Cancel, Apply

Click **Next**.

- 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 3. Click **Next**.



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**.

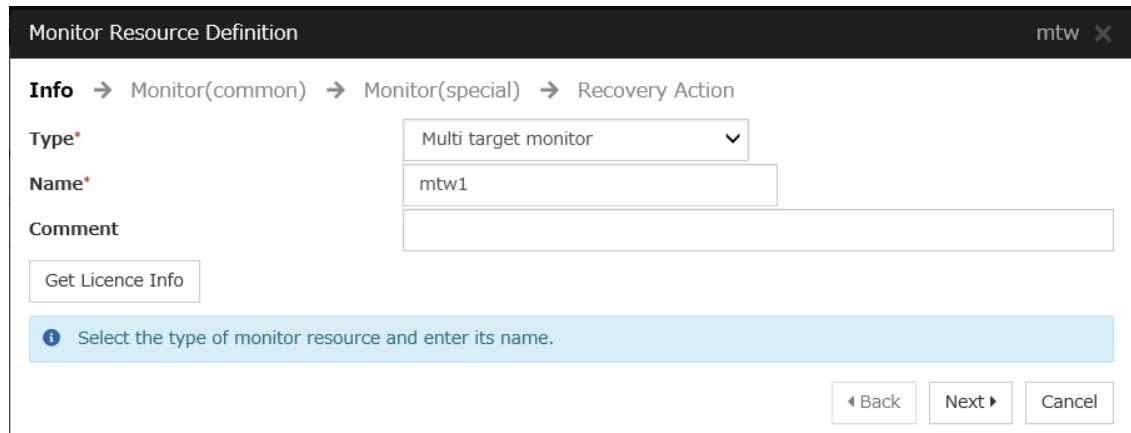
6. Click **Finish** to finish setting.
 7. Then, create a monitor resource on the other server. Click **Add** on the **Monitor Resource List** page.
 8. Select the monitor resource type (IP monitor) from the **Type** box and enter the monitor resource name (ipw2) in the **Name** box. Click **Next**.
 9. The **Monitor (common)** window is displayed.
Confirm that **Monitor Timing** is **Always**.
Select one available server for **Choose servers that execute monitoring**.
Click **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 both the custom monitor resource monitoring communication to Microsoft Azure Service Management API and the IP monitor resource between clusters that are configured with virtual machines.

If the statuses of both monitor resources are abnormal, execute the script in which the processing for NP resolution is described.

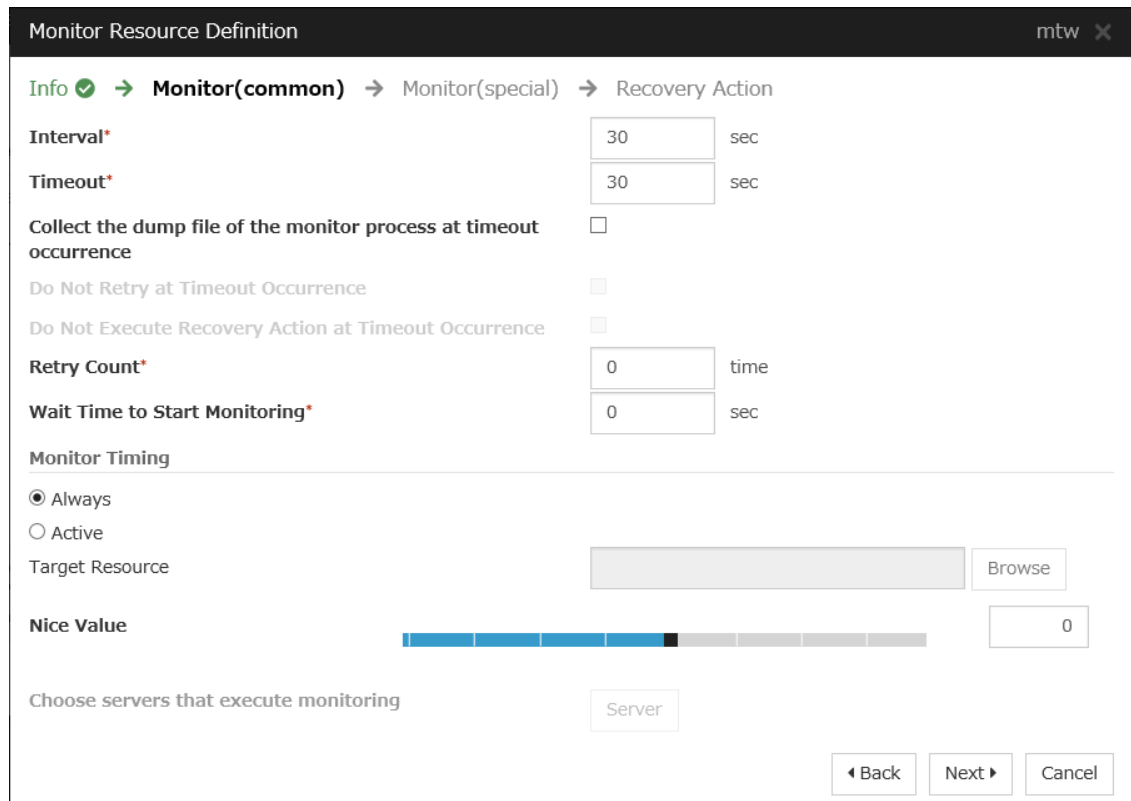
For details about the multi target monitor resource, see Understanding multi target monitor resources in the Reference Guide.

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 breadcrumb 'Info → Monitor(common) → Monitor(special) → Recovery Action'. The 'Type' dropdown is set to 'Multi target monitor' and the 'Name' field contains 'mtw1'. A blue information bar at the bottom states: 'Select the type of monitor resource and enter its name.' Navigation buttons for 'Back', 'Next', and 'Cancel' are visible at the bottom right.

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 breadcrumb 'Info → Monitor(common) → Monitor(special) → Recovery Action'. The 'Monitor Timing' section has 'Always' selected. Other fields include 'Interval' (30 sec), 'Timeout' (30 sec), 'Retry Count' (0 time), and 'Wait Time to Start Monitoring' (0 sec). There are checkboxes for 'Collect the dump file of the monitor process at timeout occurrence', 'Do Not Retry at Timeout Occurrence', and 'Do Not Execute Recovery Action at Timeout Occurrence'. A 'Target Resource' field with a 'Browse' button and a 'Nice Value' slider (set to 0) are also present. A 'Choose servers that execute monitoring' field contains 'Server'. Navigation buttons for 'Back', 'Next', and 'Cancel' are visible at the bottom right.

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**.

Monitor Resource Definition mtw X

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

Monitor Resources		Available Monitor Resources	
Monitor Resource	Type	Monitor Resource	Type
genw1	genw	No Available Monitor Resources	
ipw1	ipw		
ipw2	ipw		

← Add → Remove

Tuning

◀ 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 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:

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**.

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 a cluster name.



Cluster Name: Cluster1
Comment:
Language: English

OK Cancel Apply

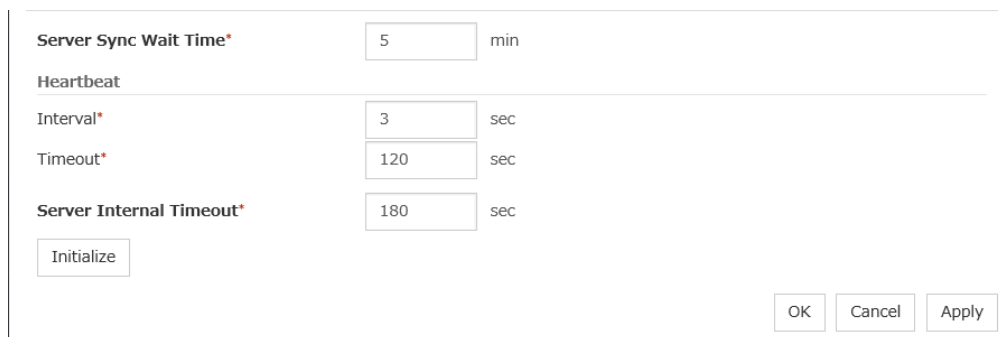
2. Select the **Timeout** tab. For **Timeout of Heartbeat**, specify a value calculated by "A+B+C" as described below.

- 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 it took for the multi target monitor resource 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.



Server Sync Wait Time*: 5 min
Heartbeat
Interval*: 3 sec
Timeout*: 120 sec
Server Internal Timeout*: 180 sec

Initialize

OK Cancel Apply

3. Click **OK**.

5) Applying the settings and starting the cluster

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

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 (node1). In the **Status** tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node1 is **Normal**.
2. Log in to the Microsoft Azure portal, select cluster1.zone on the DNS zone, 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, 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 node2. In the **Status** tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node2 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 node1 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 node1 and node2)

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

Continued on next page

Table 5.1 – continued from previous page

Setting item	Setting value
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
- Network IP configuration	10.5.0.110 10.5.0.111
- 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	

Continued on next page

Table 5.1 – continued from previous page

Setting item	Setting value
- Name	TestHTTP
- Protocol	TCP
Destination Port range	8080 (Port number offering the operation)

- Microsoft Azure settings (specific to each of node1 and node2)

Setting item	Setting value	
	node1	node2
Virtual machine setting		
- Disk type	Standard HDD	Standard HDD
- User name	testlogin	testlogin
- Password	PassWord_123	PassWord_123
- Resource group	TestGroup1	TestGroup1
- Region	(Asia Pacific) Japan East	(Asia Pacific) Japan East
Network security group setting		
- Name	node1-nsg	node2-nsg
Availability set setting		
- Name	AvailabilitySet1	AvailabilitySet1
- Update domains	5	5
- Fault domains	2	2
Diagnostics storage account setting		
- Name	Automatically generated	Automatically generated
- Performance	Standard	Standard

Continued on next page

Table 5.2 – continued from previous page

Setting item	Setting value	
	node1	node2
– Replication	Locally-redundant storage (LRS)	Locally-redundant storage (LRS)
IP configuration setting		
– IP address	10.5.0.110	10.5.0.111
Disk setting		
– Name	node1_DataDisk_0	node2_DataDisk_0
– Source type	None (empty disk)	None (empty disk)
– Account type	Standard HDD	Standard HDD
– Size	20	20

- EXPRESSCLUSTER settings (cluster properties)

Setting item	Setting value	
	node1	node2
– Cluster Name	Cluster1	Cluster1
– Server Name	node1	node2
– Timeout Tab: Heartbeat timeout	120	120

- EXPRESSCLUSTER settings (failover group)

Resource name	Setting item	Setting value
Mirror disk resource	Name	md
	Details Tab: Mount Point	/mnt/md
	Details Tab: Data Partition Device Name	/dev/sdc2
	Details Tab: Cluster Partition Device Name	/dev/sdc1
	Details Tab: File System	ext4
	Mirror Tab: Execute the initial mirror construction	On
	Mirror Tab: Execute initial mkfs	On

Continued on next page

Table 5.4 – continued from previous page

Resource name	Setting item	Setting value
Azure probe port resource	Name	azurepp1
	Probe port	26001 (Value specified for Port of Health probe)

- EXPRESSCLUSTER settings (monitor resource)

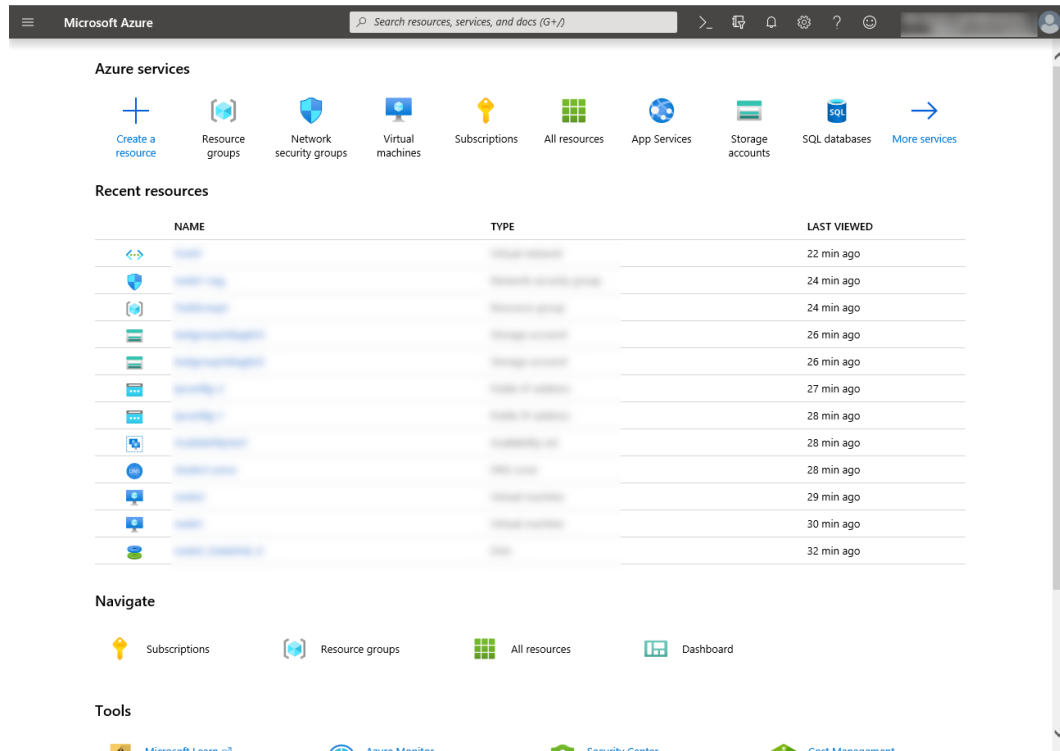
Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	Name	mdw1
Azure probe port monitor resource	Name	azureppw1
	Recovery Target	azurepp1
Azure load balance monitor resource	Monitor resource name	azurelbw1
	Recovery Target	azurepp1
Custom monitor resource	Name	genw1
	Script created 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	node1
	IP Address	10.5.0.111
	Recovery Action	Execute only the final action
IP monitor resource	Recovery Target	LocalServer
	Name	ipw2
	Server to monitor	node2
	IP Address	10.5.0.110
Multi target monitor resource	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
	Execute Script before Final Action	On
	Timeout	30

5.2 Configuring Microsoft Azure

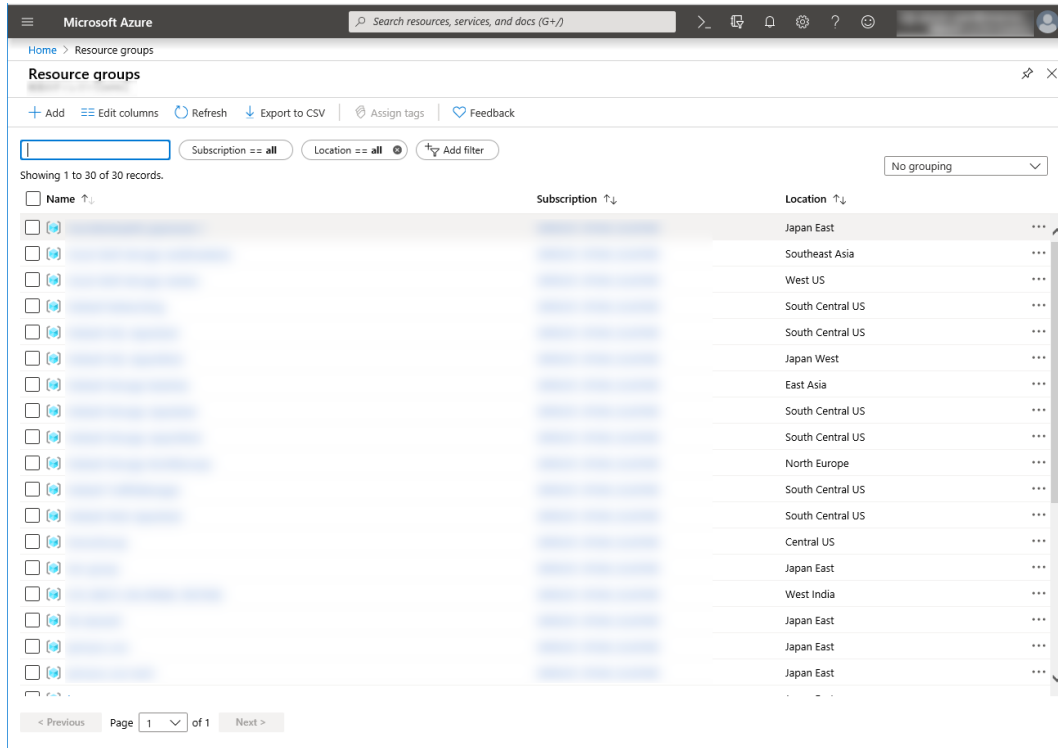
1. Creating a resource group

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

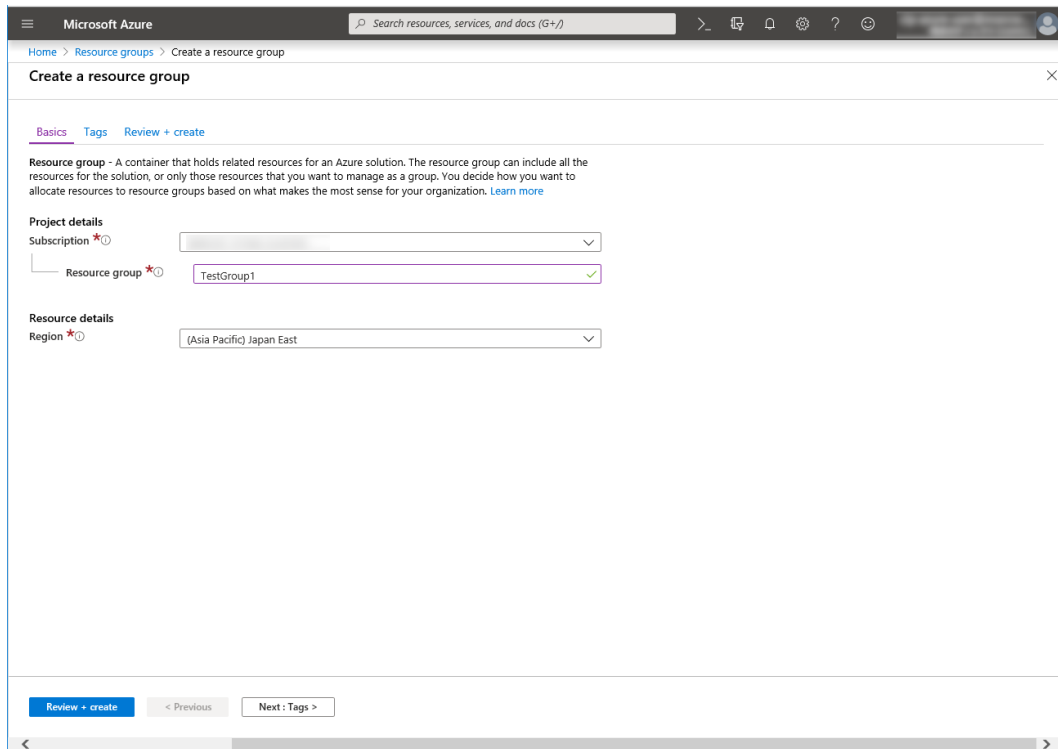
1. Select the **Resource groups** icon on the upper part of the window. If there are existing resource groups, they are displayed in a list.



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



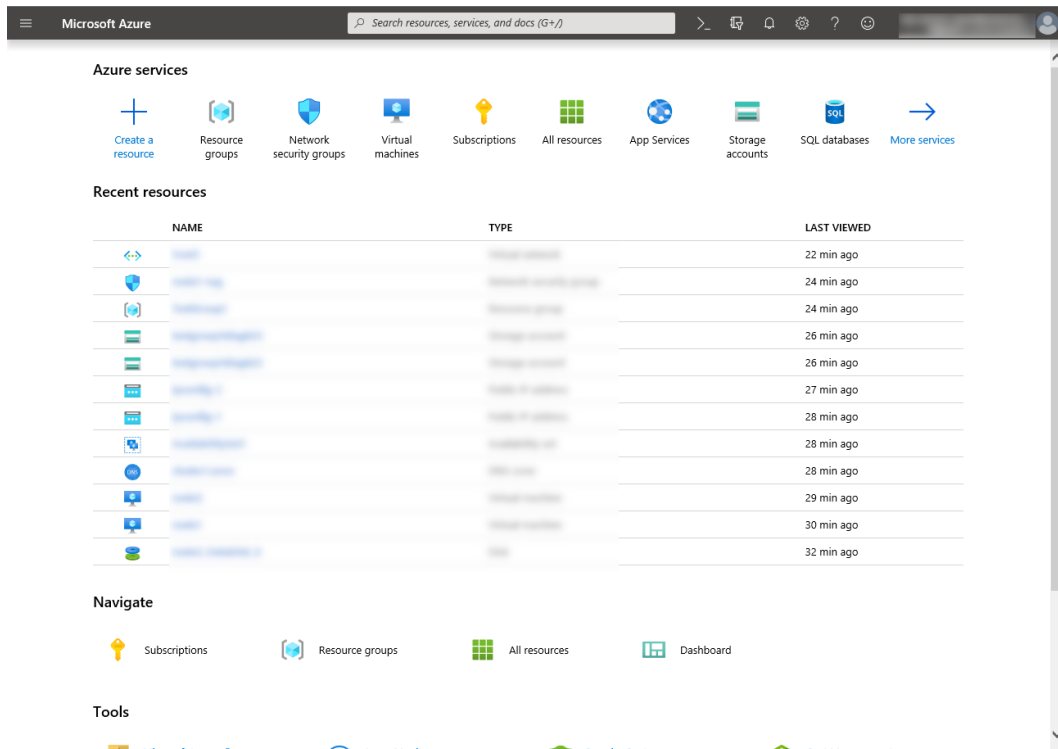
3. Specify **Subscription**, **Resource group**, and **Region**, and click **Review+Create**.



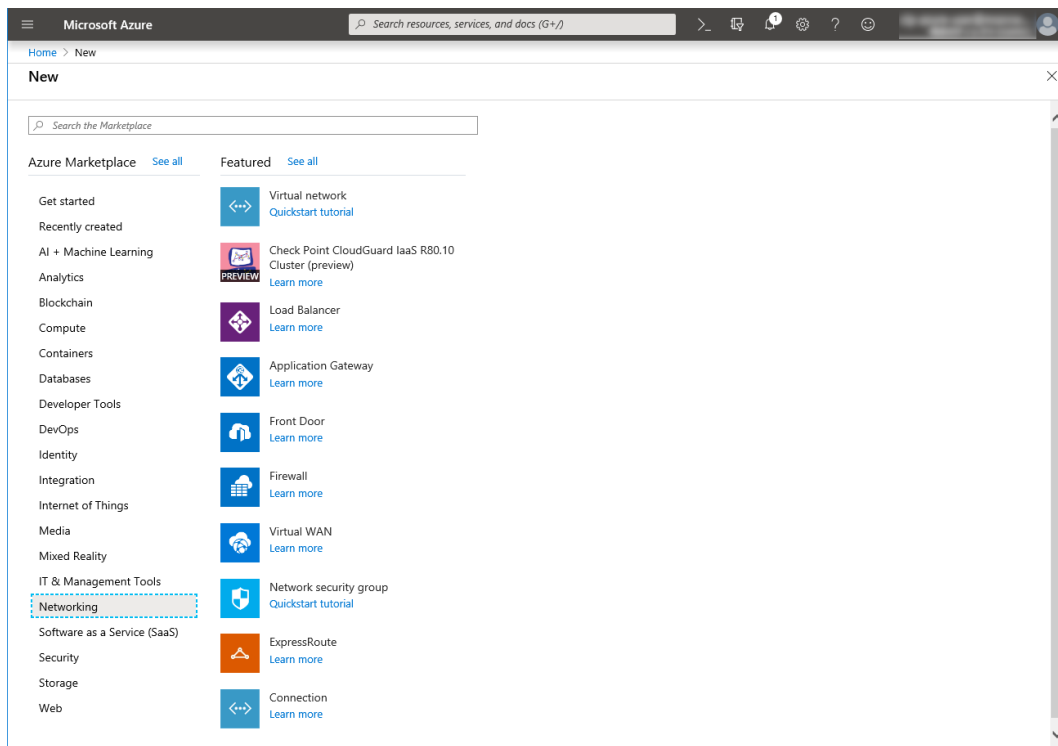
2. **Creating a virtual network**

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

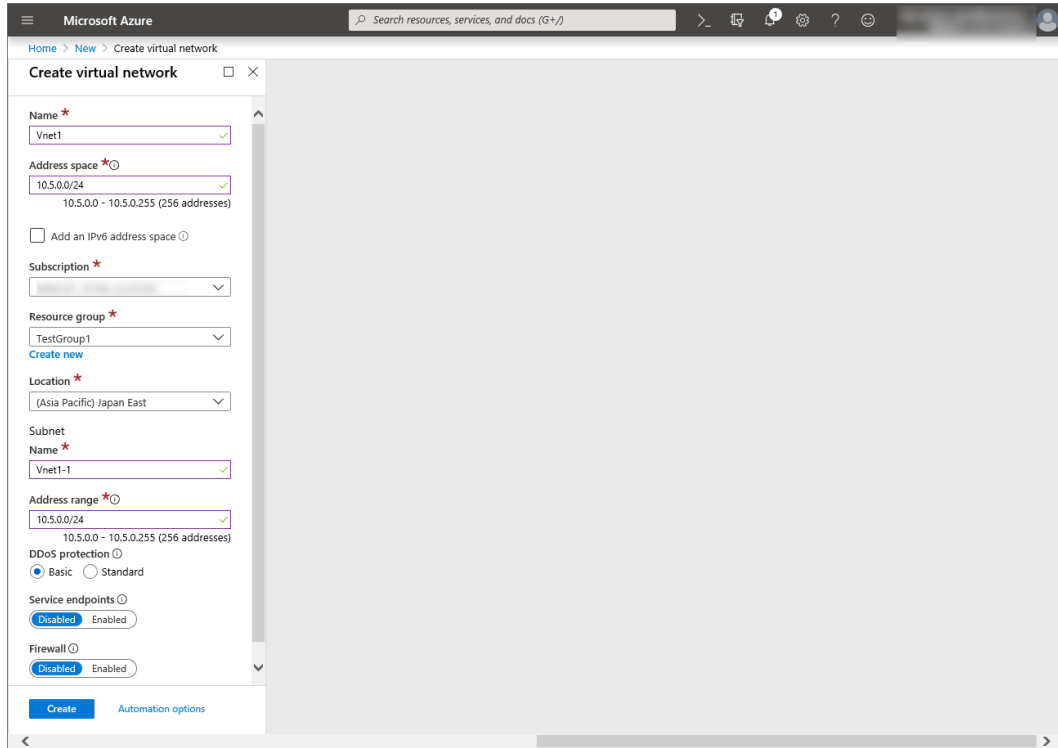
1. Select the **Create a resource** icon on the upper part of the window.



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



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

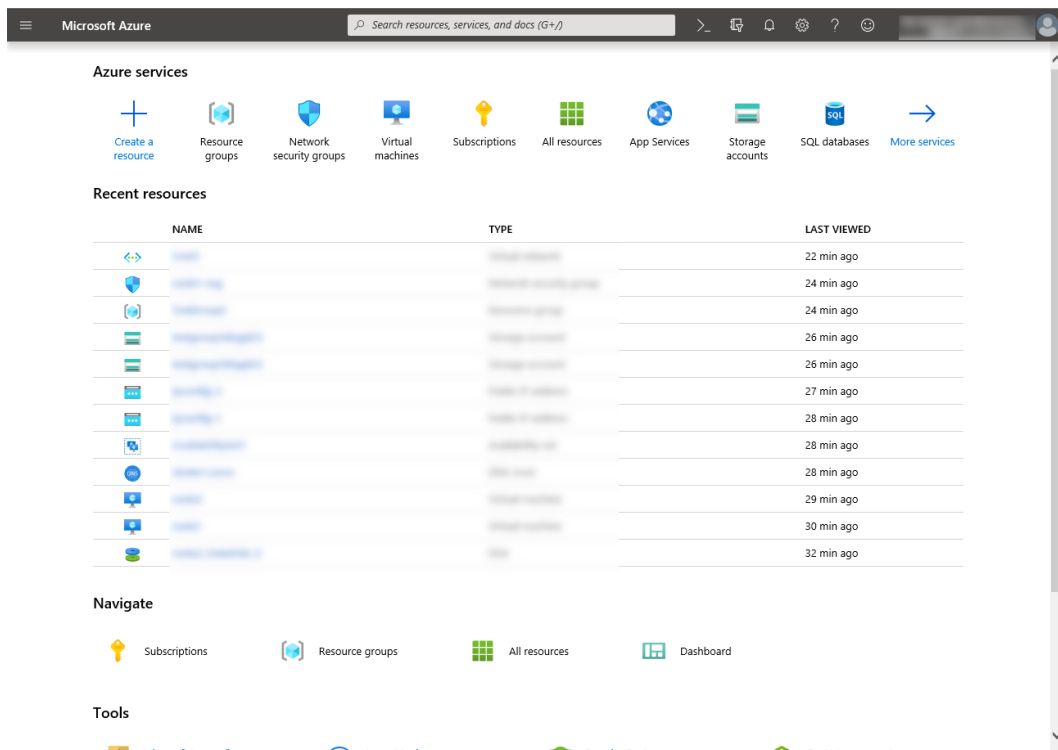


3. Creating a virtual machine

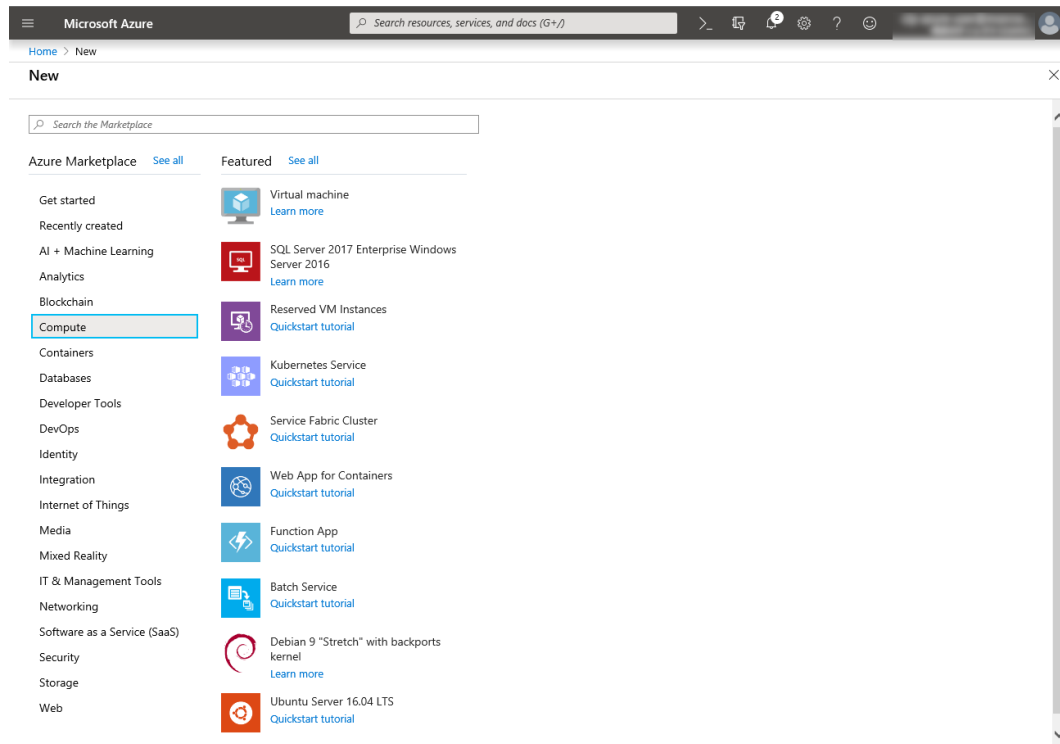
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create virtual machines and disks following the steps below.

Create as many virtual machines as required to create a cluster. Create node1 and then node2.

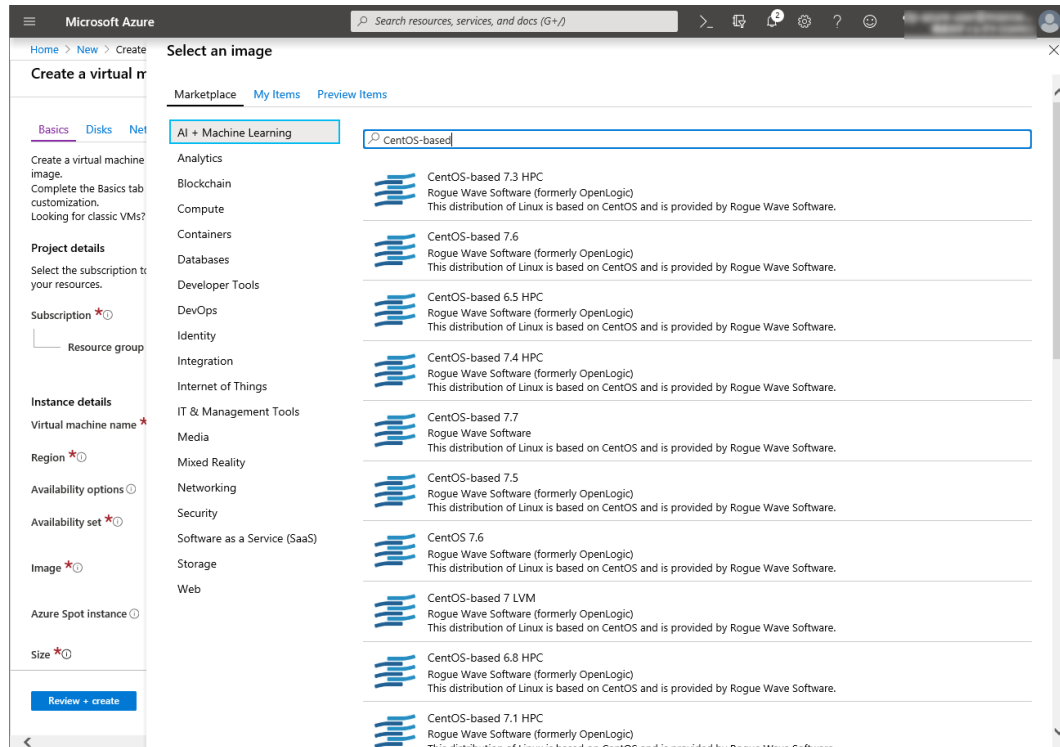
1. Select the **Create a resource** icon on the upper part of the window.



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



3. Select **CentOS-based 7.6**

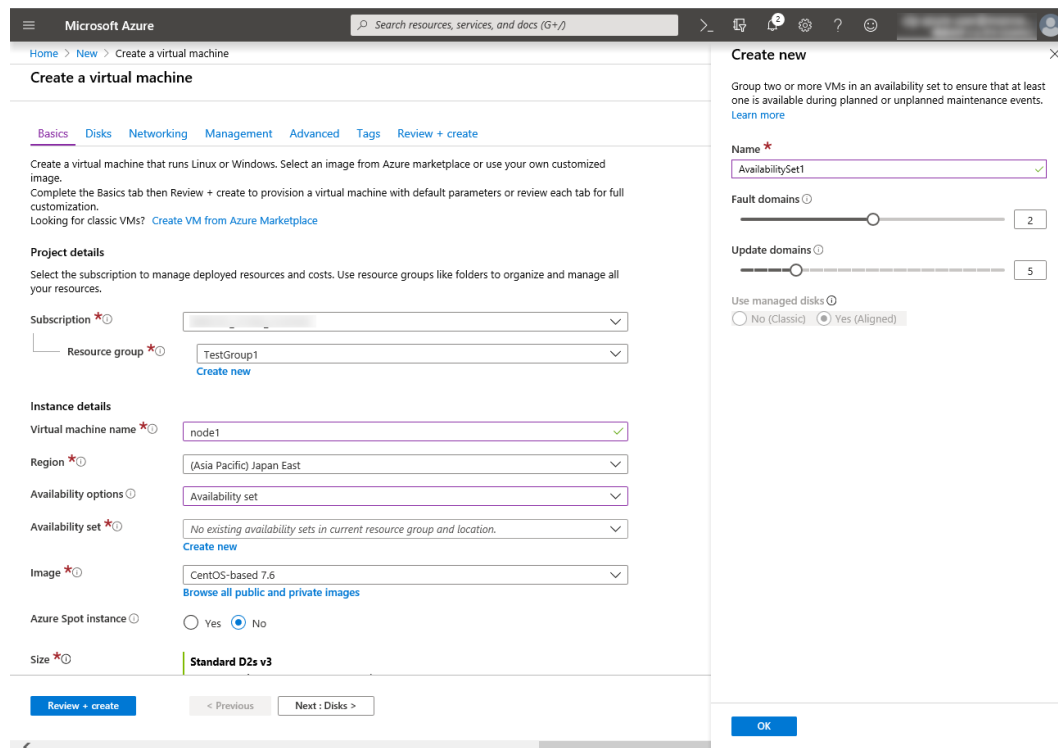
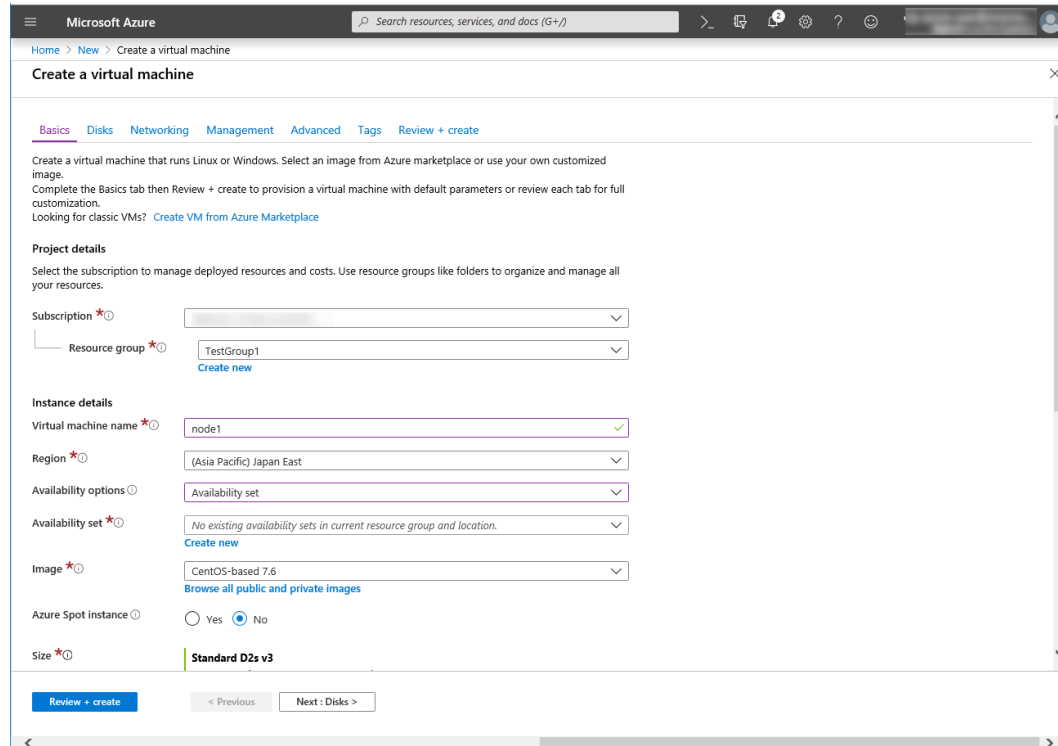


4. Click **Create**.

5. 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 **Create new** appears, specify the settings of **Name, Fault domains, and Update domains**. Then click **OK**.



6. Click **Change size** to display **Select a VM size**.

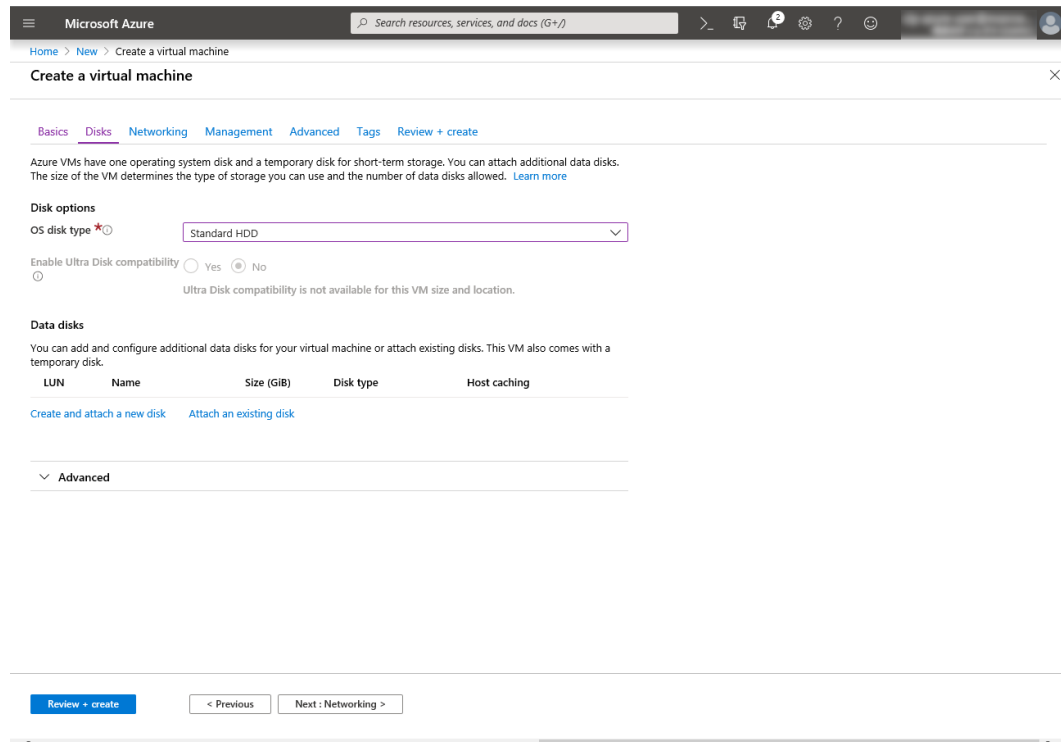
From the list, choose a size (**Standard - A1** in this guide) suitable for your virtual machine and click **Select**.

Regarding the **Virtual machine name**, node1 is for node1, and node2 is for node2.

Click **Next: Disks >**

7. 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**.



8. **Create a new disk** appears. Specify the settings of **Name**, **Source type** and **Size**. Then click **OK**. Click **Next: Networking >**.

Create a new disk

Create a new disk to store applications and data on your VM. Disk pricing varies by storage type, and number of transactions. [Learn more about Azure Marketplace](#)

Name *

Source type *

Size * **1024 GiB**
Standard SSD
[Change size](#)

Select a disk size

Browse available disk sizes and their features.

Account type

Size	Disk tier	Max IOPS	Max throughput
32 GiB	S4	500	60
64 GiB	S6	500	60
128 GiB	S10	500	60
256 GiB	S15	500	60
512 GiB	S20	500	60
1024 GiB	S30	500	60
2048 GiB	S40	500	60
4096 GiB	S50	500	60
8192 GiB	S60	1300	300
16384 GiB	S70	2000	500
32767 GiB	S80	2000	500

Create a custom size

Enter the size of the disk you would like to create. You will be charged the same rate for your provisioned disk, regardless of how much of the disk space is being used. For example, a 200 GiB disk is provisioned on a 256 GiB disk, so you would be billed for the 256 GiB provisioned.

Custom disk size (GiB) *

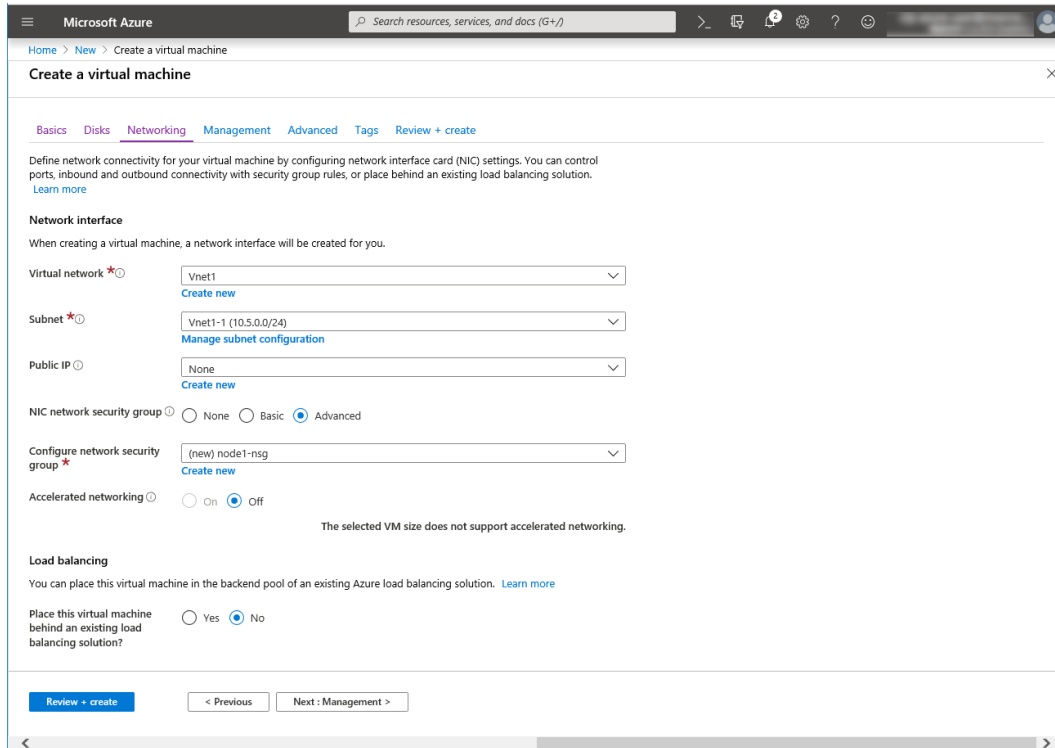
- The **Networking** tab appears.

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

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

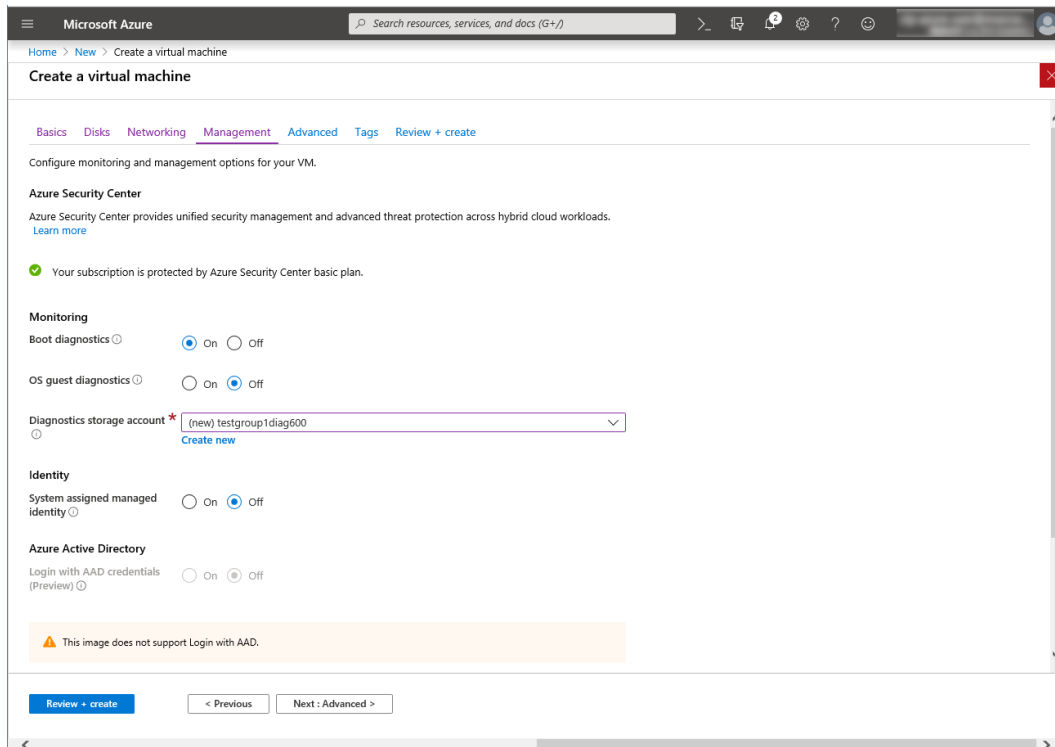
Click **Next: Management** >.

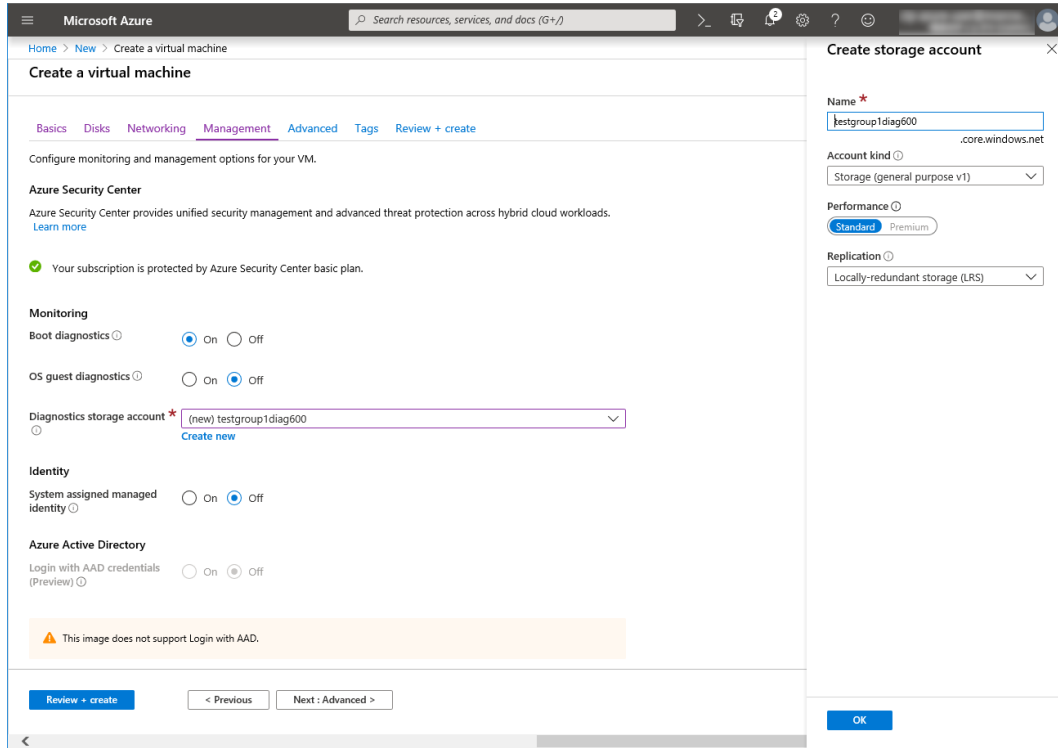
EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



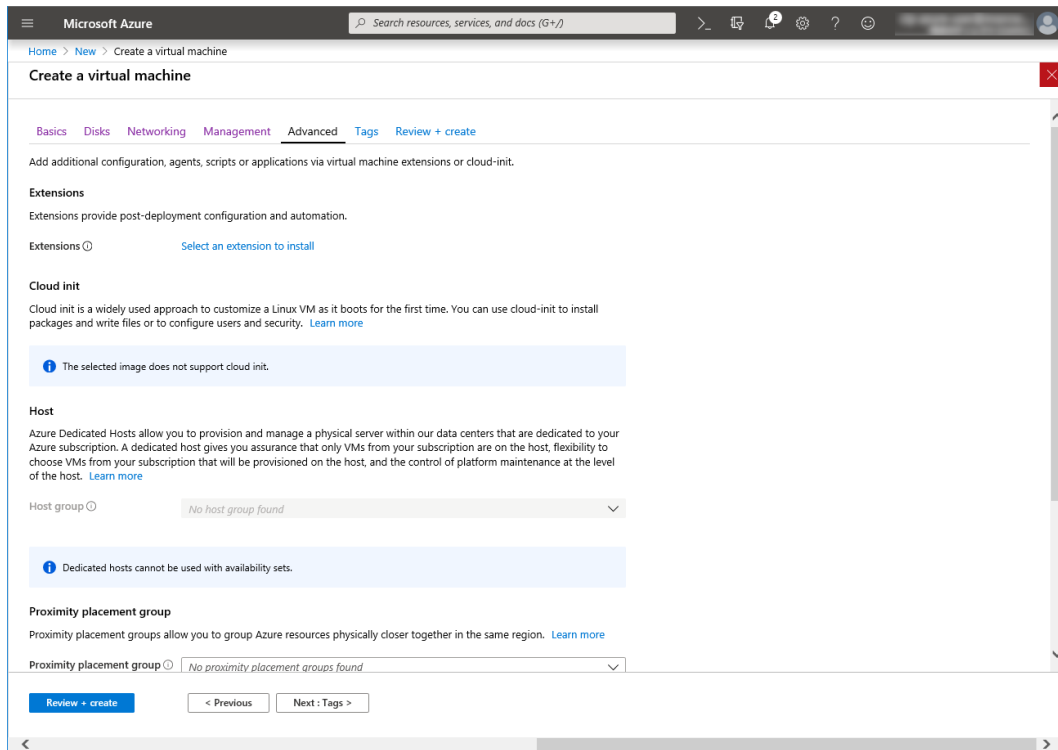
10. The **Management** tab appears.

Click **Create new** under the **Diagnostics storage account** field to display **Create storage account**. 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: Details >**.



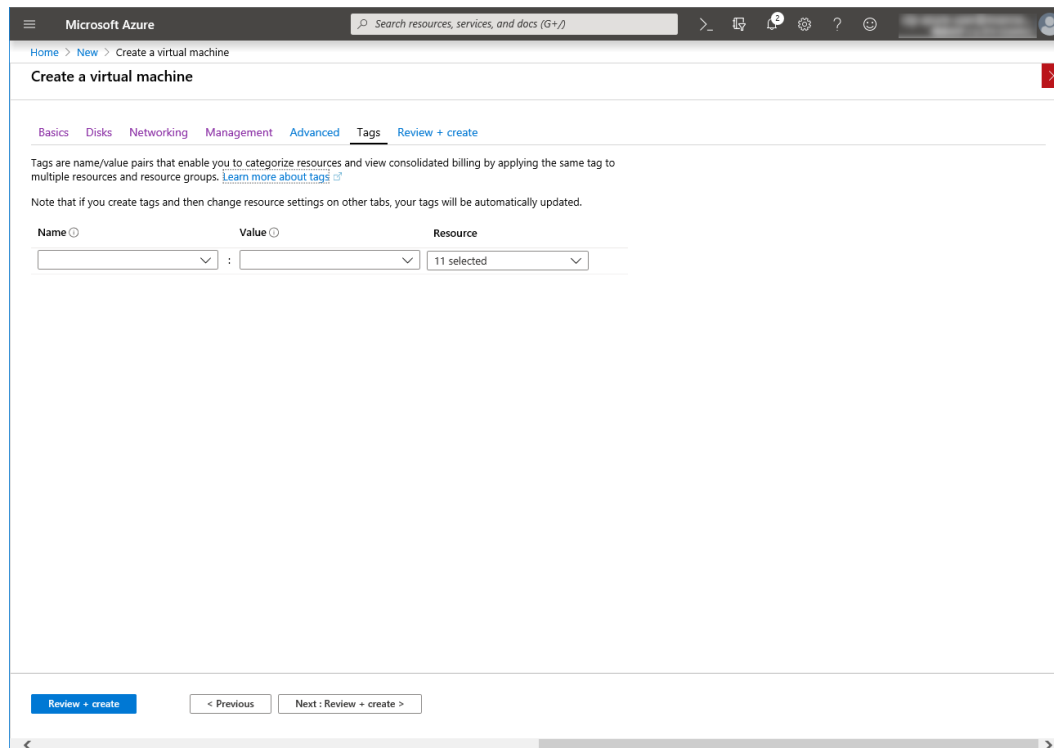


11. Click **Next: Tags >**.

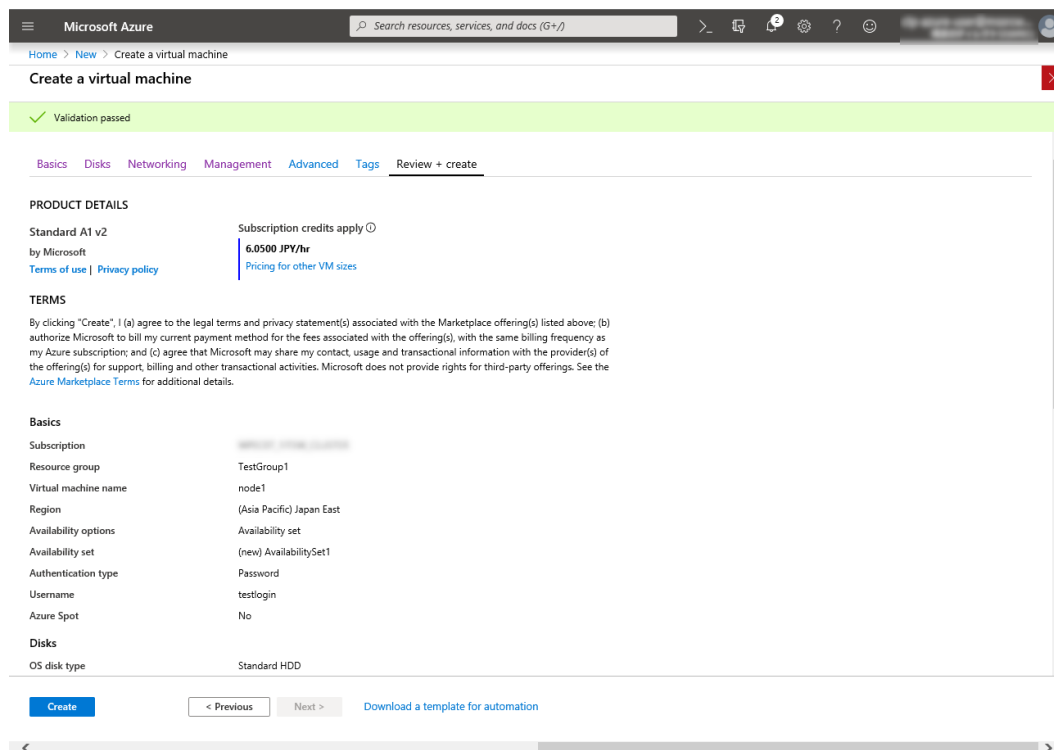


12. Click **Next: Review + create >**.

EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



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

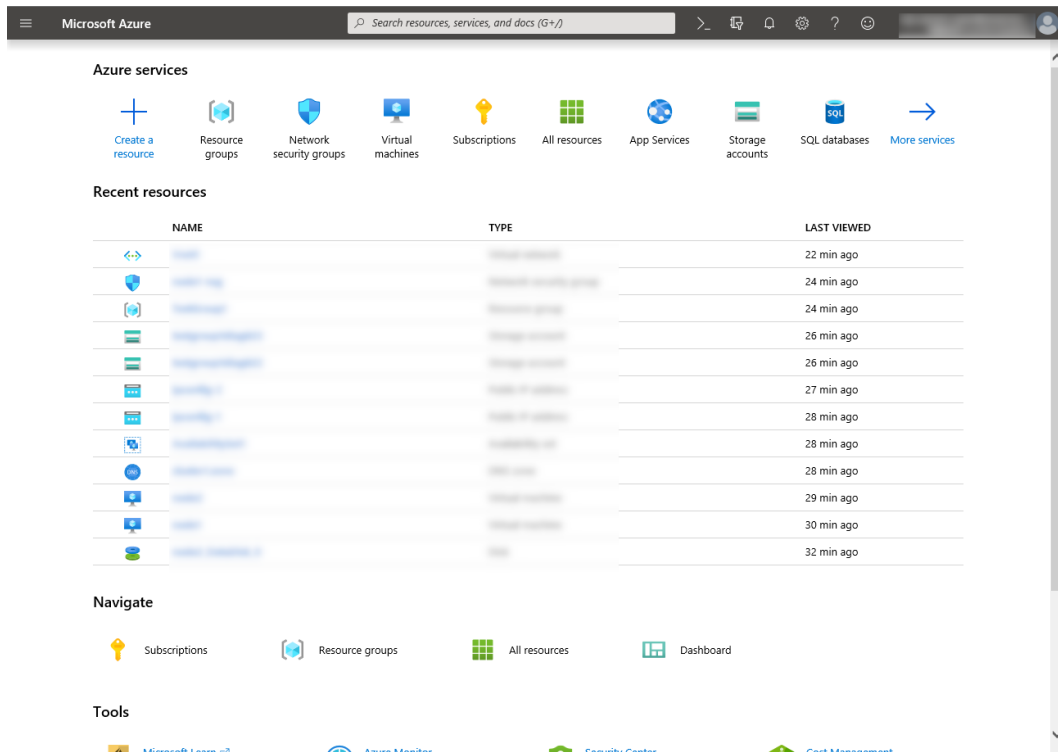


4. Setting a private IP address

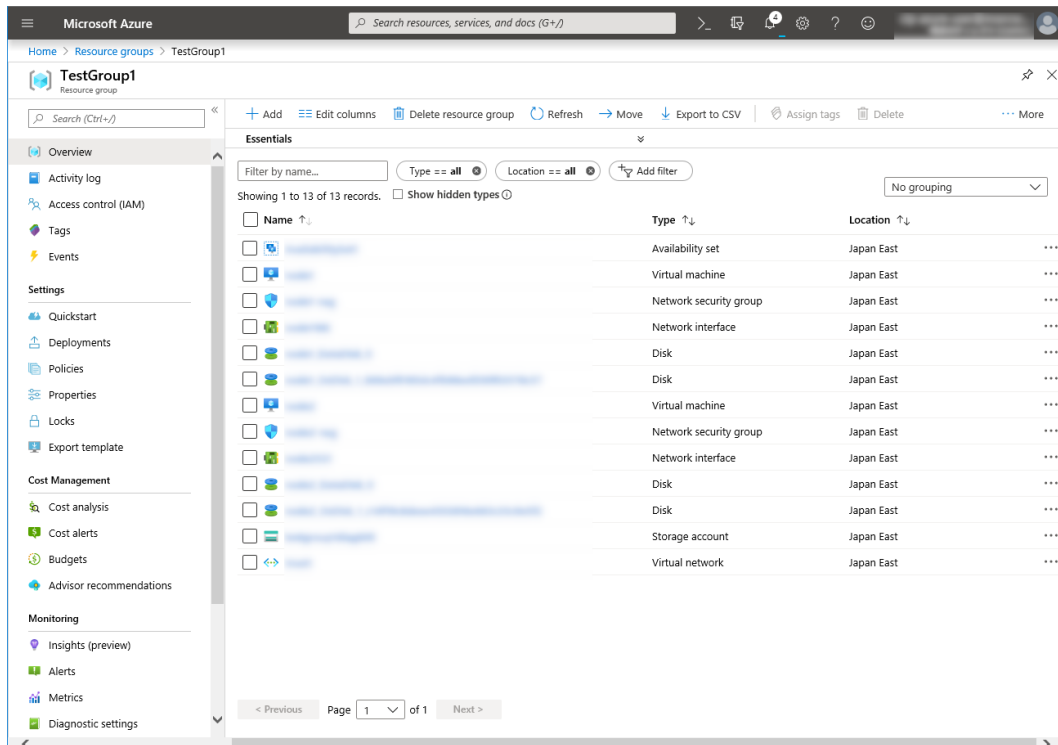
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and change the private IP address setting following the steps below. Since an IP address is initially set to be assigned dynamically, change the

setting so that an IP address is assigned statically. Change the settings of node1 and then node2.

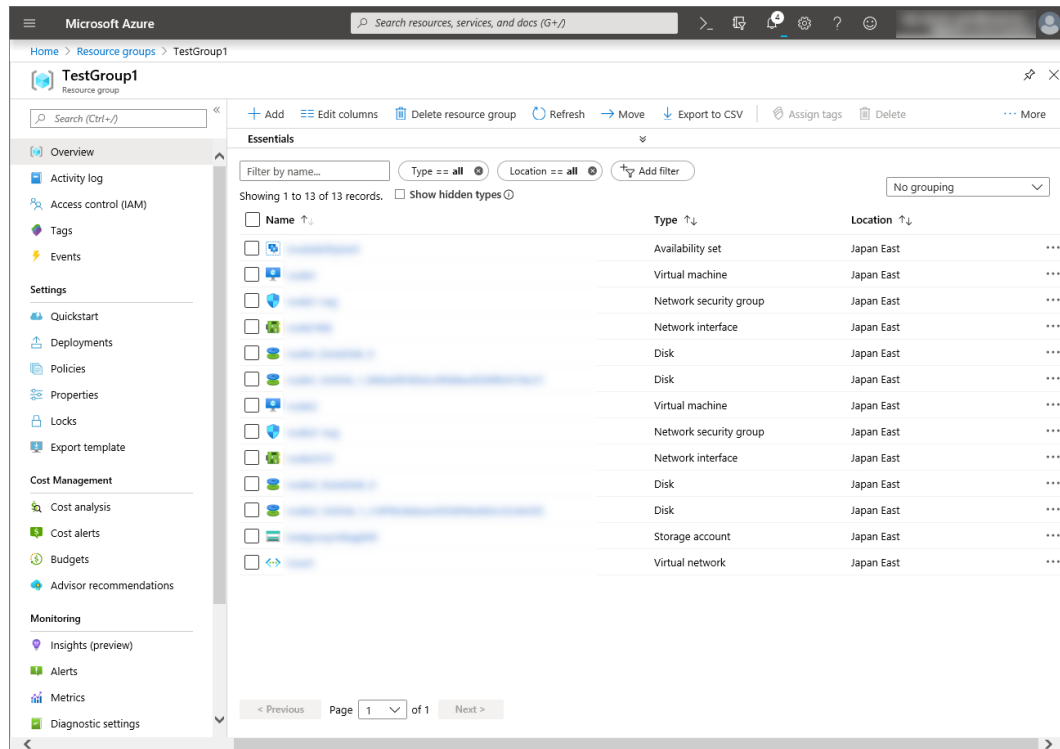
1. Select the **Resource groups** icon on the upper part of the window.



2. Select TestGroup1 from the resource group list.
3. The summary of TestGroup1 is displayed. Select virtual machine node1 or node2 from the item list.

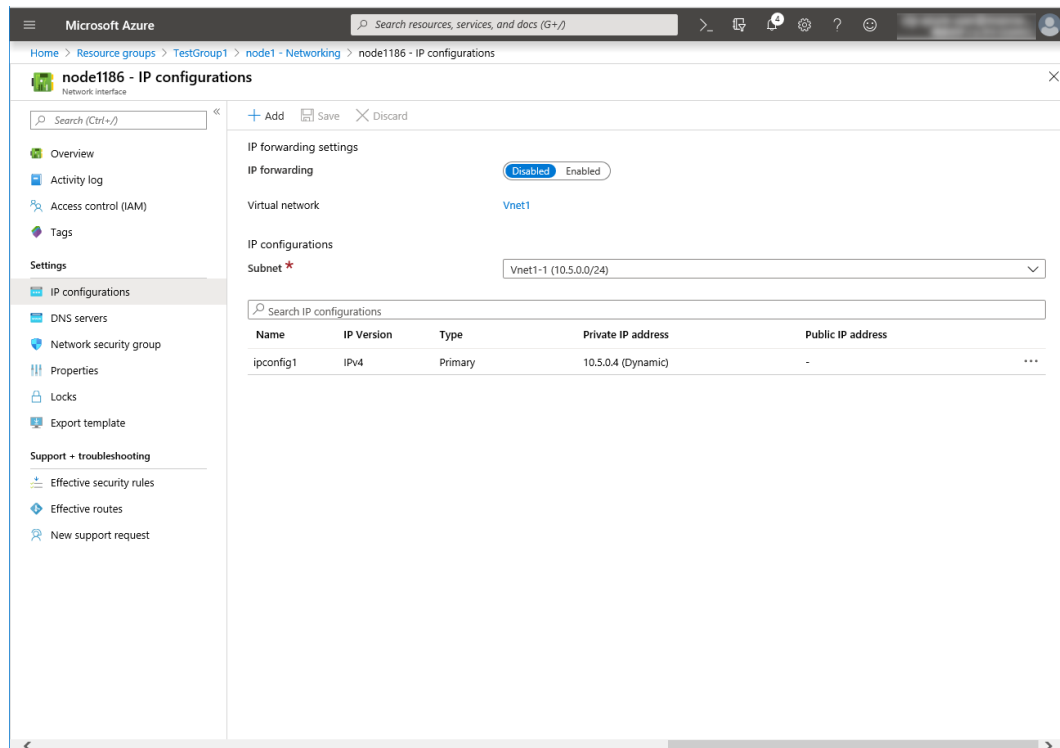


4. Select Networking.

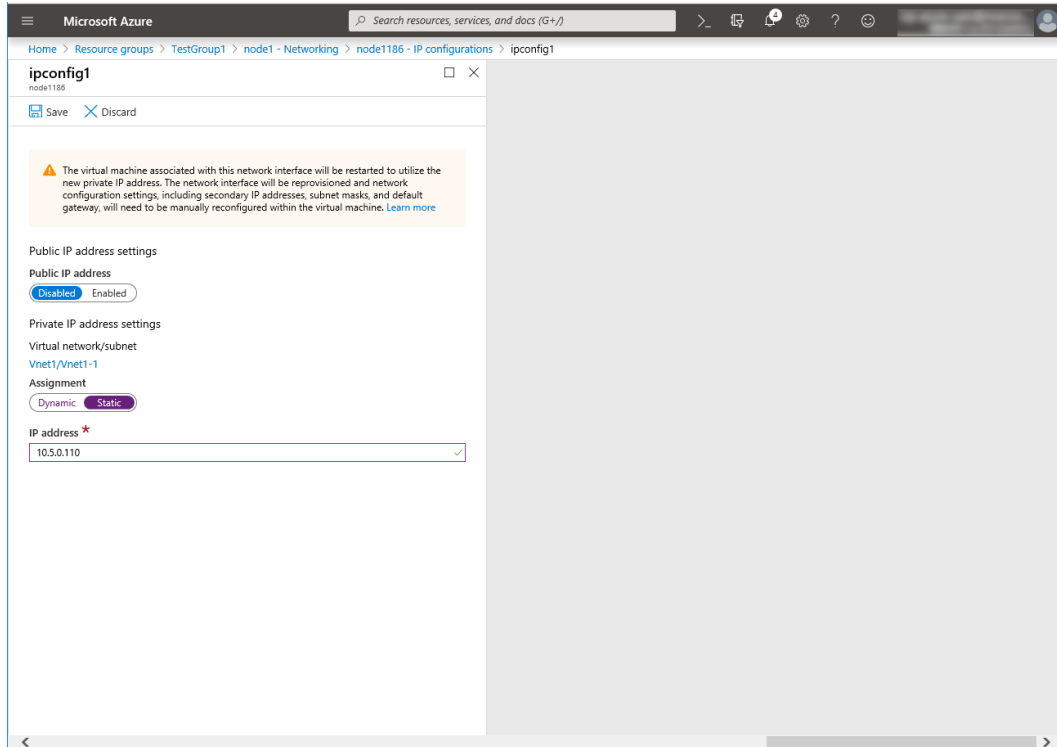


5. Select a network interface displayed in the list. The network interface name is generated automatically.

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 node1 is 10.5.0.110. The IP address of node2 is 10.5.0.111.



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

5. Configuring virtual machines

Log in to the created node1 and node2 and specify the settings following the procedure below. Set a partition for the mirror disk resource. Create a file system in the added disk. Secure an area in the added disk by using the fdisk command and then create a file system. 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. Check the partition list. In the following example, the last line shows the added disk.

```
$ cat /proc/partitions
major minor #blocks name
2          0           4 fd0
8          0    31457280 sda
8          1     512000 sda1
8          2    30944256 sda2
8         16    73400320 sdb
8         17    73398272 sdb1
8         32    20971520 sdc
```

2. Create a cluster partition and data partition in the added disk by using the fdisk command. Allocate 1 GB (1*1024*1024*1024 bytes) or more to a cluster partition. (If the size is specified as just 1 GB,

the actual size will be larger than 1 GB depending on the disk geometry difference. This is not a problem.) Also, do not create a file system in a cluster partition.

3. If you select **Execute initial mkfs** when creating the cluster configuration data by using Cluster WebUI, EXPRESSCLUSTER creates a file system automatically. Note that existing data in the partition will be lost.

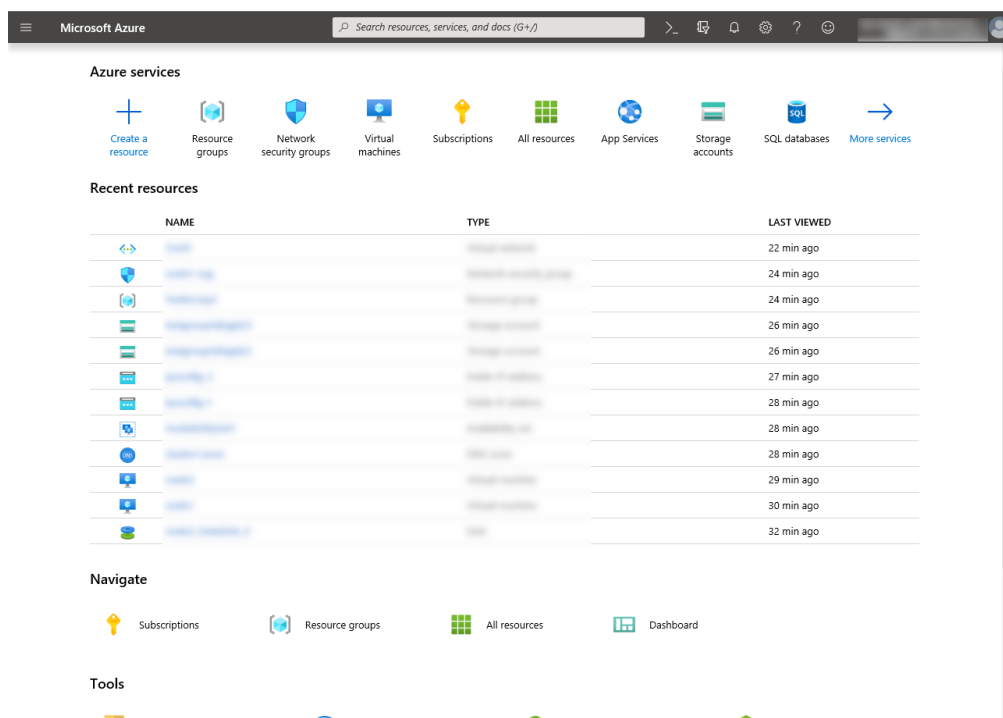
6. Configuring a load balancer

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

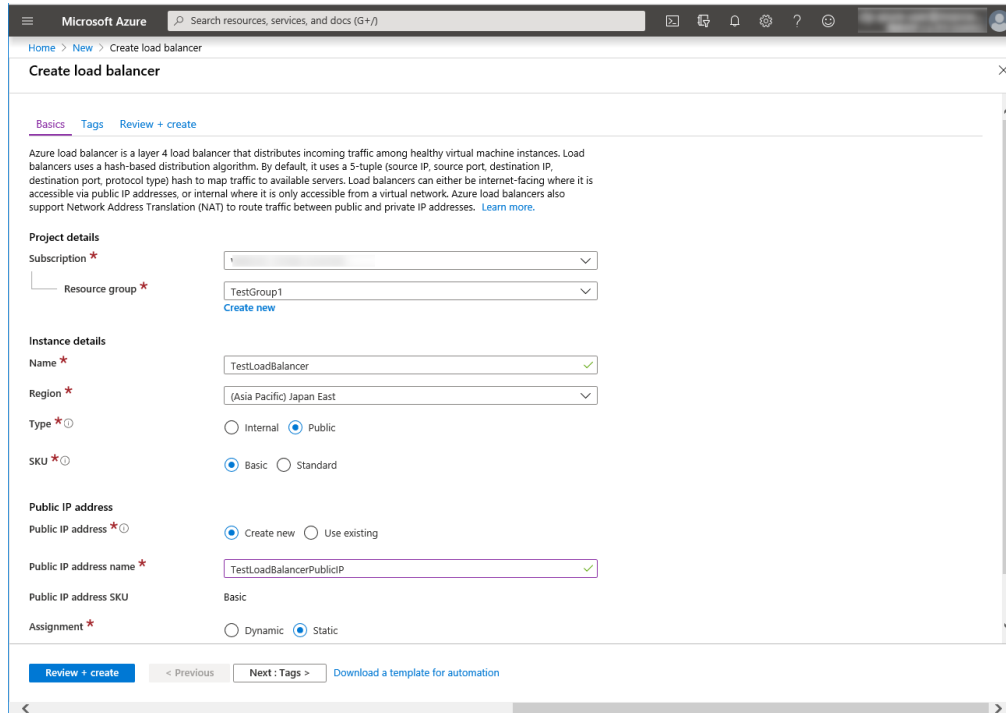
For details, see the following websites:

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

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

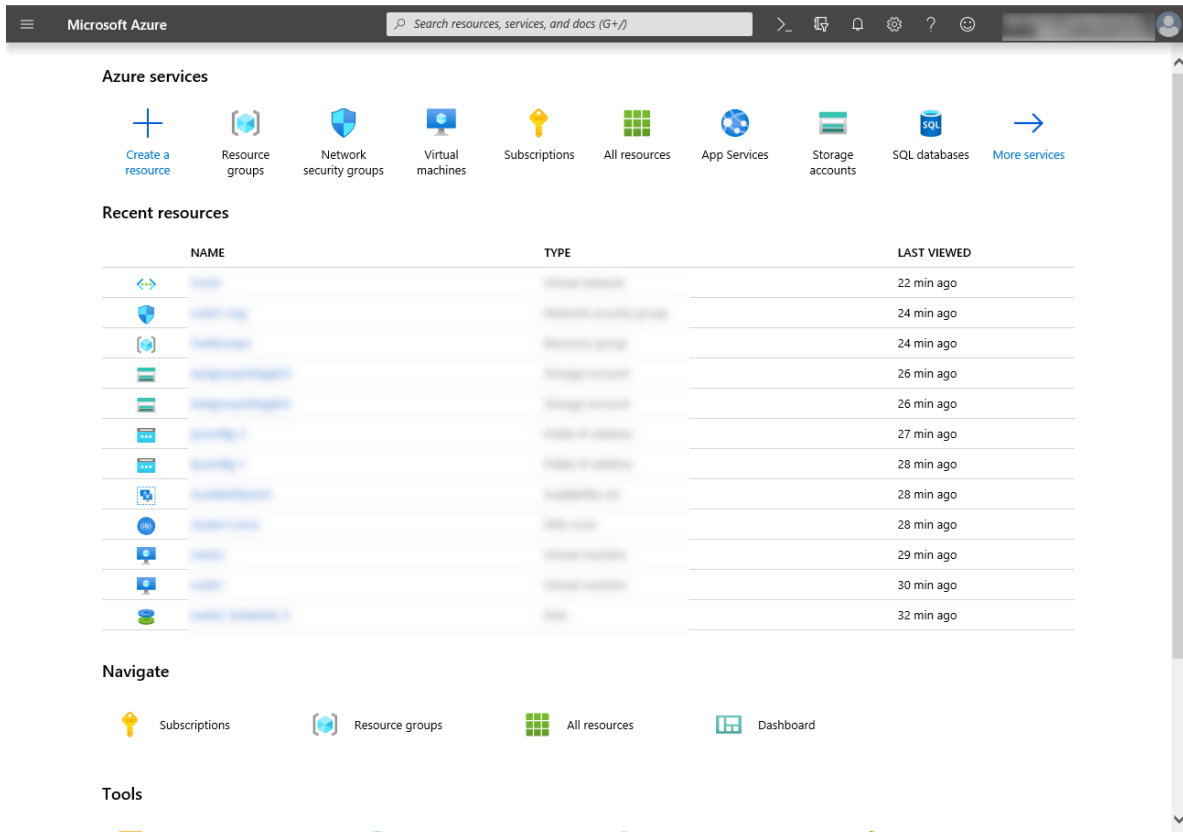


2. Select **Networking** and then **Load Balancer**.
3. The **Create load balancer** blade is displayed. Specify **Name**. Select **Public** for **Type** and **Basic** for **SKU**, respectively.
4. Specify **Create new**, **Public IP address Name** and **Assignment** for **Public IP address**.
5. Specify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



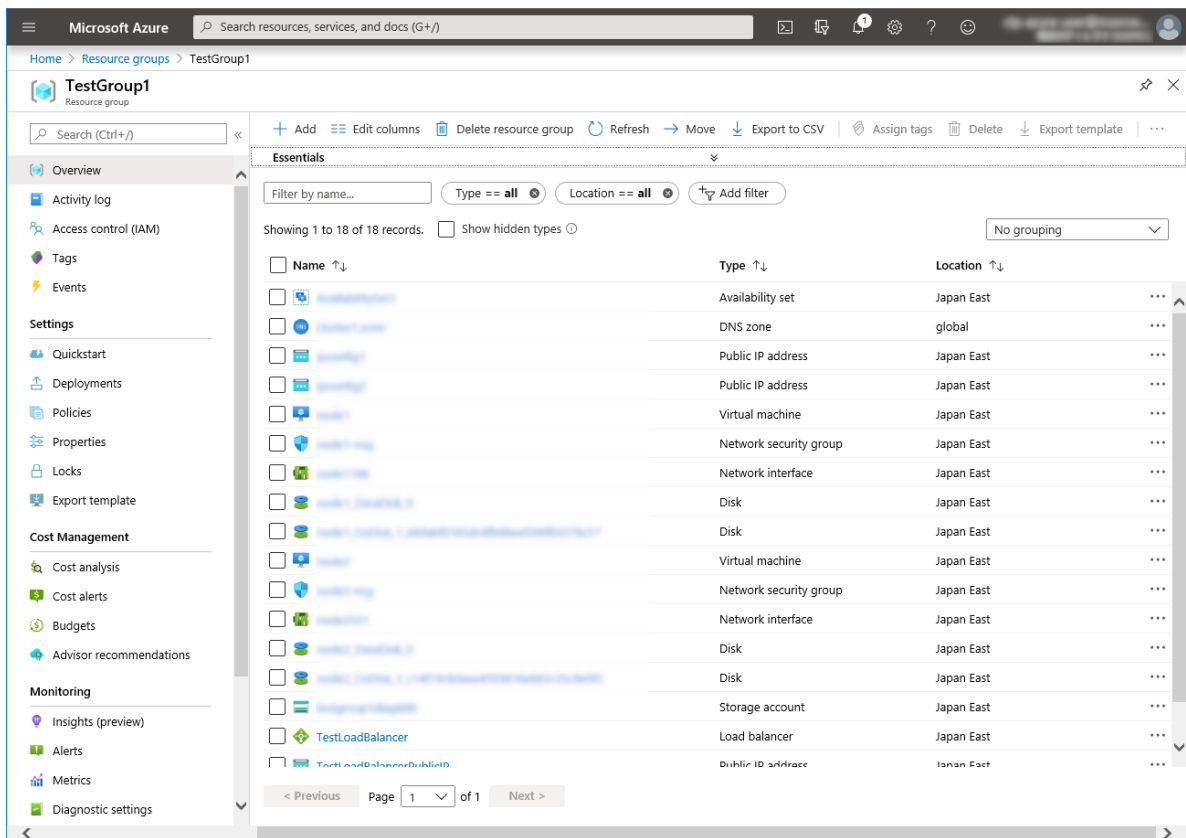
7. Configuring a load balancer (configuring a backend pool)

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

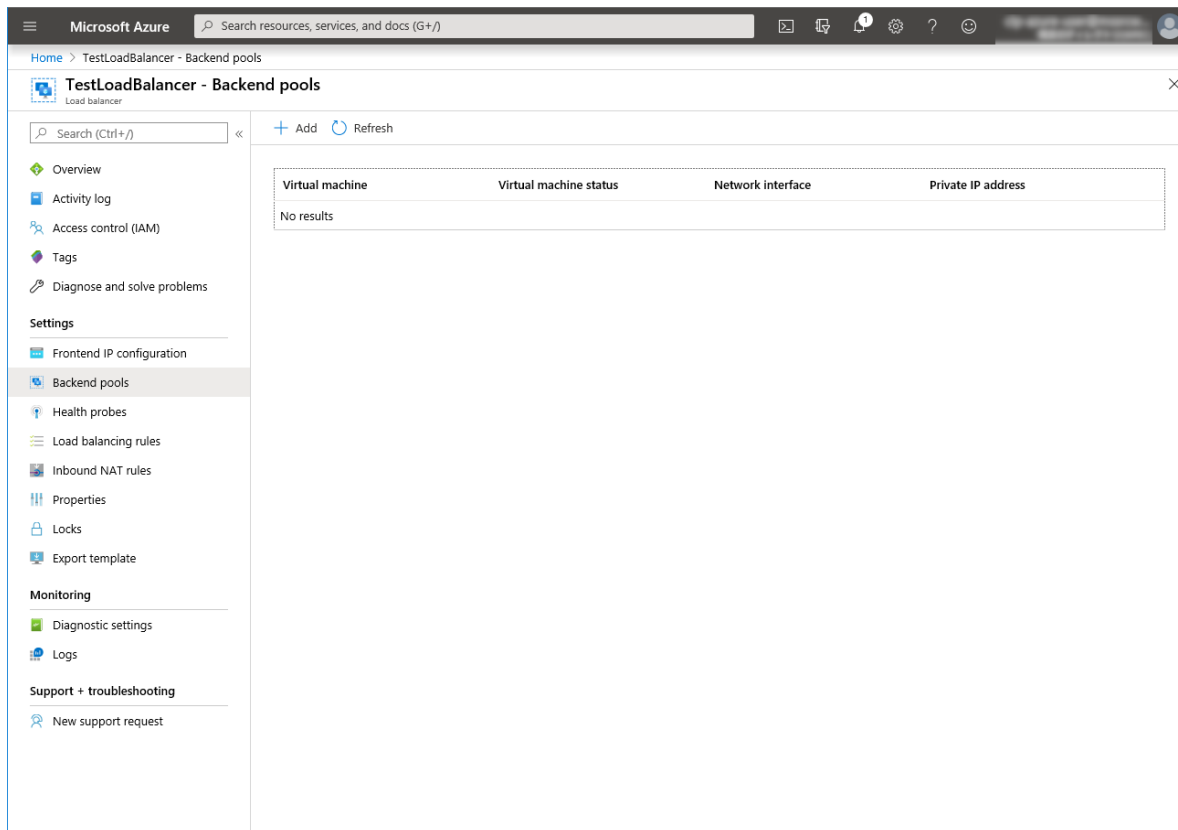


EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2

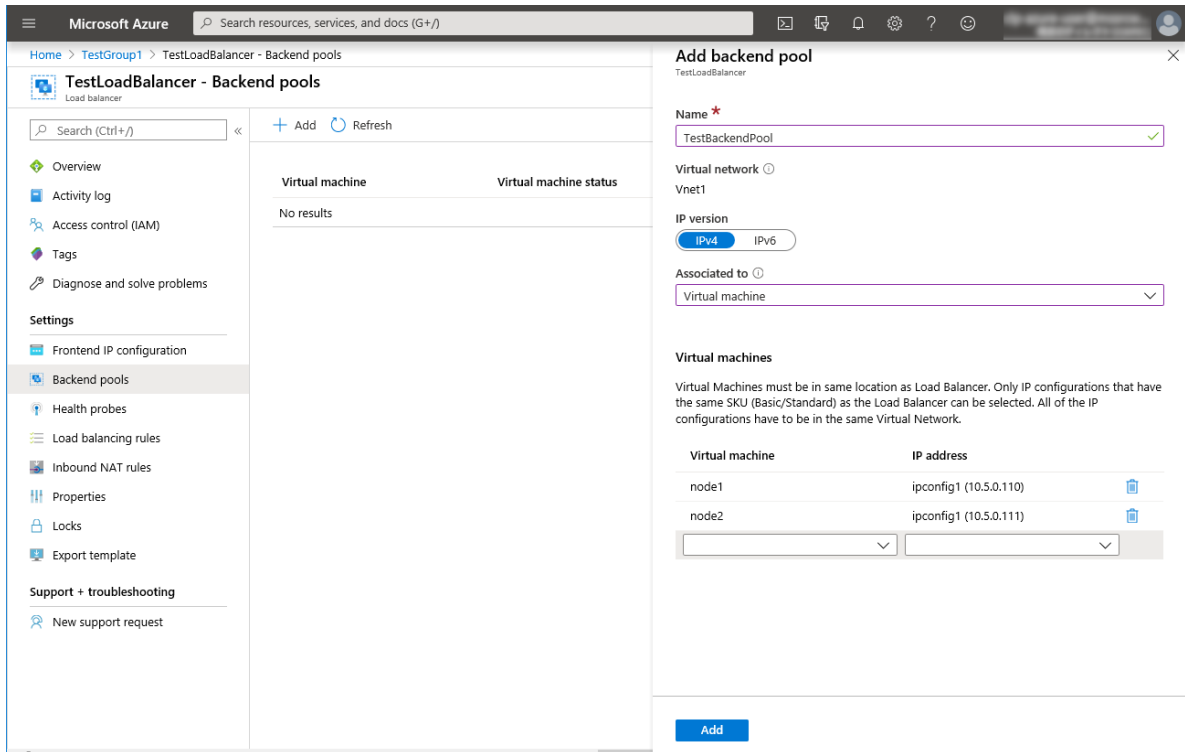
2. Select the resource group to which the created load balancer belongs from the resource group list.
3. The summary of the selected resource group is displayed. Select the created load balancer from the item list.



4. Select **Backend pools**.
5. Click **Add**.

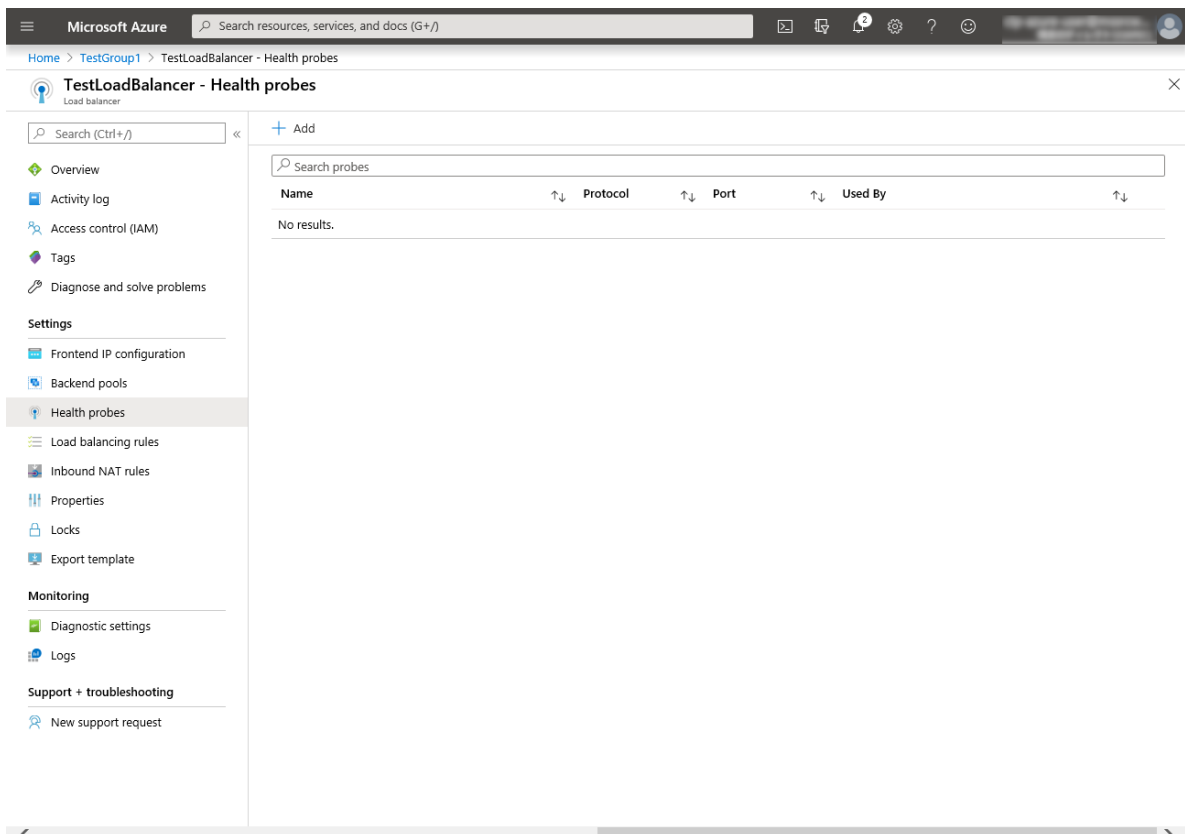


6. **Add backend pool** is displayed. Specify **Name**.
7. Select **Virtual machine** for **Associated to**.
8. Specify **Virtual machine** and **IP address** for the virtual machine you want to associate. Repeat this procedure for the rest of such virtual machines.
9. Then click **Add**.

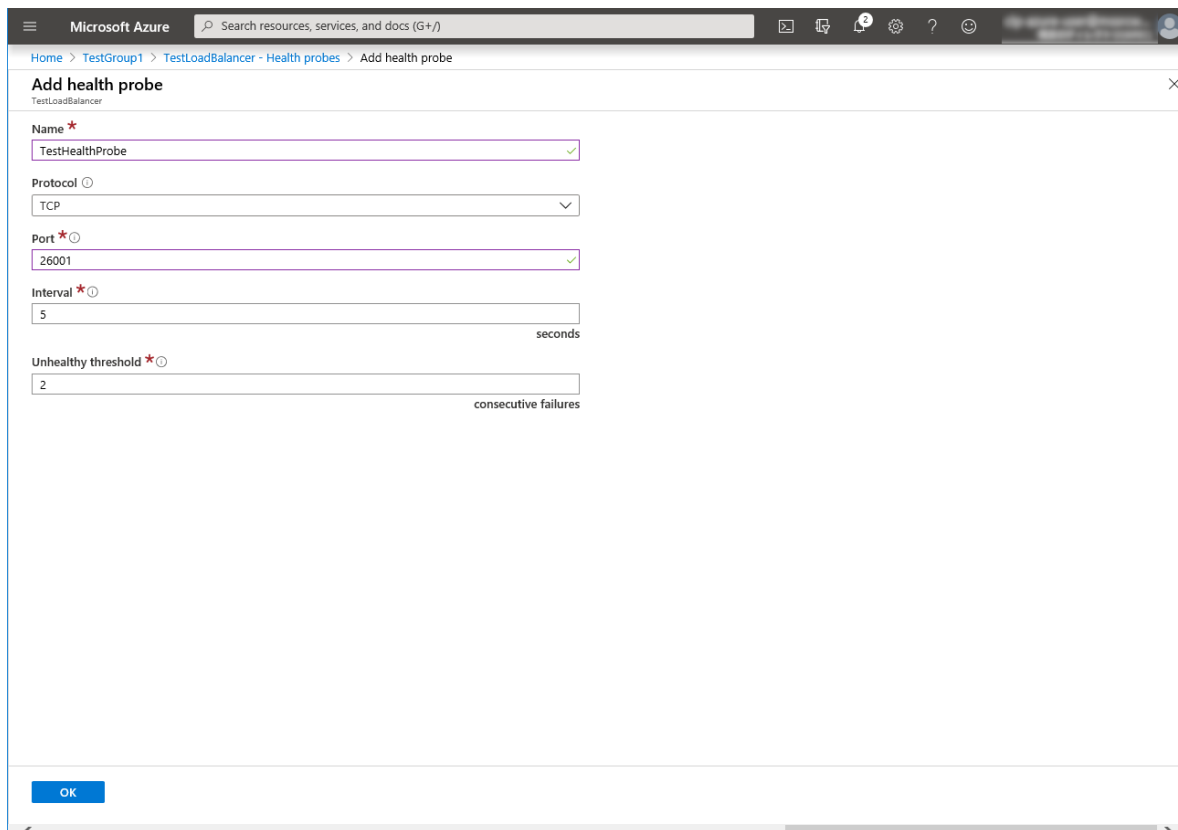


8. Configuring a load balancer (configuring a health probe)

1. Select Health probes.



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

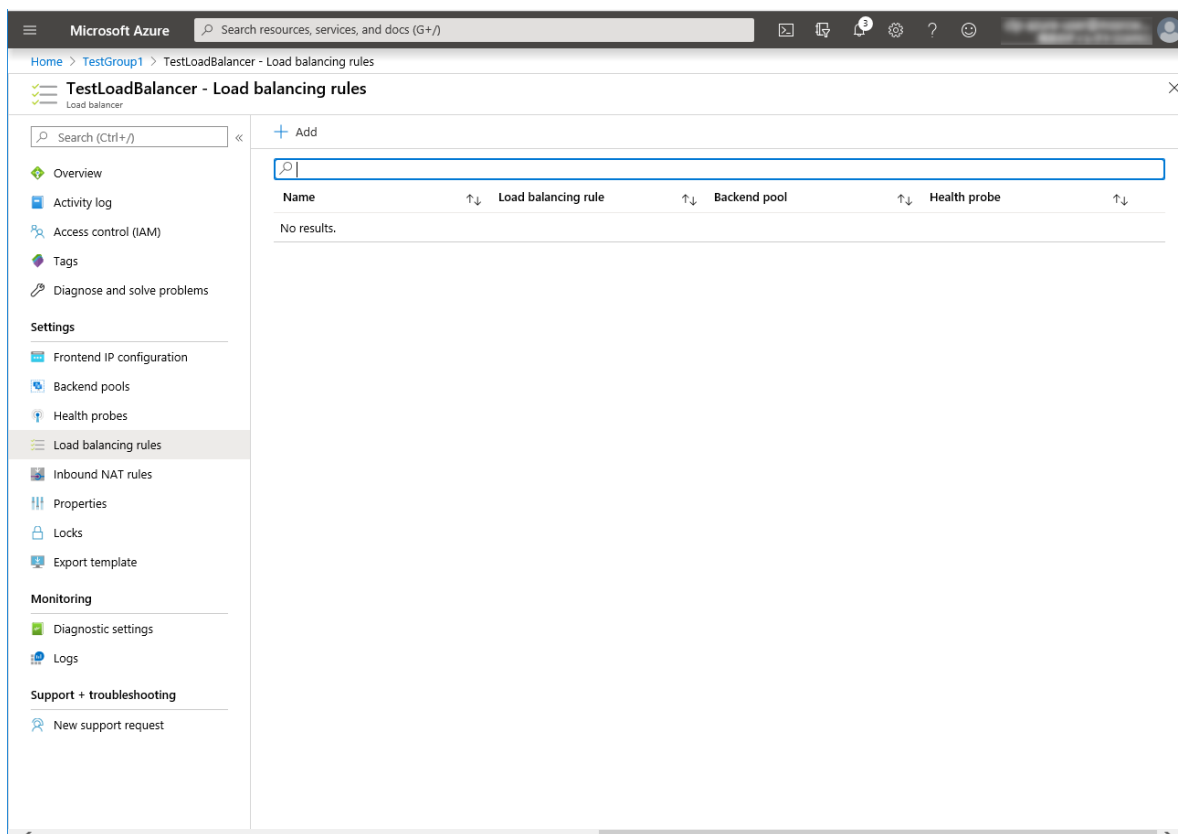


The screenshot shows the 'Add health probe' dialog box in the Microsoft Azure portal. The dialog is titled 'Add health probe' and is associated with 'TestLoadBalancer'. It contains the following fields:

- Name ***: A text input field containing 'TestHealthProbe' with a checkmark icon on the right.
- Protocol**: A dropdown menu showing 'TCP'.
- Port ***: A text input field containing '26001' with a checkmark icon on the right.
- Interval ***: A text input field containing '5', with 'seconds' written below it.
- Unhealthy threshold ***: A text input field containing '2', with 'consecutive failures' written below it.

At the bottom of the dialog, there is a blue 'OK' button.

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' dialog box in the Microsoft Azure portal. The dialog is titled 'Add load balancing rule' and is part of the 'TestLoadBalancer' resource. The fields are as follows:

- Name ***: TestLoadBalancingRule
- IP Version ***: IPv4 (selected), IPv6
- Frontend IP address ***: 52.185.154.20 (LoadBalancerFrontEnd)
- Protocol**: TCP (selected), UDP
- Port ***: 80
- Backend port ***: 8080
- Backend pool**: TestBackendPool
- Health probe**: TestHealthProbe (TCP:26001)
- Session persistence**: None
- Idle timeout (minutes)**: 4
- Floating IP (direct server return)**: Disabled (selected), Enabled

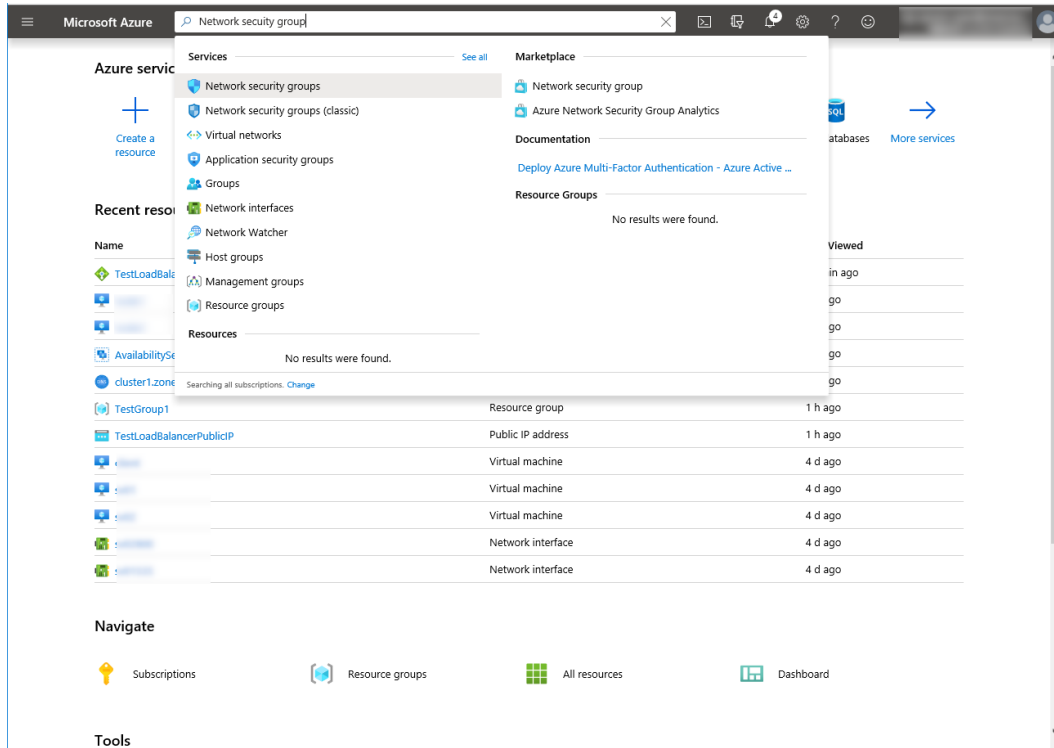
An 'OK' button is located at the bottom left of the dialog.

10. Setting the inbound security rules

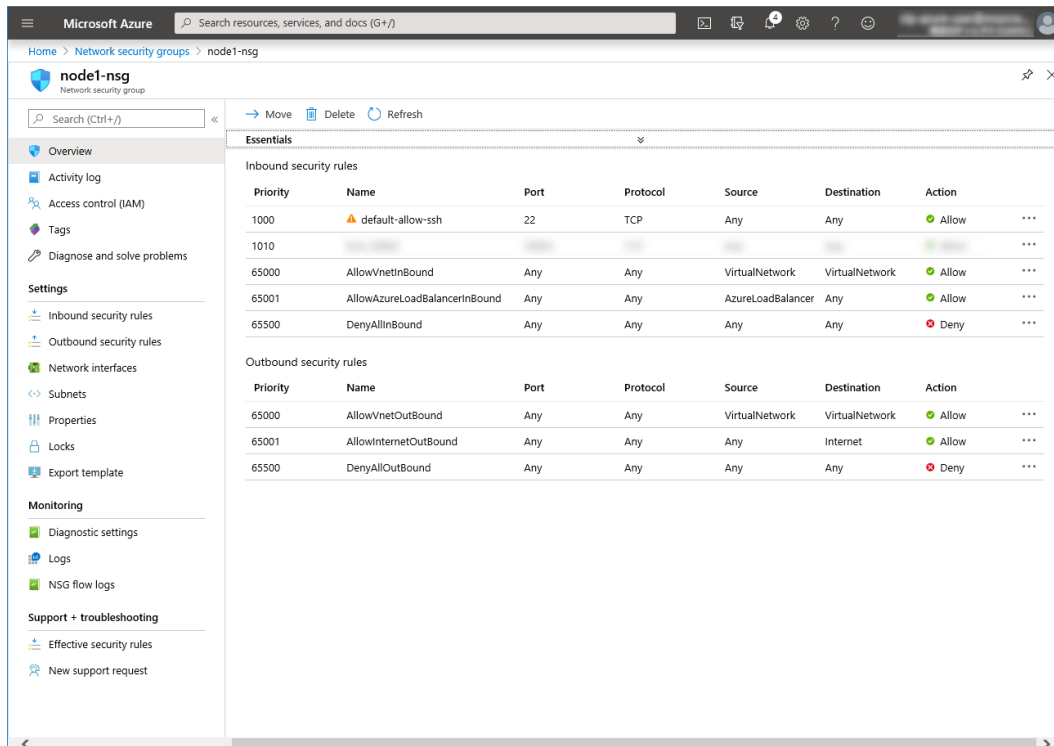
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and set the inbound security rules following the steps below.

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

EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2

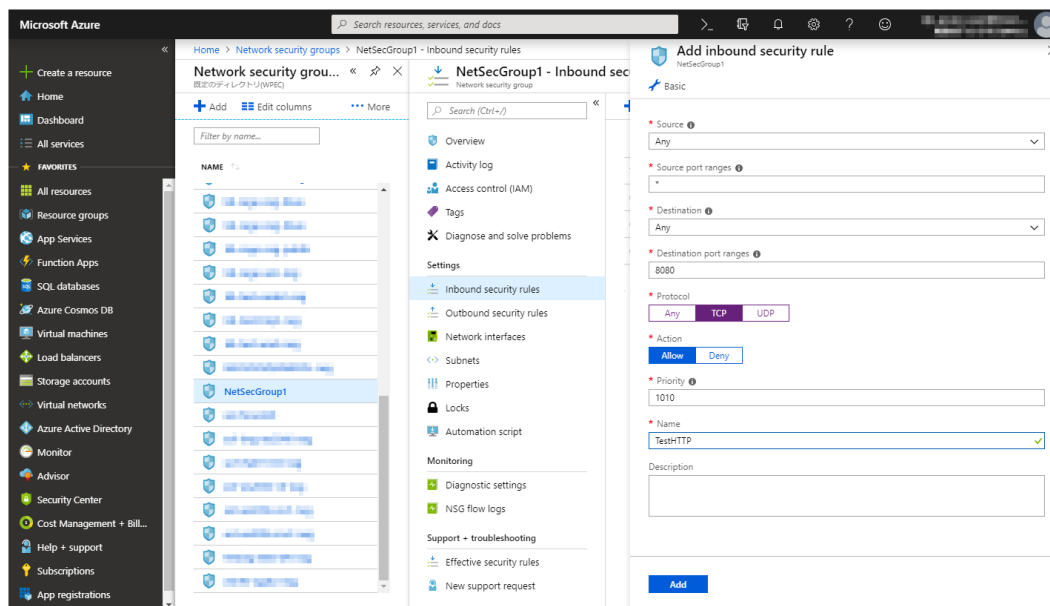


3. From the network security group list, select node1-nsg for node1 or node2-nsg for node2.
4. The summary is displayed.



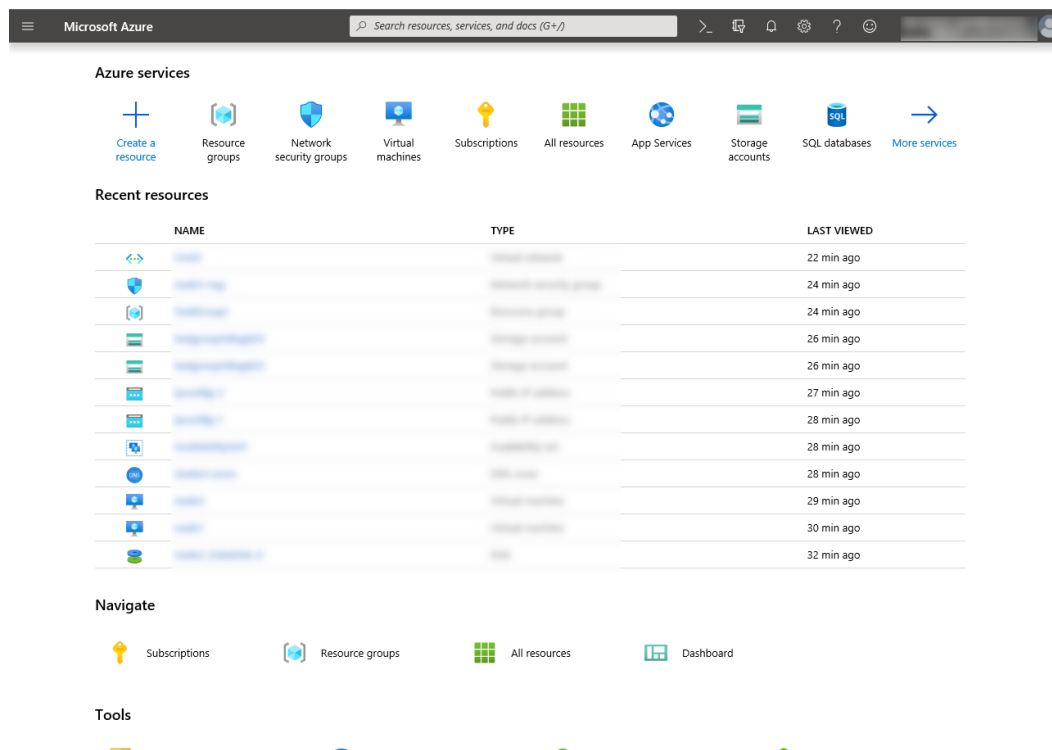
5. Select **Inbound security rules**.
6. Click **Add**.

7. The **Add inbound security rule** blade is displayed. Specify **Name**.
8. Specify **Destination port range** and **Protocol**, and click **Add**.



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.

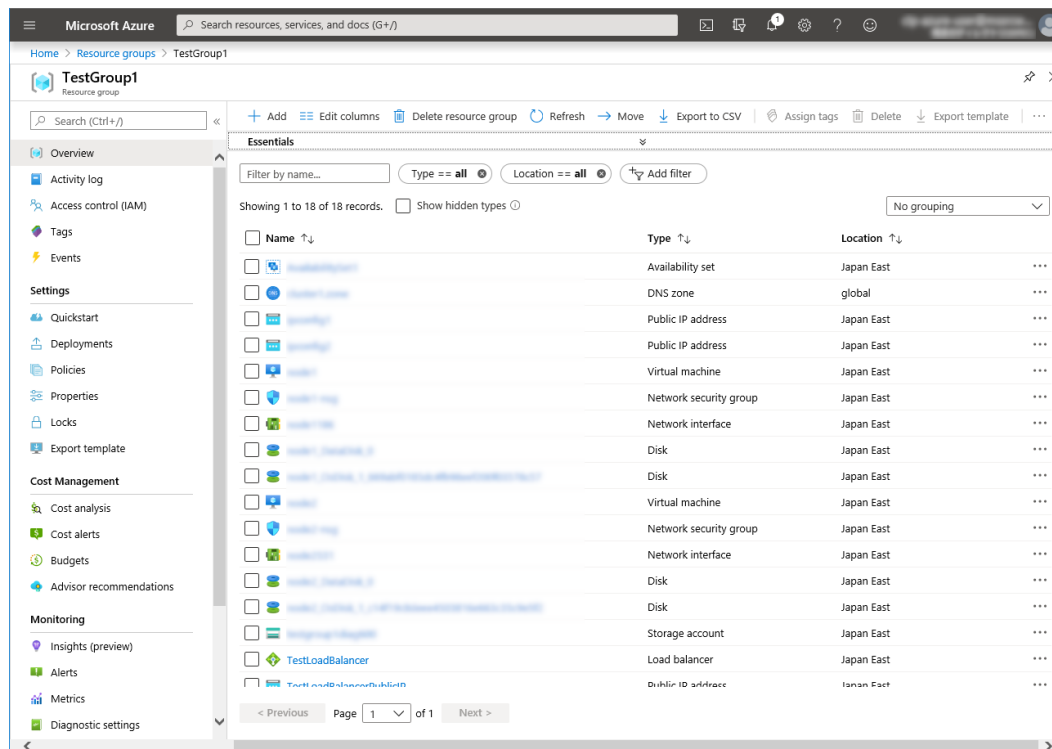
1. Select the **Resource groups** icon on the upper part of the window.



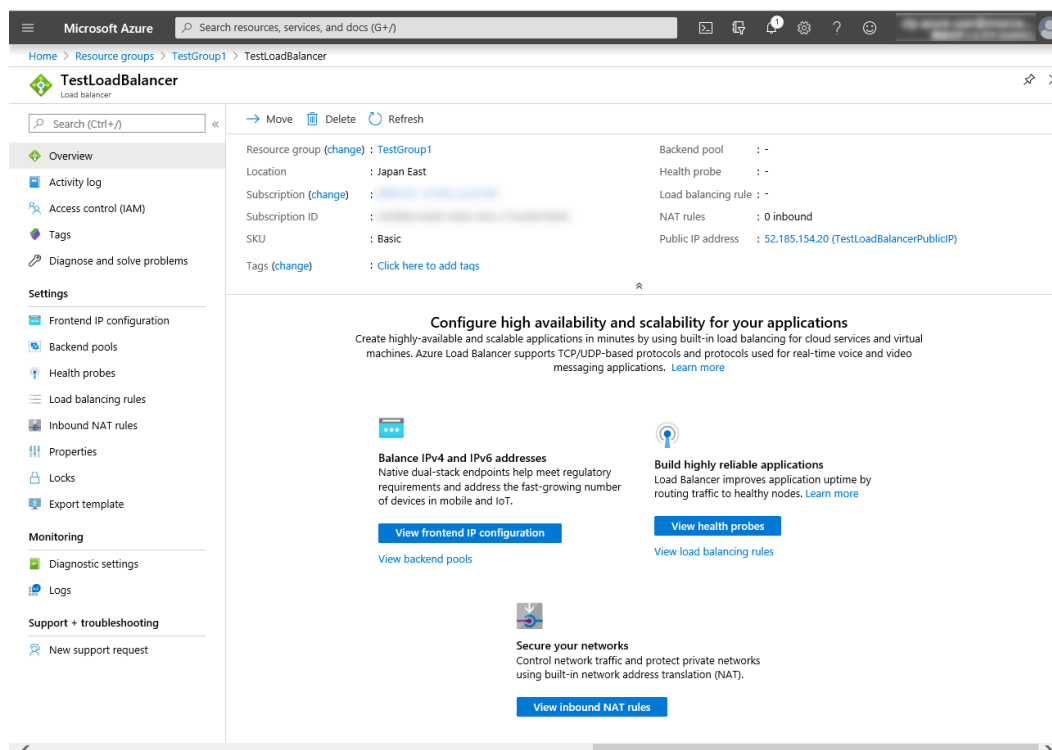
2. Select the resource group to which the created load balancer belongs from the resource group list.

EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2

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 root file system, checking the firewall setting, synchronizing the server time, and checking the SELinux setting.

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 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)

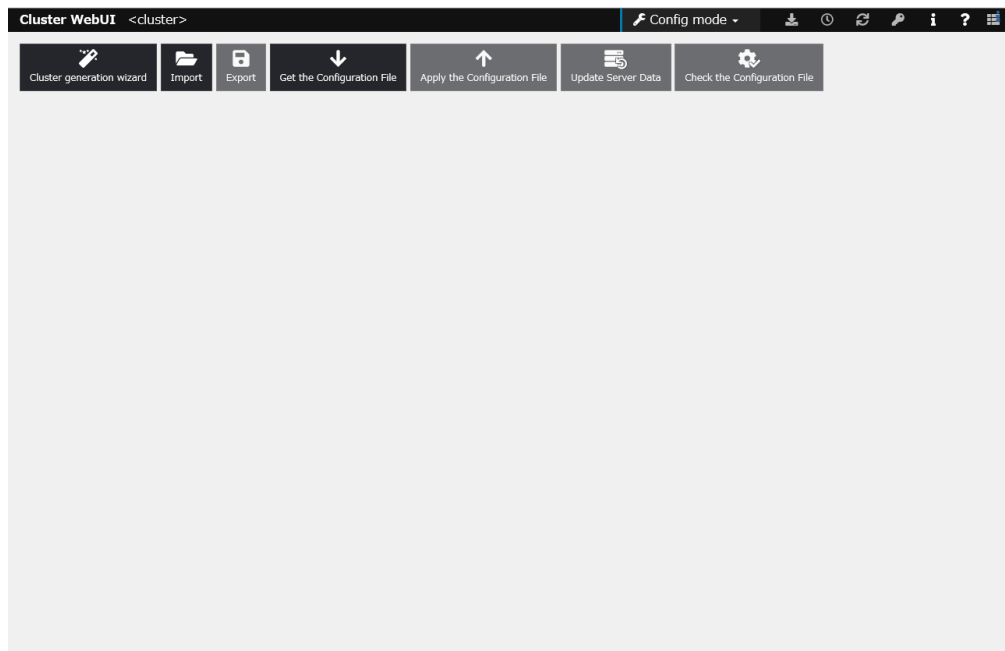
For the settings of other resources and monitor resources, see the Installation and Configuration Guide and the Reference Guide.

1) Creating a cluster

Start the Cluster generation wizard to create a cluster.

- Creating a cluster

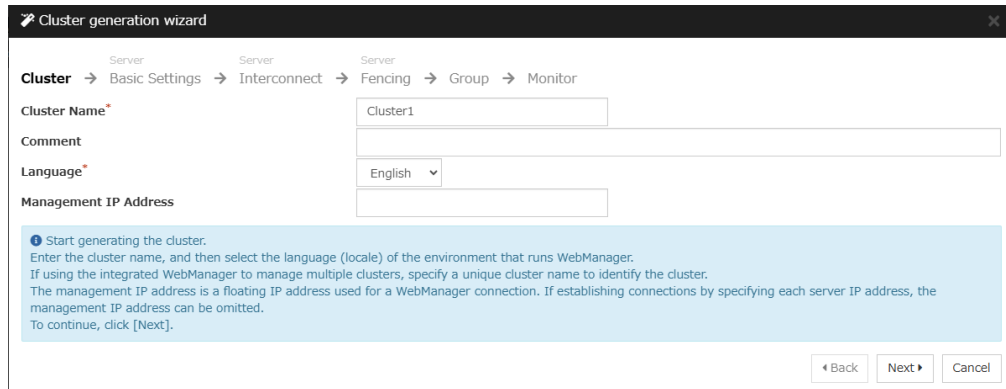
1. Access Cluster WebUI, and click **Cluster generation wizard**.



2. **Cluster of Cluster generation wizard** is displayed.

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

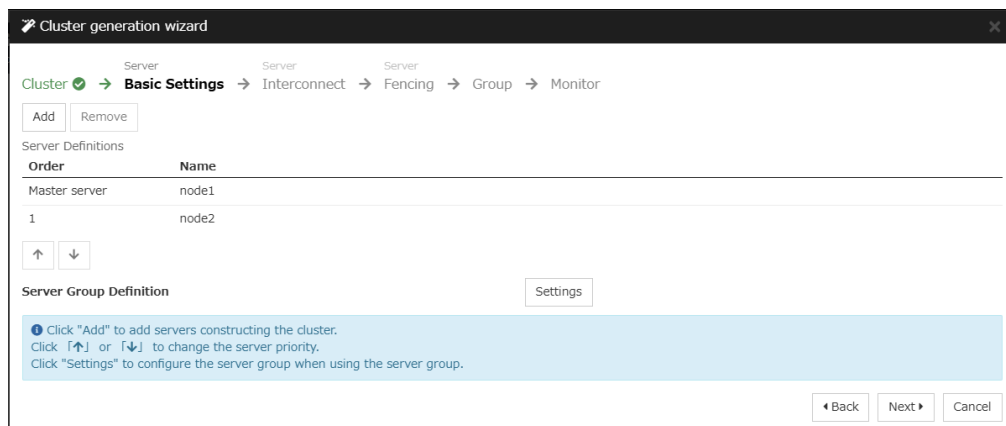
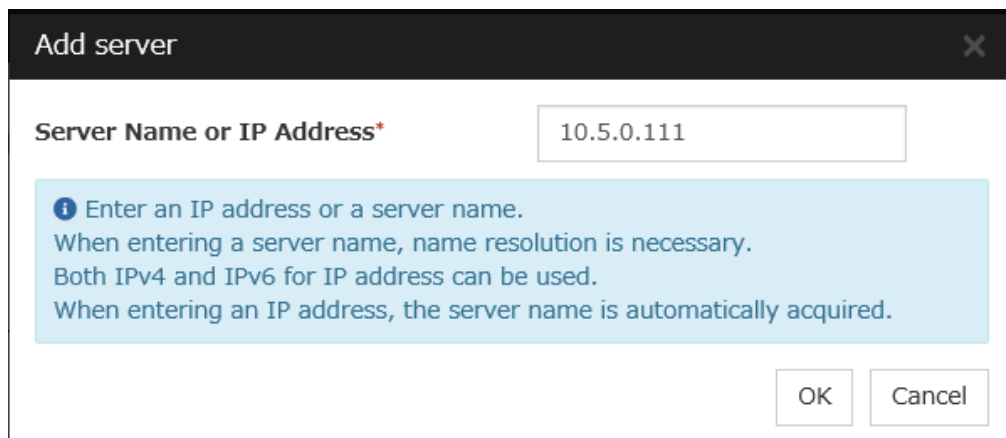
Select an appropriate language in **Language**. Click **Next**.



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

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

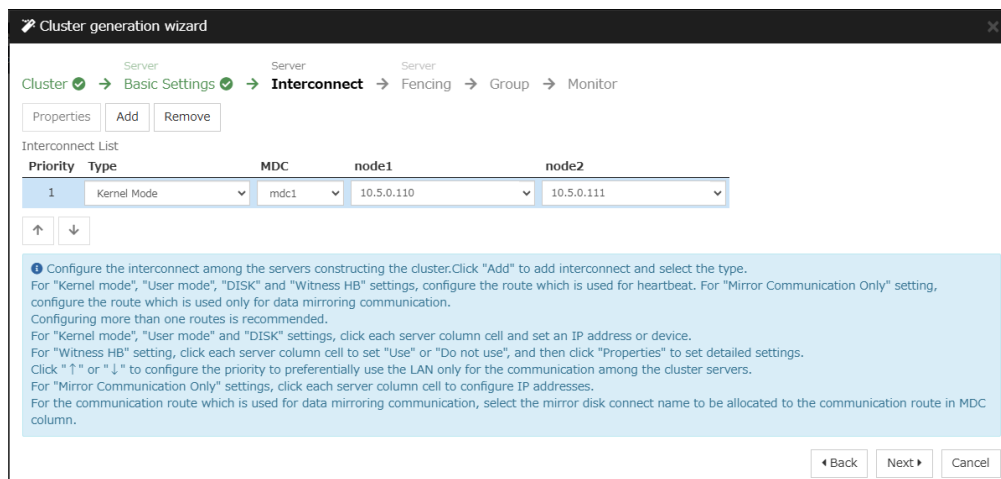
Click **Add** to add the remaining instances (by specifying the private IP address of each instance). Click **Next**.



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**.

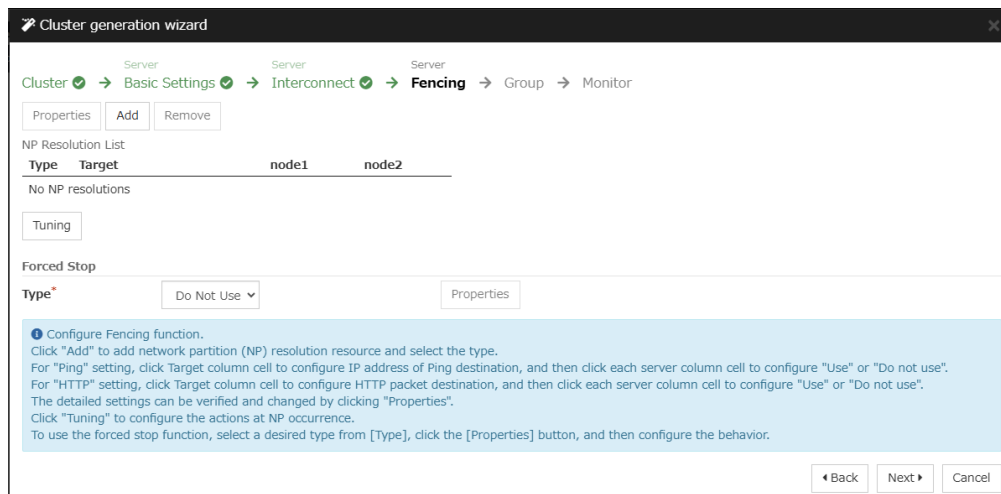


5. The **Fencing** window is displayed.

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**.



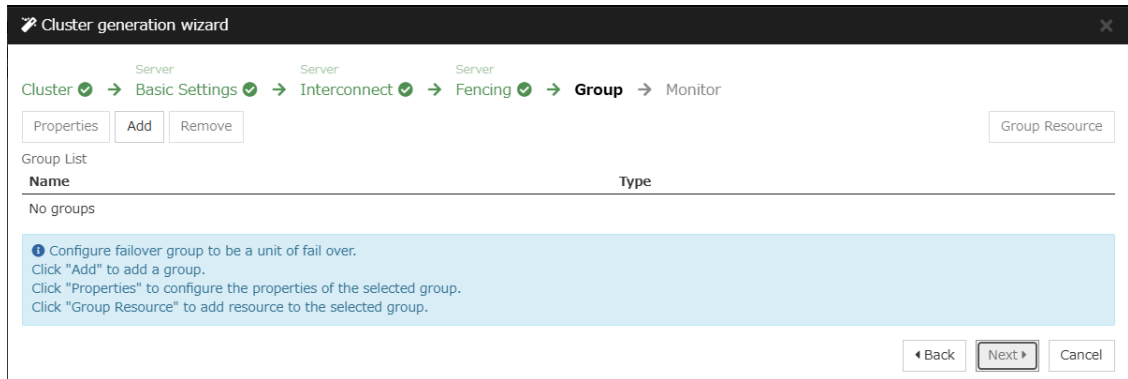
2) **Adding a group resource**

- Defining a group

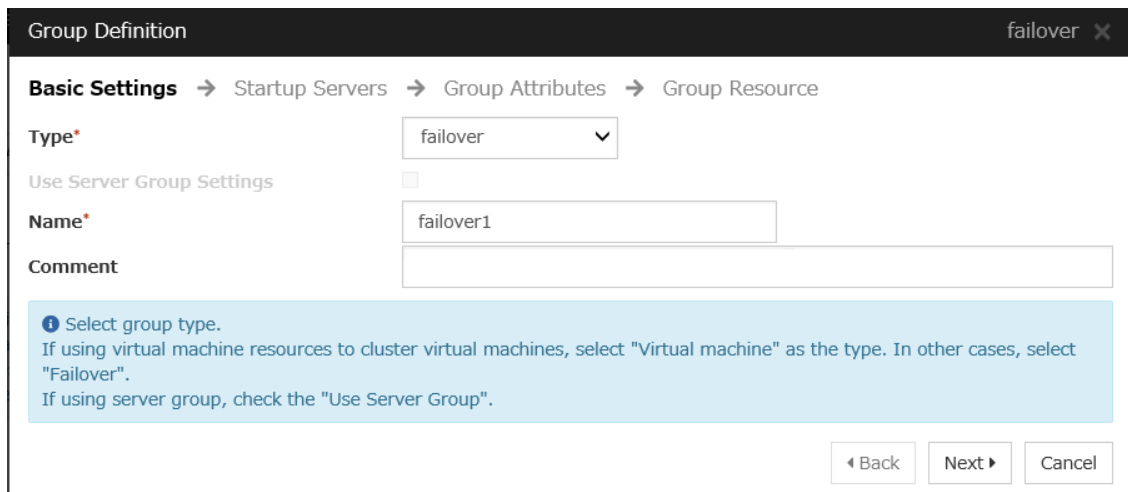
Create a failover group.

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

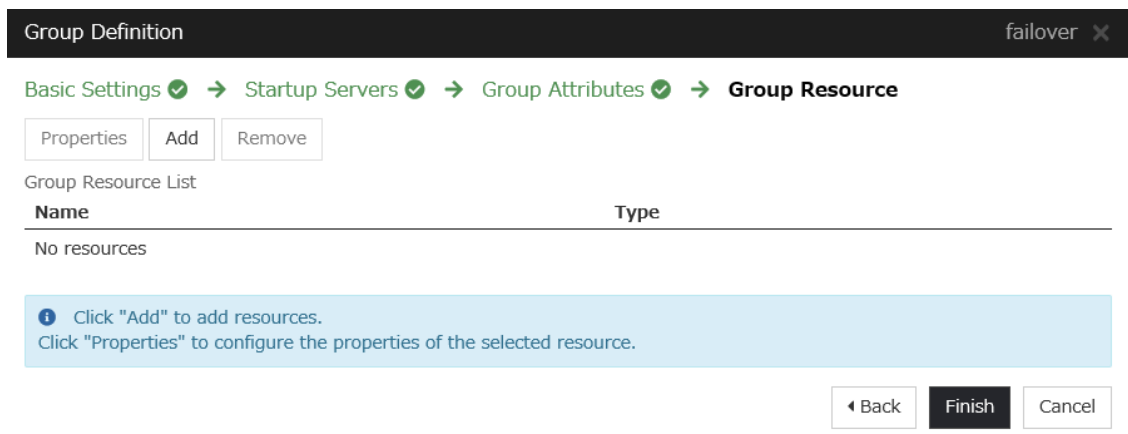
Click **Add**.



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



- The **Startup Servers** window is displayed.
Click **Next** without specifying anything.
- The **Group Attributes** window is displayed.
Click **Next** without specifying anything.
- 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.
Enter the device name of the partition created in "5. Configuring virtual machines" in **Data Partition Device Name** and **Cluster Partition Device Name**. Specify **Mount Point** and **File System**. Click **Finish** to finish setting.

Resource Definition of Group | failover1 md X

Info ✓ → Dependency ✓ → Recovery Operation ✓ → Details

Common node1 node2

Mirror Partition Device Name* /dev/NMP1

Mount Point* /mnt/md

Data Partition Device Name* /dev/sdc2

Cluster Partition Device Name* /dev/sdc1

File System* ext4

Mirror Disk Connect Select

Tuning

Back Finish Cancel

- 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 "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 (Azure probe port resource) from the **Type** box and enter the group name (azurepp1) in the **Name** box. Click **Next**.

Resource Definition of Group | failover1 azurepp ✕

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. For **Probeport**, enter the value specified for **Port** when configuring a load balancer (configuring health probe).

Resource Definition of Group | failover1 azurepp ✕

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

Probeport*

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 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

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* 0 time

Wait Time to Start Monitoring* 0 sec

Monitor Timing

Always

Active

Target Resource Browse

Nice Value 0

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.

```
#!/bin/sh
```

```
<EXPRESSCLUSTER_installation_path>/bin/clpazure_port_checker -h  
↪management.core.windows.net -p 443  
exit $?
```

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

Monitor Type
 Synchronous
 Asynchronous

Wait a period of time for Application/Script monitor to start sec

Log Output Path

Rotate Log

Rotation Size byte

Normal Return Value*

Wait for activation monitoring to stop before stopping the cluster

- 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 for a resource named 'genw'. 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 this are three sections of settings, each with a checkbox and a numeric input field followed by the word 'time':
1. 'Recovery Script Execution Count' with input '0'.
2. 'Execute Script before Reactivation' (checkbox) and 'Maximum Reactivation Count' with input '0'.
3. 'Execute Script before Failover' (checkbox), 'Execute migration before Failover' (checkbox), and 'Maximum Failover Count' with input '0'.
At the bottom, there is a checkbox for 'Execute Script before Final Action' and a 'Final Action' dropdown set to 'No operation'. A 'Script Settings' button is located to the right. At the bottom right are three buttons: 'Back', 'Finish' (highlighted in black), and '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 for a resource named 'ipw'. The breadcrumb trail is 'Info' → 'Monitor(common)' → 'Monitor(special)' → 'Recovery Action'. The 'Type' dropdown is set to 'IP monitor'. The 'Name' text box contains 'ipw1'. The 'Comment' text box is empty. There is a 'Get Licence Info' button. A blue information banner at the bottom states: 'Select the type of monitor resource and enter its name.' At the bottom right are three buttons: 'Back', 'Next' (highlighted in black), and 'Cancel'.

3. The **Monitor (common)** window is displayed.

Confirm that **Monitor Timing** is **Always**.

Monitor Resource Definition ipw X

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

Interval* sec

Timeout* sec

Collect the dump file of the monitor process at timeout occurrence

Do Not Retry at Timeout Occurrence

Do Not Execute Recovery Action at Timeout Occurrence

Retry Count* time

Wait Time to Start Monitoring* sec

Monitor Timing

Always

Active

Target Resource

Nice Value

Choose servers that execute monitoring

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

Failure Detection Server

All servers

Select

Servers that can run the Group

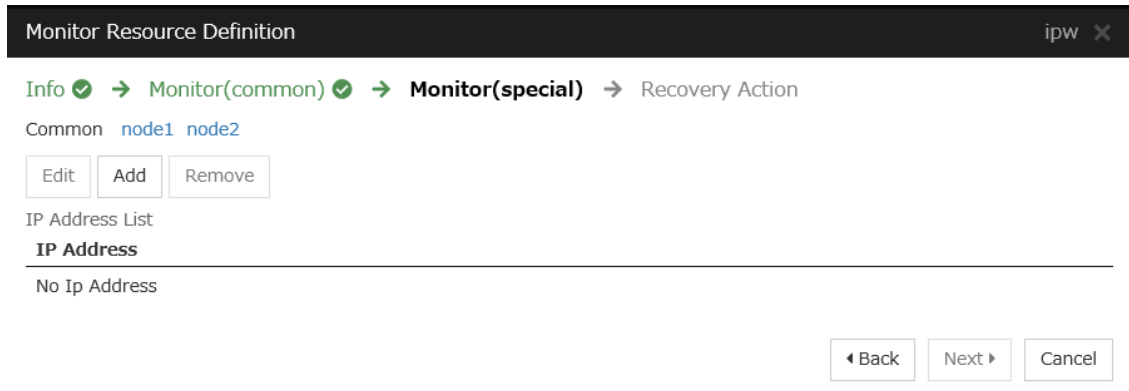
Name
node1

Available Servers

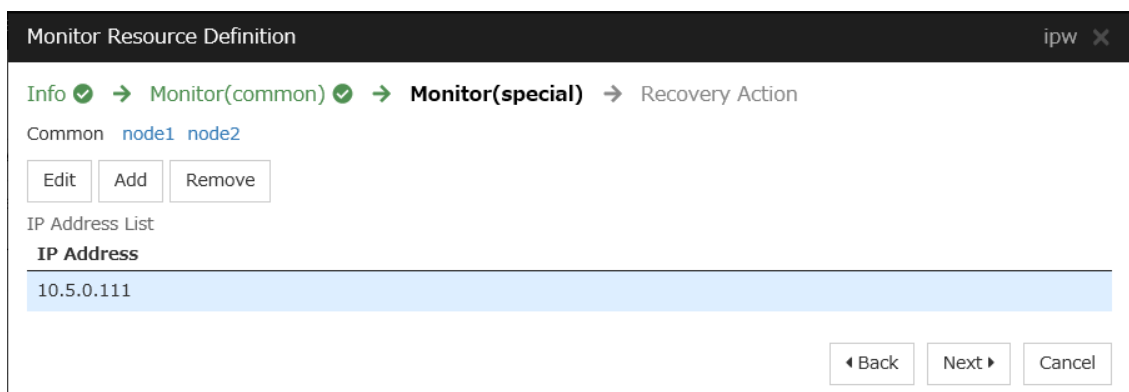
Name
node2

Click **Next**.

- 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 3. Click **Next**.



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**.

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 **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**.

Monitor Resource Definition mtw X

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

Interval* 30 sec

Timeout* 30 sec

Collect the dump file of the monitor process at timeout occurrence

Do Not Retry at Timeout Occurrence

Do Not Execute Recovery Action at Timeout Occurrence

Retry Count* 0 time

Wait Time to Start Monitoring* 0 sec

Monitor Timing

Always

Active

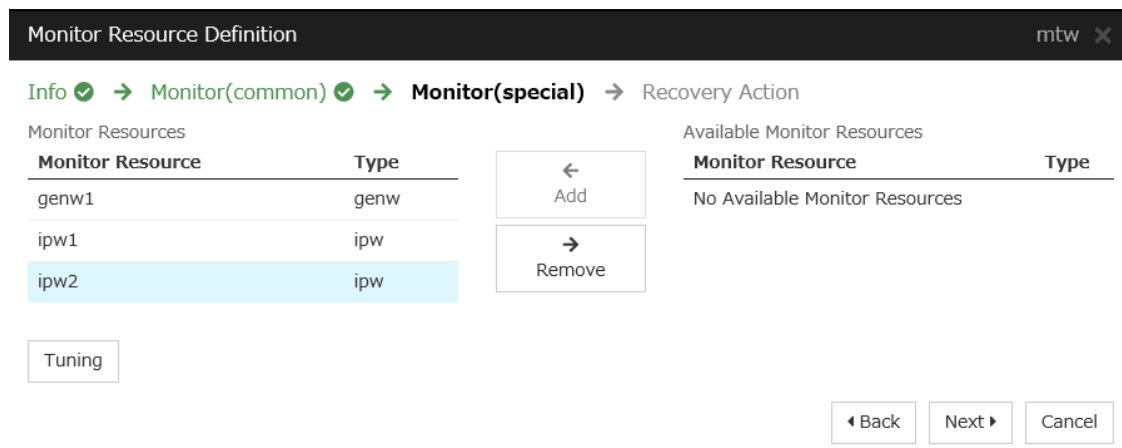
Target Resource Browse

Nice Value 0

Choose servers that execute monitoring

◀ Back Next ▶ Cancel

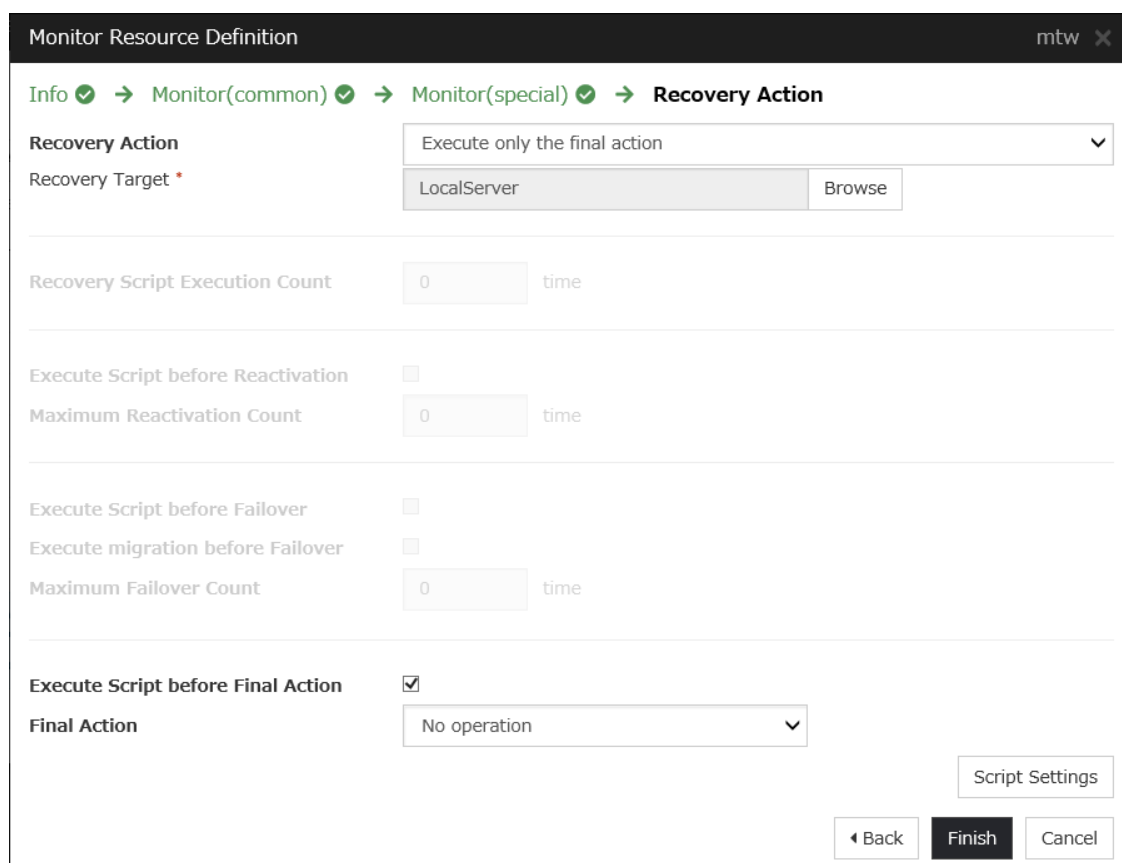
4. The **Monitor (special)** window is displayed.
From **Available Monitor Resources**, select the custom monitor resource (genw1) for checking communication with Service Management API and two IP monitor resources (ipw1 and ipw2) that are set to both servers. Then, click **Add** to add them to **Monitor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



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.



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

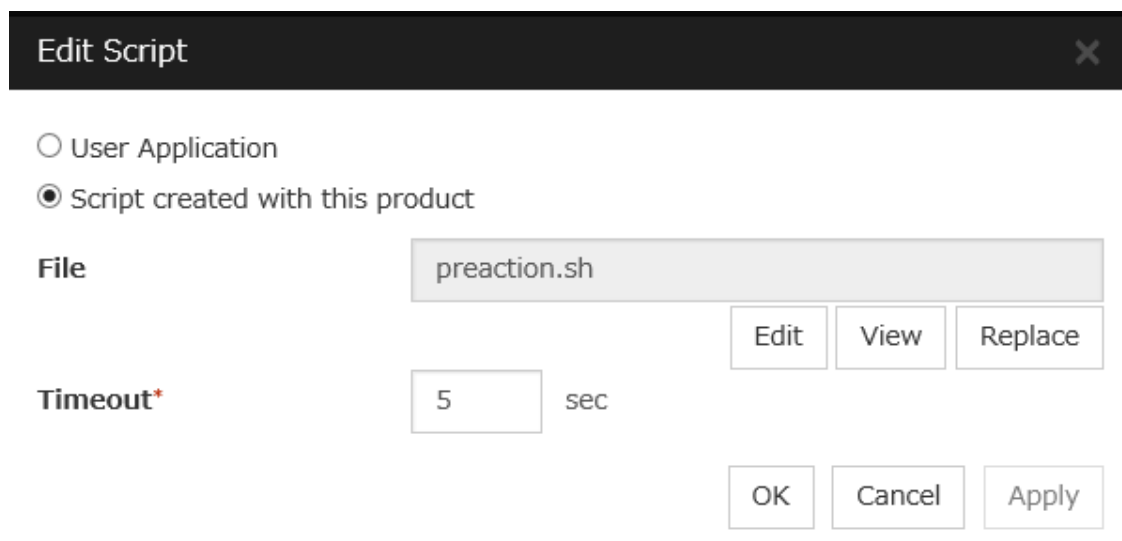
Set the public IP address that you wrote down in "10) Setting the inbound security rules" to the following:

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

```
#!/bin/sh
<EXPRESSCLUSTER_installation_path>/bin/clpazure_port_checker -h 127.0.
↪0.1 -p <Backend_port_of_the_load_balancer_of_Load_balancing_rule>
if [ $? -ne 0 ]
then
    clpdown
    exit 0
fi
<EXPRESSCLUSTER_installation_path>/bin/clpazure_port_checker -h
↪<Frontend_IP (public_IP_address)_of_the_load_balancer> -p <Port_of_
↪the_load_balancer_of_Load_balancing_rule>
if [ $? -ne 0 ]
then
    clpdown
    exit 0
fi
```

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**.



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.

Server Sync Wait Time*	<input type="text" value="5"/>	min
Heartbeat		
Interval*	<input type="text" value="3"/>	sec
Timeout*	<input type="text" value="120"/>	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** on the **File** in the config mode of Cluster WebUI.
 If the upload succeeds, the message saying "The application finished successfully."
2. Select the **Operation Mode** on the drop down menu of the toolbar in Cluster WebUI to switch to the operation mode.
3. The procedure depends on the resource used. For details, refer to the following: Installation and Configuration Guide -> How to create a cluster

5.4 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 (node1). In the **Status** tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node1 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 node2. In the **Status** tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node2 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 node1 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 node1 and node2)

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	node1 node2

Continued on next page

Table 6.1 – continued from previous page

Setting item	Setting value
Network IP configuration	10.5.0.110 10.5.0.111
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 node1 and node2)

Setting item	Setting value	
	node1	node2
Virtual machine setting		
– Disk type	Standard HDD	Standard HDD
– User name	testlogin	testlogin
– Password	PassWord_123	PassWord_123
– Resource group	TestGroup1	TestGroup1
– Region	(Asia Pacific) Japan East	(Asia Pacific) Japan East
Network security group setting		
– Name	node1-nsg	node2-nsg
Availability set setting		
– Name	AvailabilitySet1	AvailabilitySet1
– Update domains	5	5
– Fault domains	2	2
Diagnostics storage account setting		
– Name	Automatically generated	Automatically generated

Continued on next page

Table 6.2 – continued from previous page

Setting item	Setting value	
	node1	node2
– Performance	Standard	Standard
– Replication	Locally-redundant storage (LRS)	Locally-redundant storage (LRS)
IP configuration setting		
– IP address	10.5.0.110	10.5.0.111
Disk setting		
– Name	node1_DataDisk_0	node2_DataDisk_0
– Source type	None (empty disk)	None (empty disk)
– Account type	Standard HDD	Standard HDD
– Size	20	20

- EXPRESSCLUSTER settings (cluster properties)

Setting item	Setting value	
	node1	node2
– Cluster Name	Cluster1	Cluster1
– Server Name	node1	node2
– NP Resolution Tab: Type	Ping	Ping
– NP Resolution Tab: Target	10.5.0.5	10.5.0.5
– Timeout Tab: Heartbeat timeout	Use	Use

- EXPRESSCLUSTER settings (failover group)

Resource name	Setting item	Setting value
Mirror disk resource	Name	md

Continued on next page

Table 6.4 – continued from previous page

Resource name	Setting item	Setting value
	Details Tab: Mount Point	/mnt/md
	Details Tab: Data Partition Device Name	/dev/sdc2
	Details Tab: Cluster Partition Device Name	/dev/sdc1
	Details Tab: File System	ext4
	Mirror Tab: Execute the initial mirror construction	On
	Mirror Tab: Execute initial mkfs	On
Azure probe port resource	Name	azurepp1
	Probe port	26001 (Value specified for Port of Health probe)
Exec resource (for DSR)	Name	exec1

- EXPRESSCLUSTER settings (monitor resource)

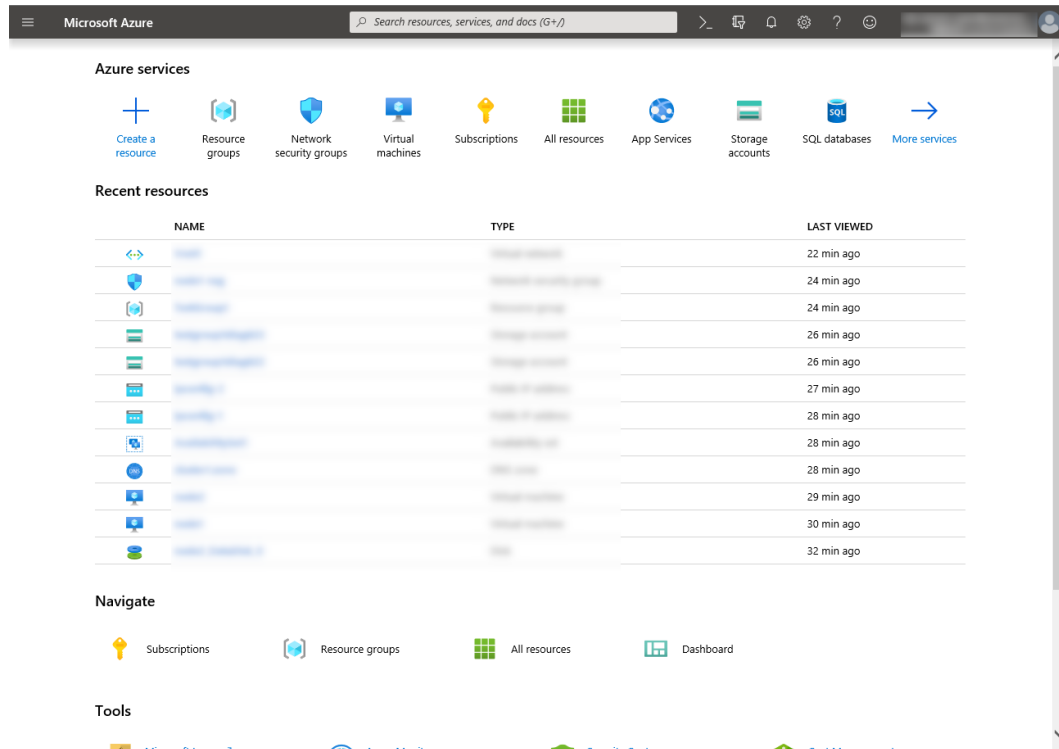
Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	Name	mdw1
Azure probe port monitor resource	Name	azureppw1
	Recovery Target	azurepp1
Azure load balance monitor resource	Name	azurelbw1
	Recovery Target	azurepp1

6.2 Configuring Microsoft Azure

1) Creating a resource group

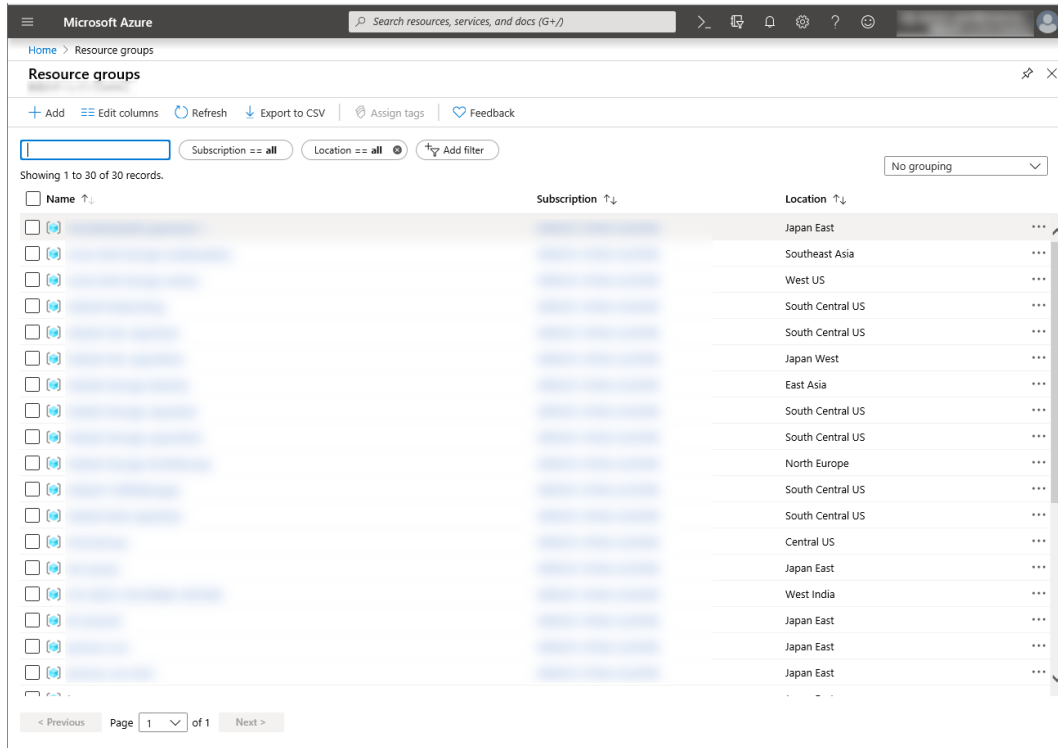
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create a resource group following the steps below.

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

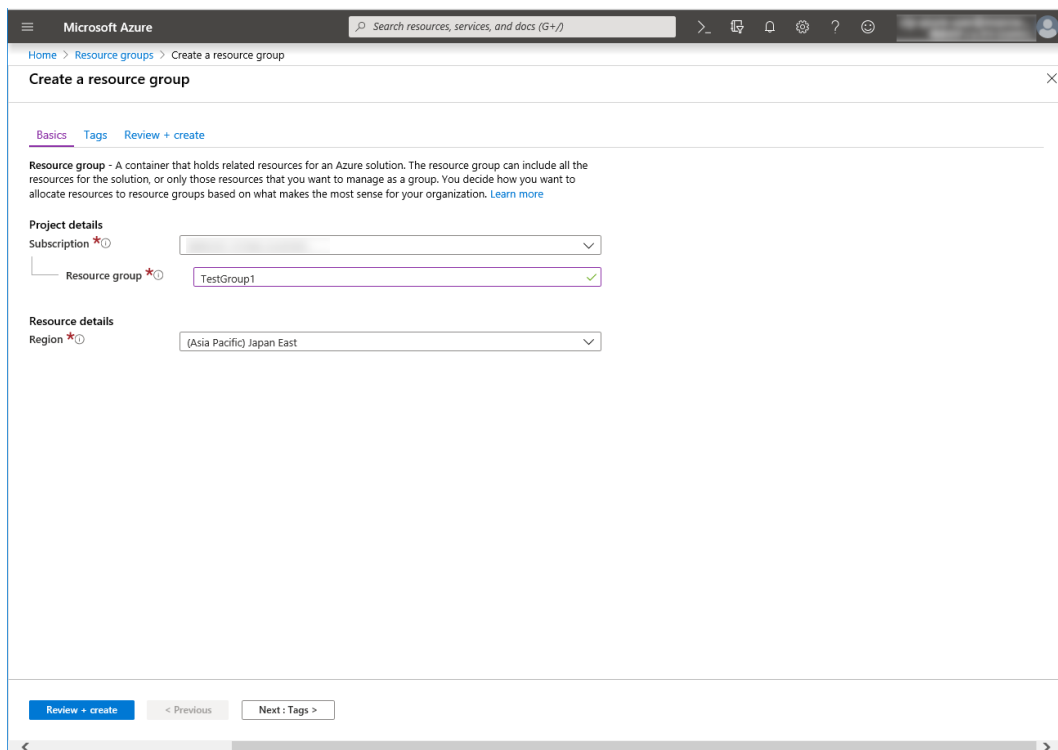


2. Select **+Add** at the upper part of the window.

EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



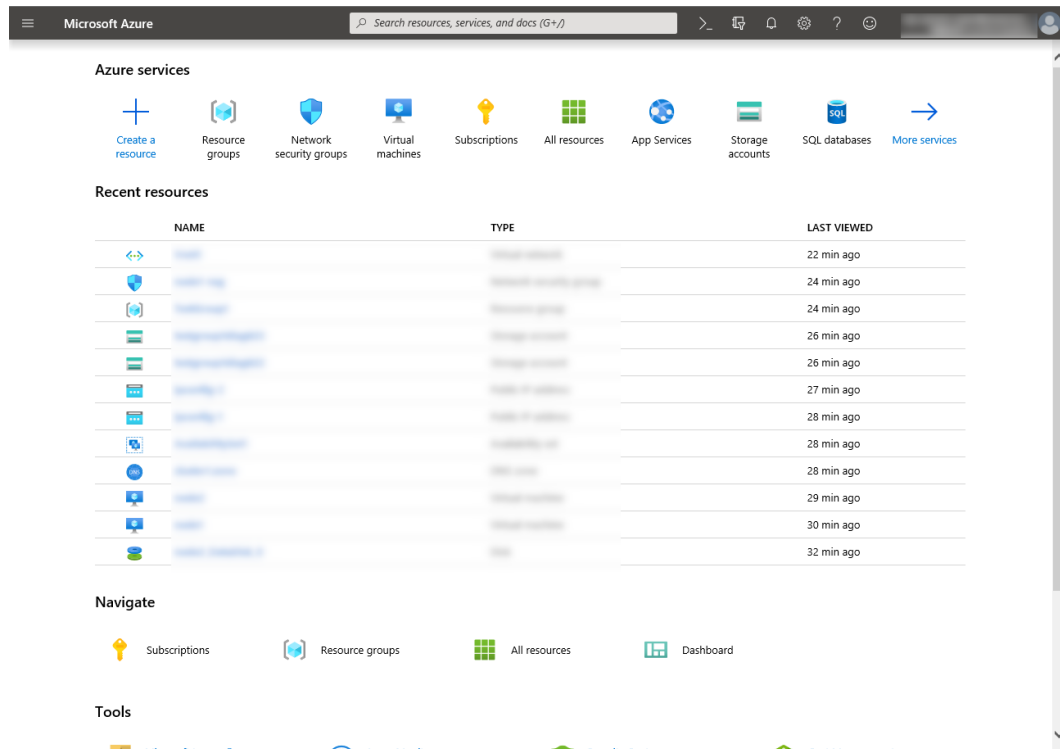
3. Specify **Subscription**, **Resource group**, and **Region**, and click **Review+Create**.



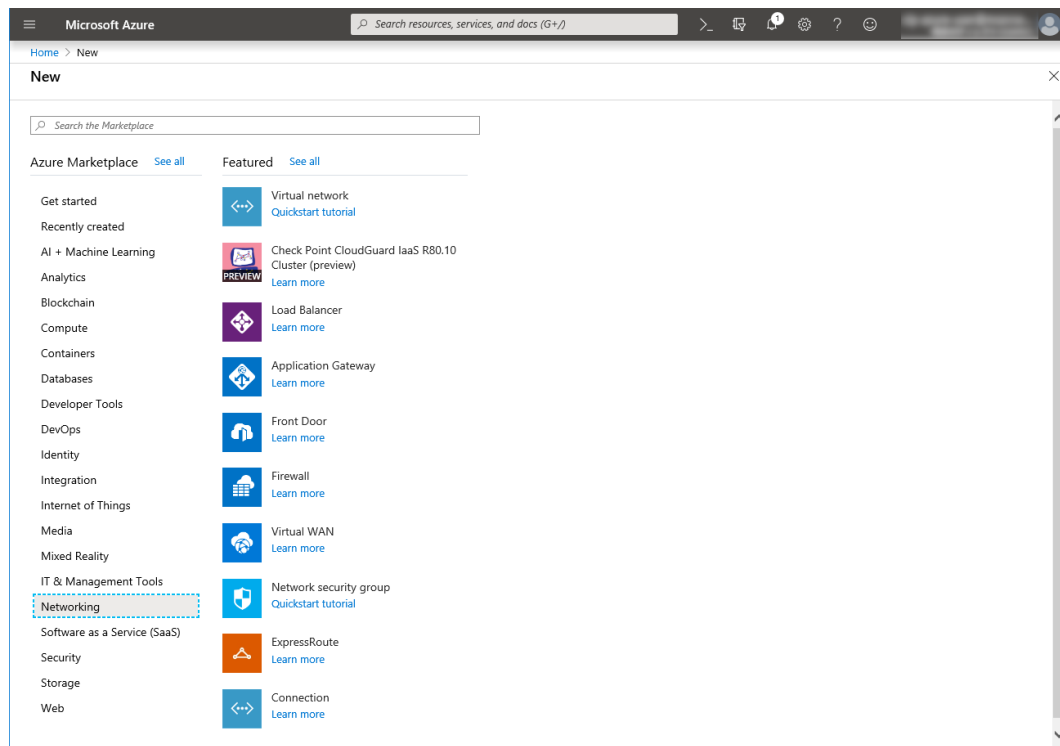
2) **Creating a virtual network**

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

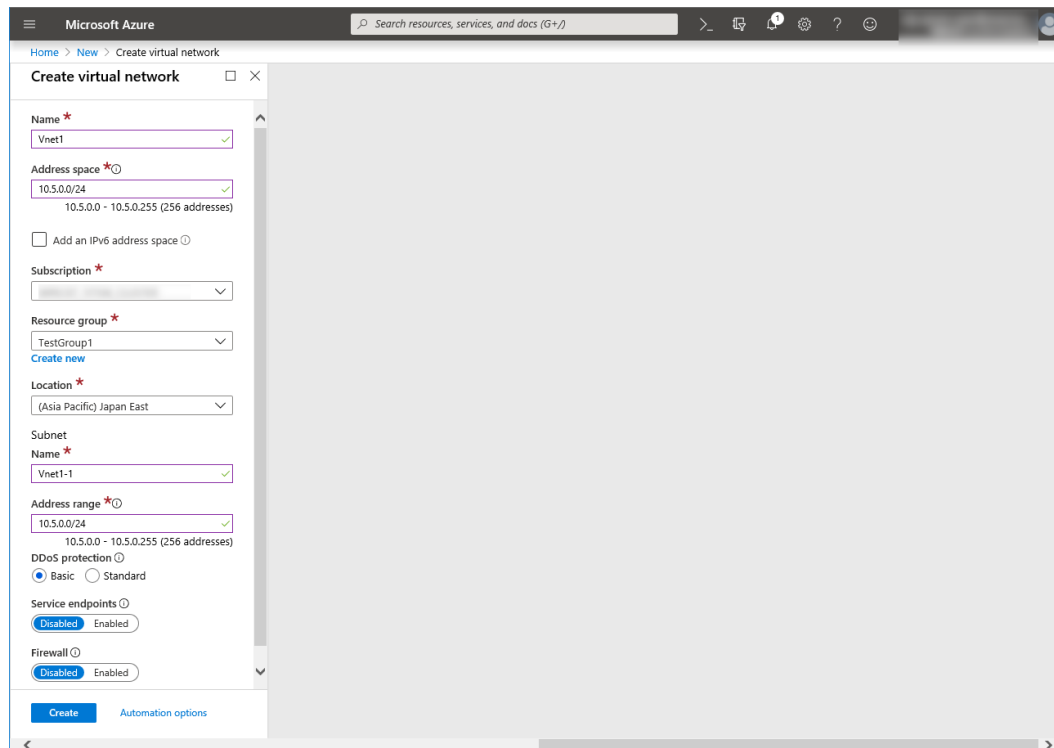
1. Select the **Create a resource** icon on the upper part of the window.



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



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

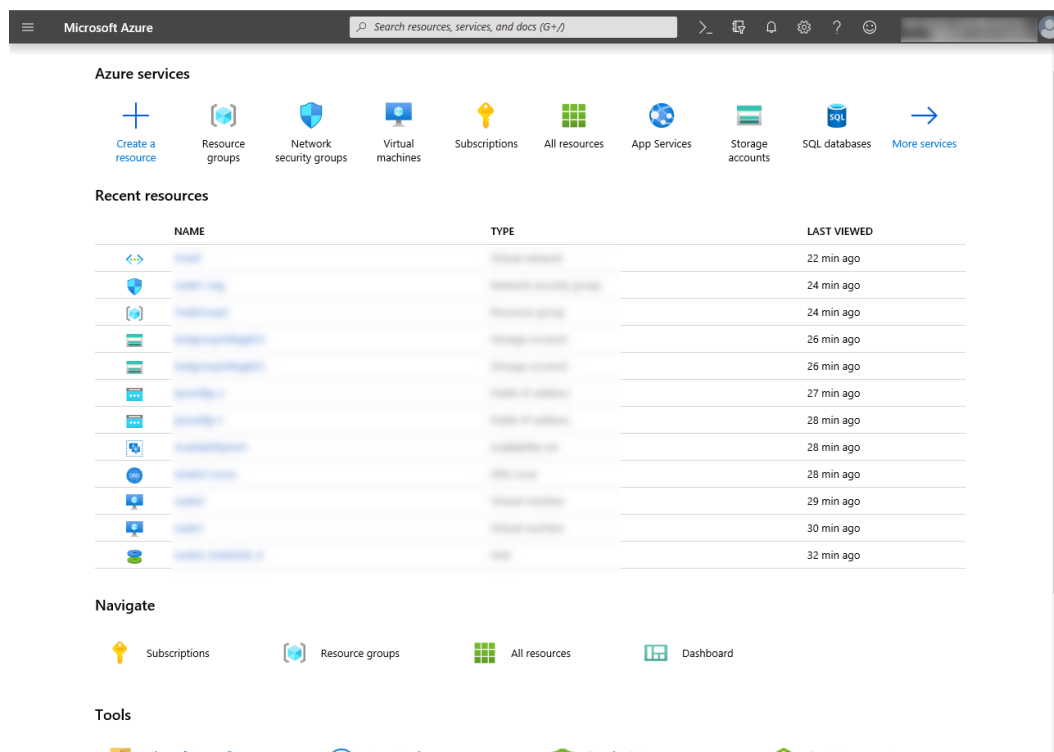


3) Creating a virtual machine

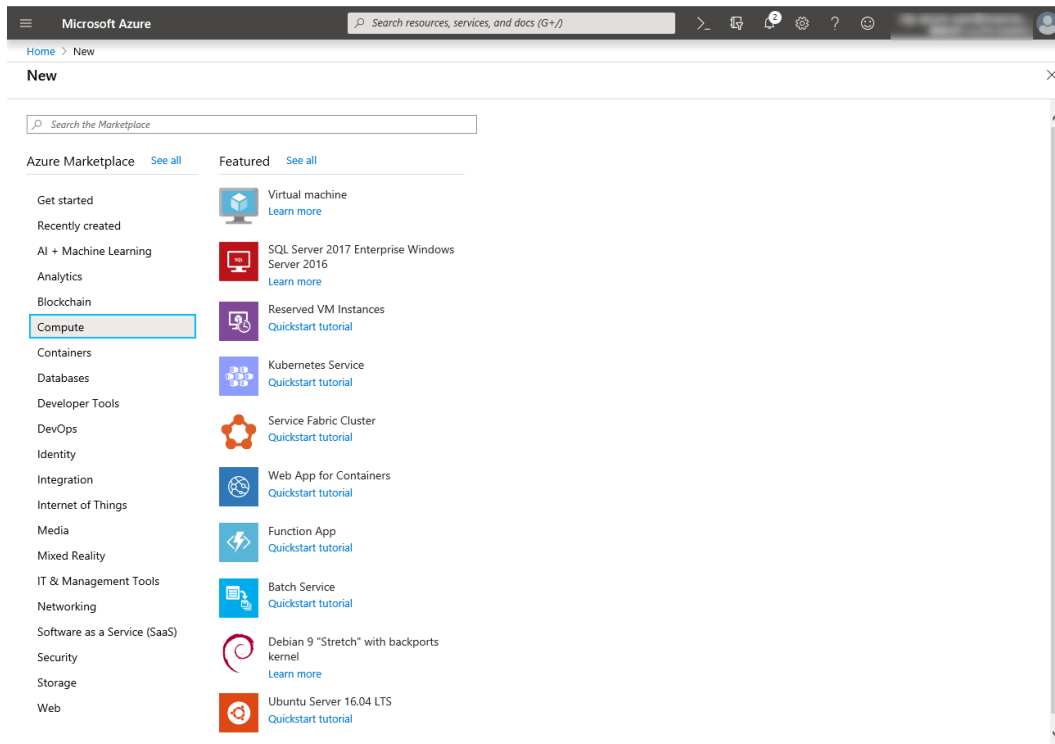
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create virtual machines and disks following the steps below.

Create as many virtual machines as required to create a cluster. Create node1 and then node2.

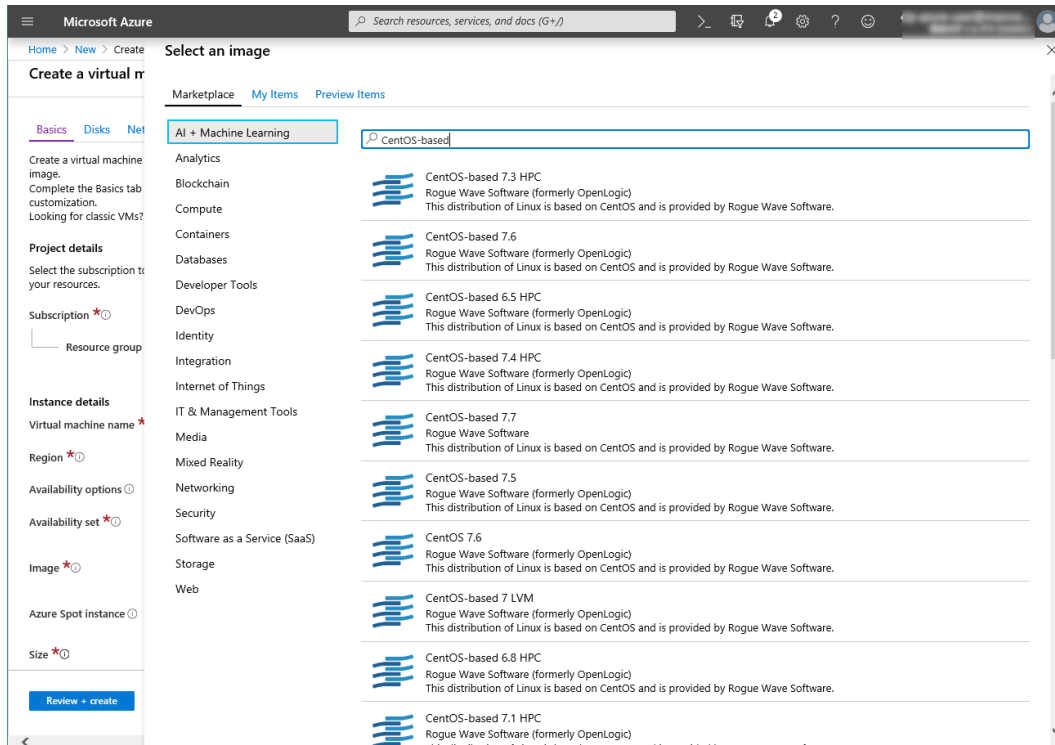
1. Select the **Create a resource** icon on the upper part of the window.



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



3. Select **CentOS-based 7.6**.

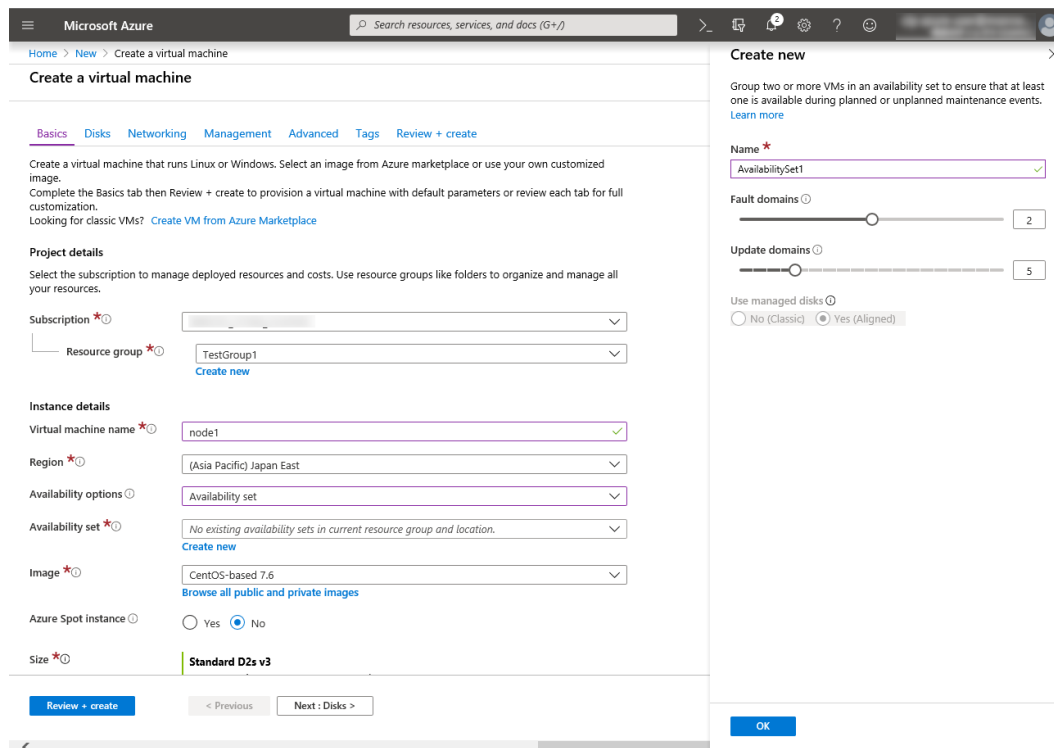
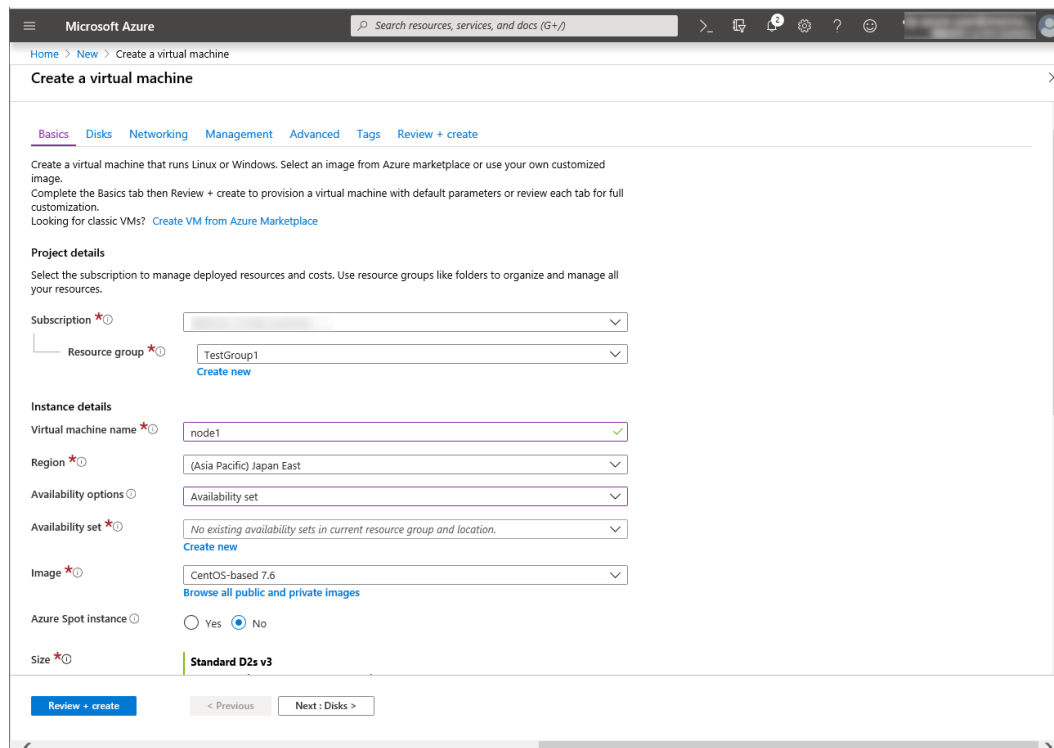


4. Click **Create**.

5. 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 **Create new** appears, specify the settings of **Name, Fault domains, and Update domains**. Then click **OK**.



6. Click **Change size** to display **Select a VM size**.

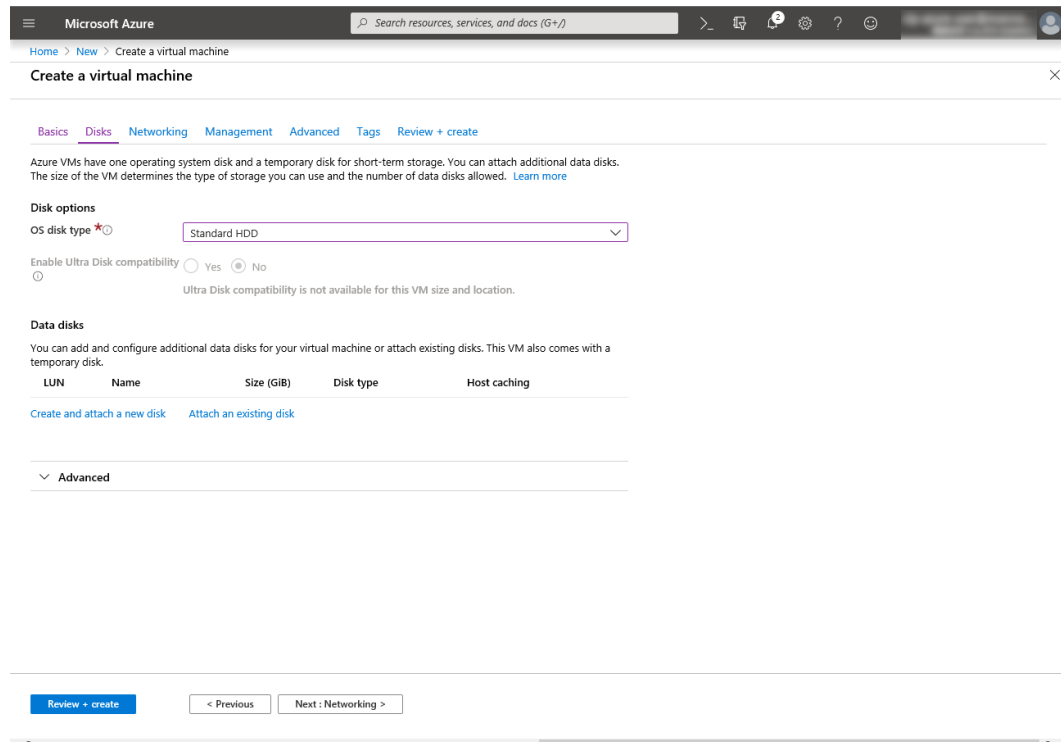
From the list, choose a size (**Standard - A1** in this guide) suitable for your virtual machine and click **Select**.

Regarding the **Virtual machine name**, node1 is for node1, and node2 is for node2.

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).

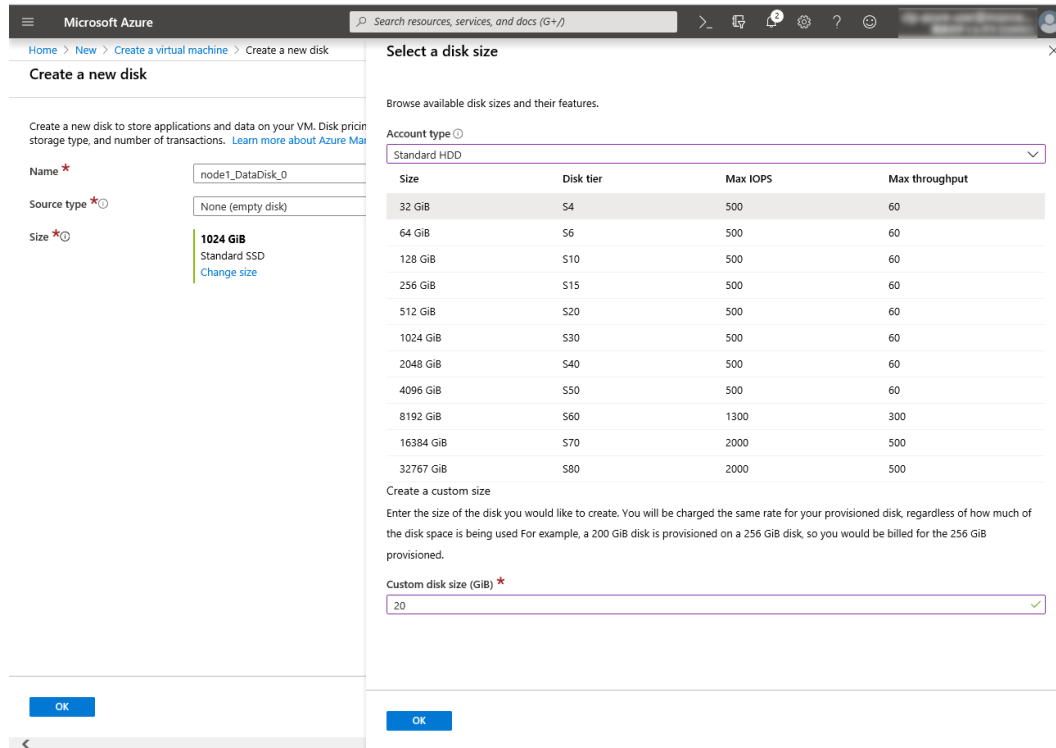
From the **DATA DISKS** list, click **Create and attach a new disk**.



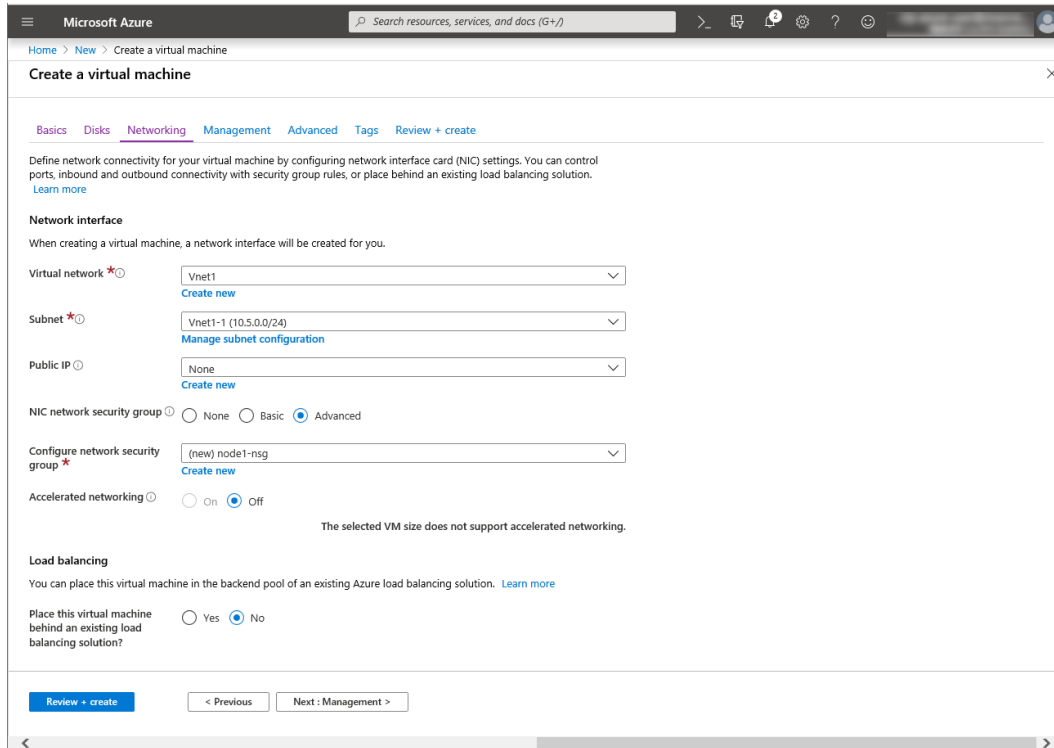
- Create a new disk** appears.

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

Click **Next: Networking >**

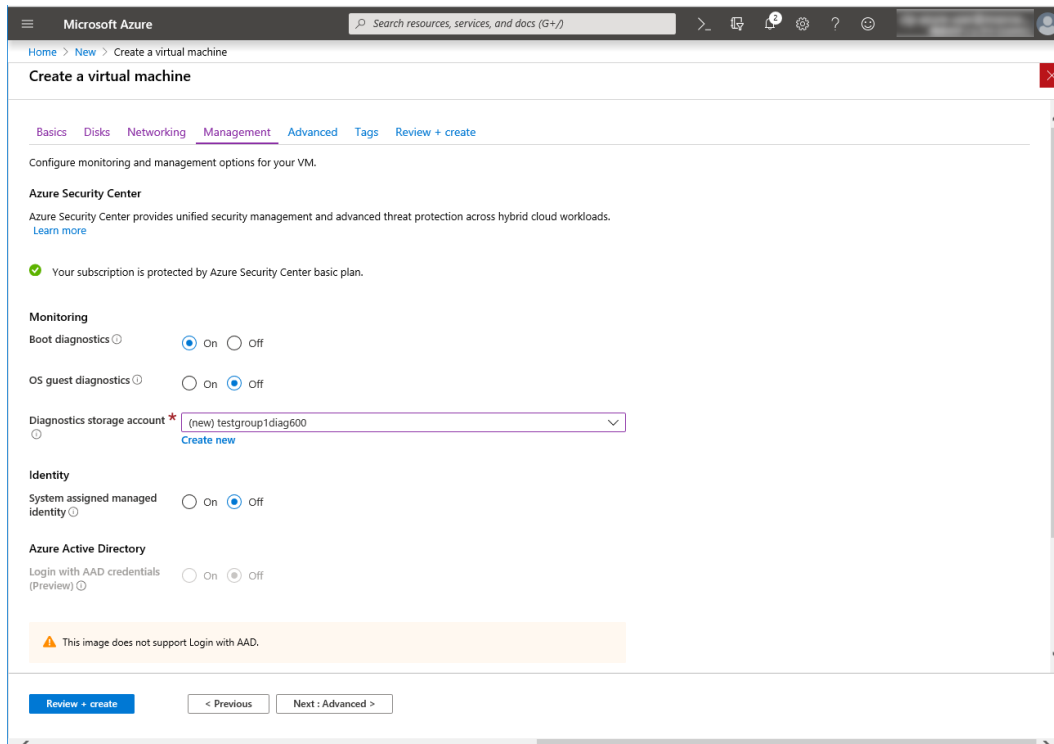


9. The **Networking** tab appears.
Specify the settings of **Virtual network**, **Subnet**, **NIC Network security group**, and **Configure network security group**.
Click **Create new** under the **Configure network security group** field to display **Create network security group**. Specify the setting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

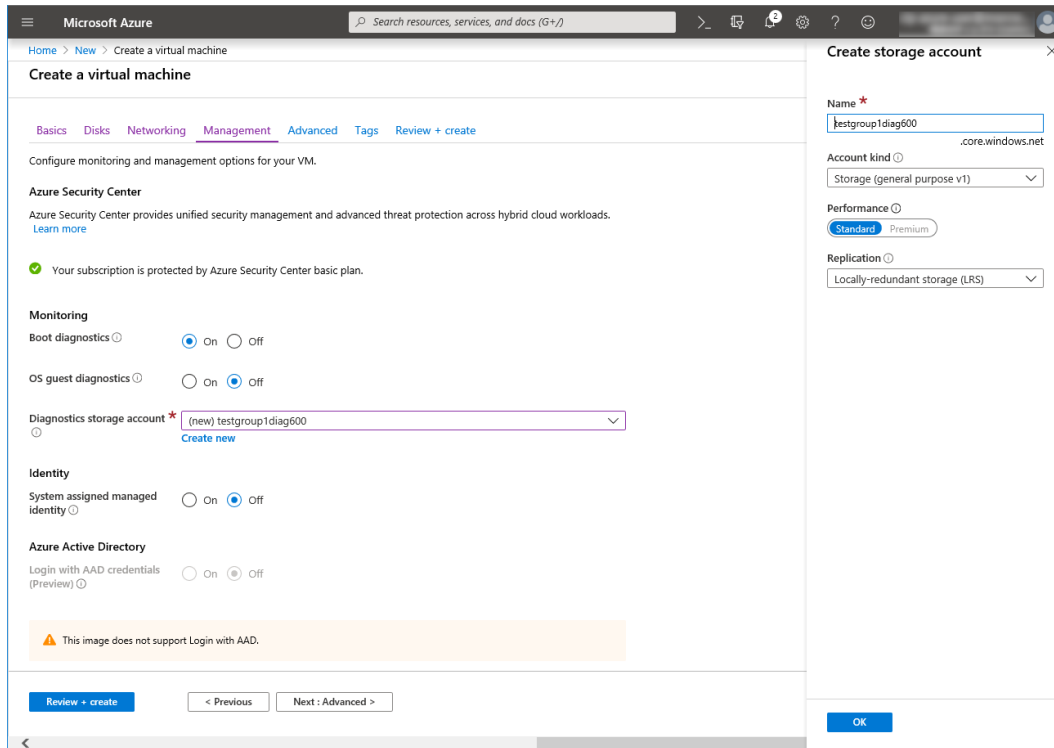


10. The **Management** tab appears.

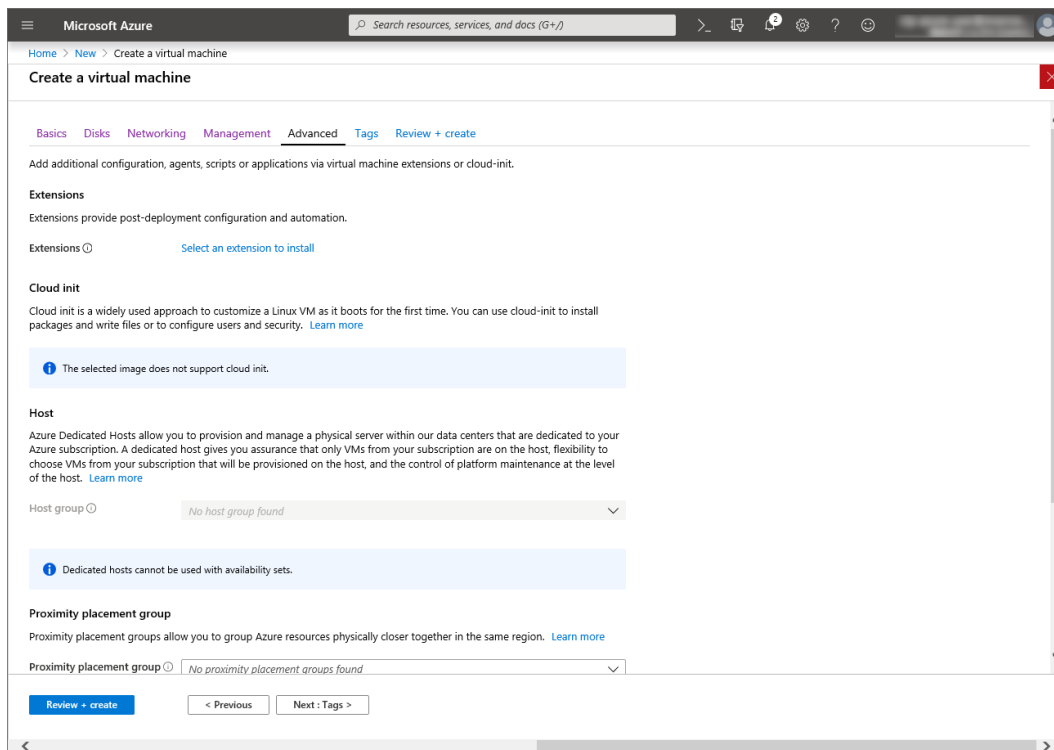
Click **Create new** under the **Diagnostics storage account** field to display **Create storage account**. Specify the settings of **Name**, **Account kind**, and **Replication**. Then click **OK**. In the **Diagnostics storage account** field, the default value is automatically generated and entered. Click **Next: Details >**



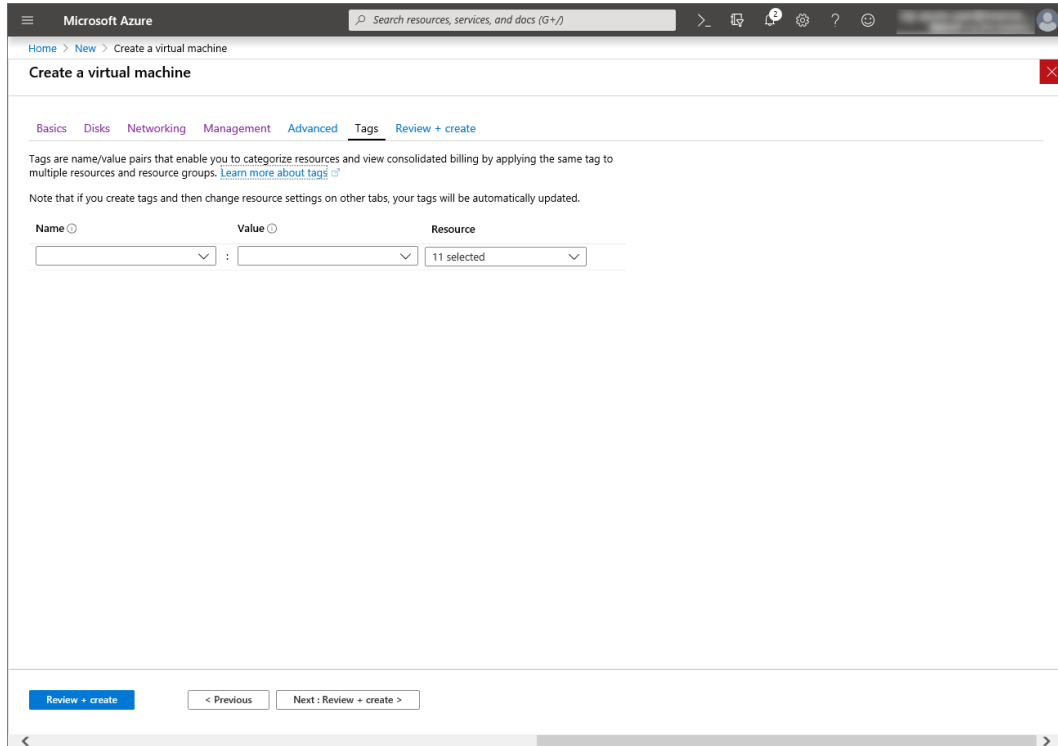
EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



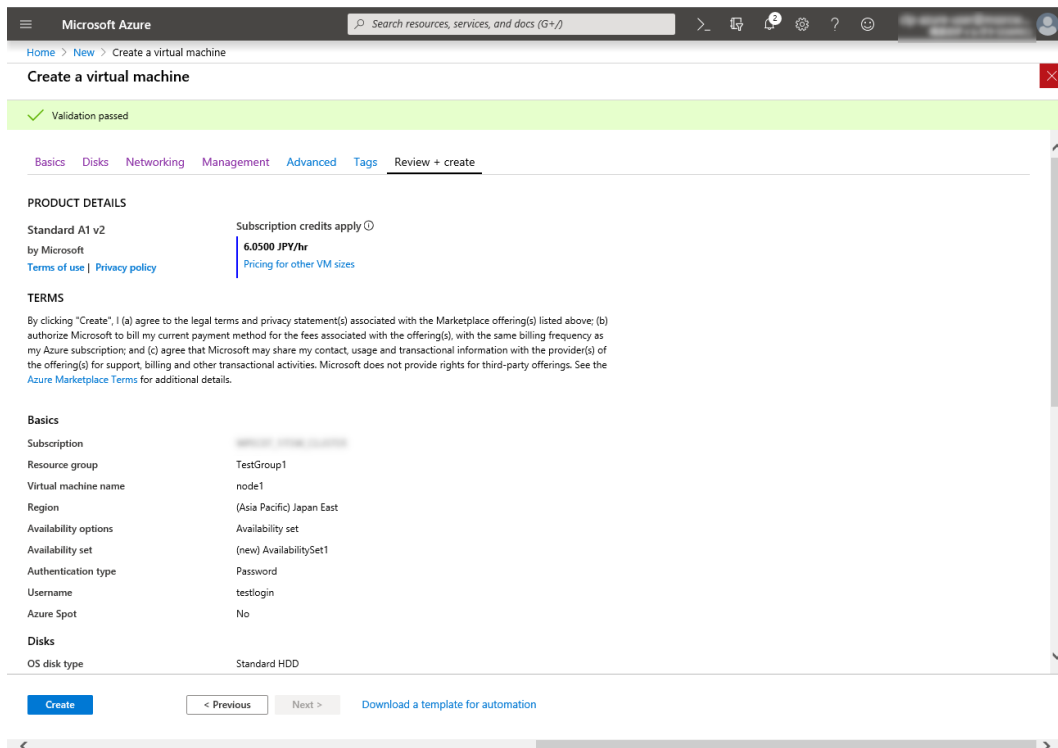
11. Click **Next: Tags >**.



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



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

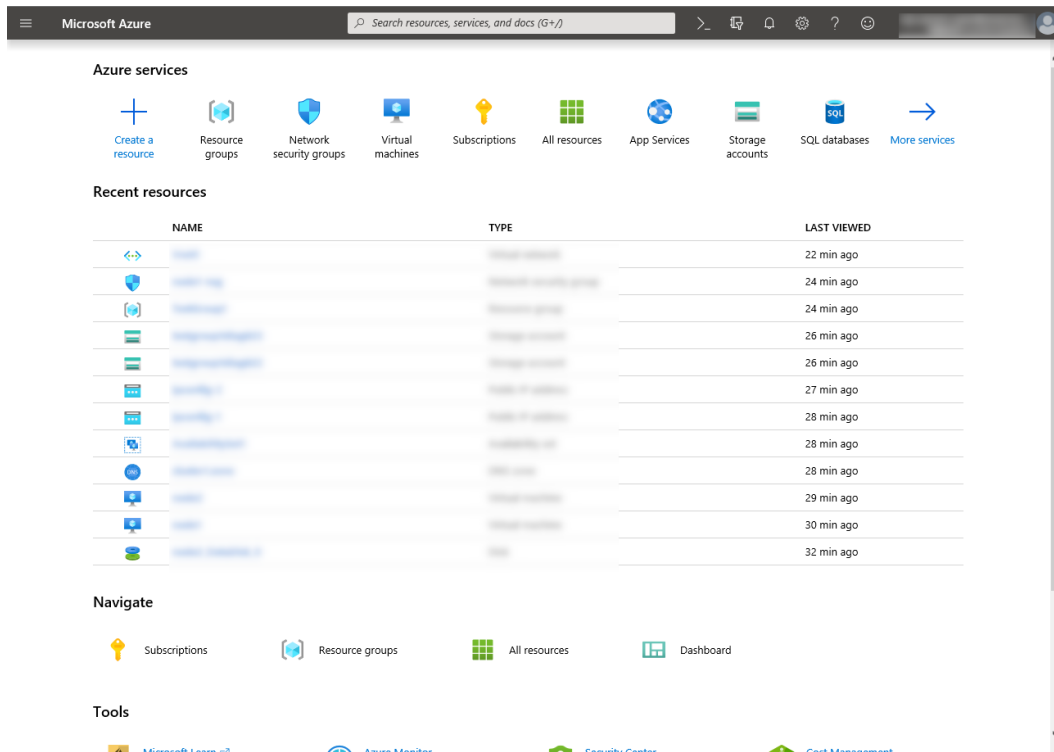


4) Setting a private IP address

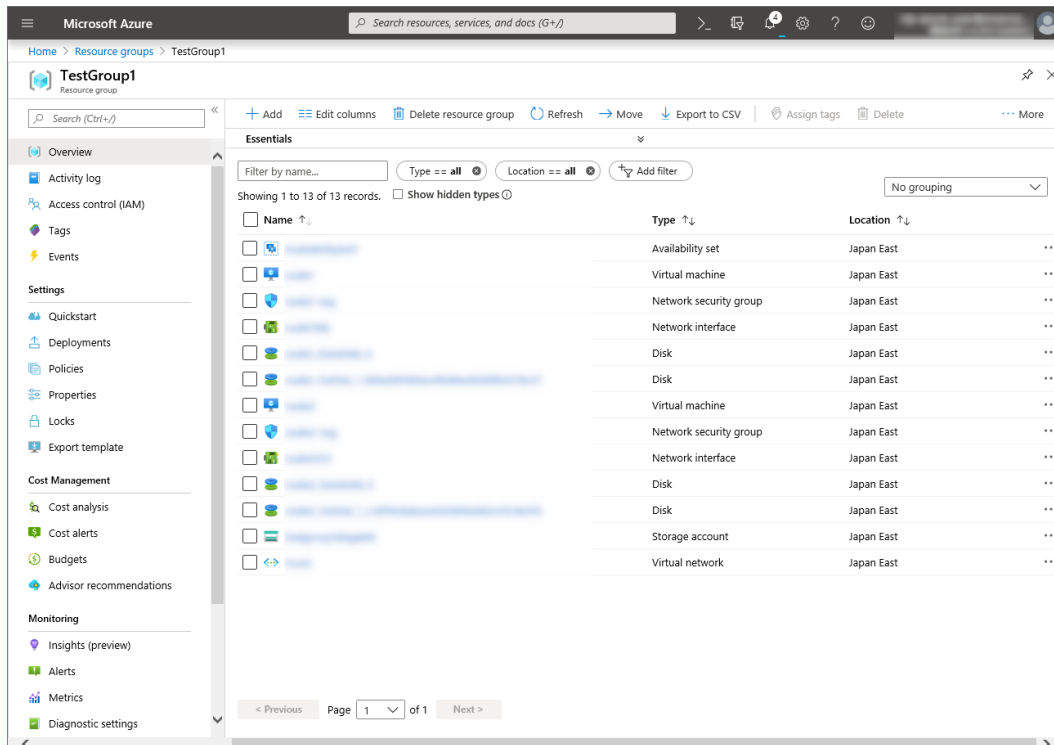
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and change the private IP address setting following the steps below. Since an IP address is initially set to be assigned dynamically, change the

setting so that an IP address is assigned statically. Change the settings of node1 and then node2.

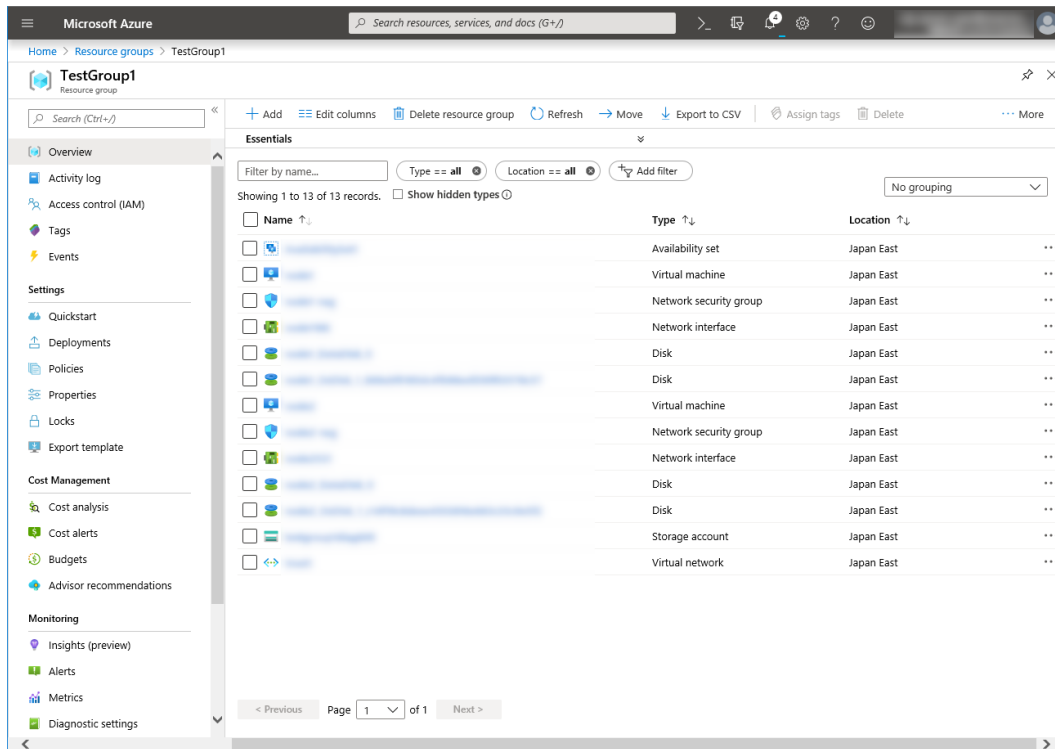
1. Select the **Resource groups** icon on the upper part of the window.



2. Select TestGroup1 from the resource group list.
3. The summary of TestGroup1 is displayed. Select virtual machine node1 or node2 from the item list.

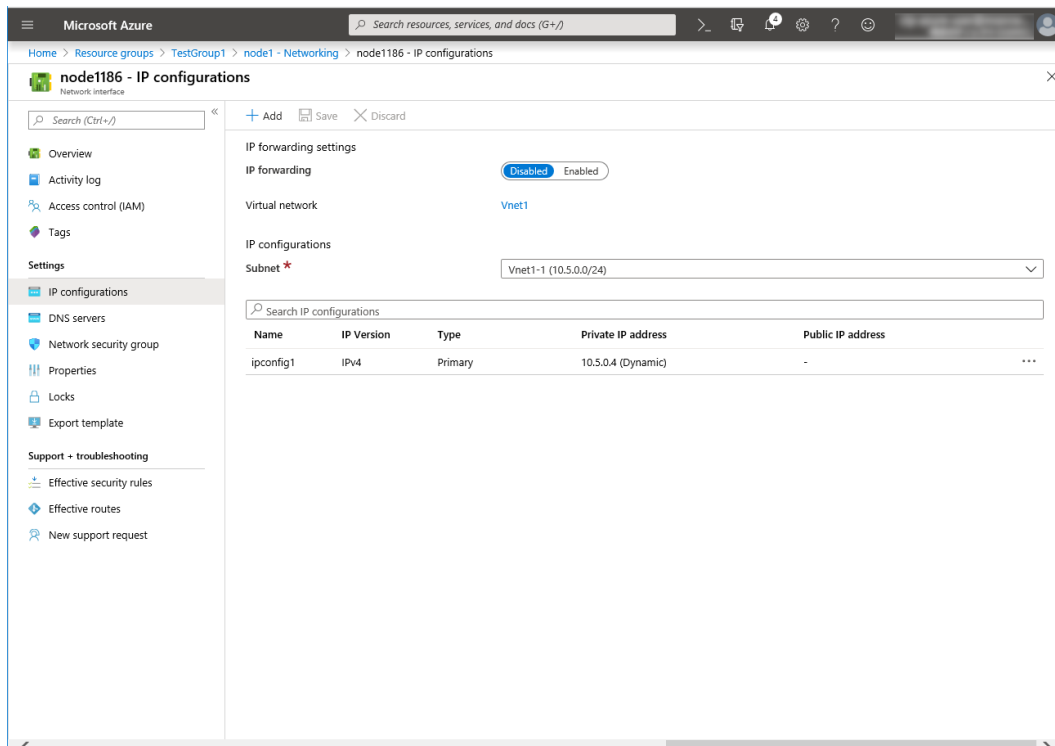


4. Select Networking.

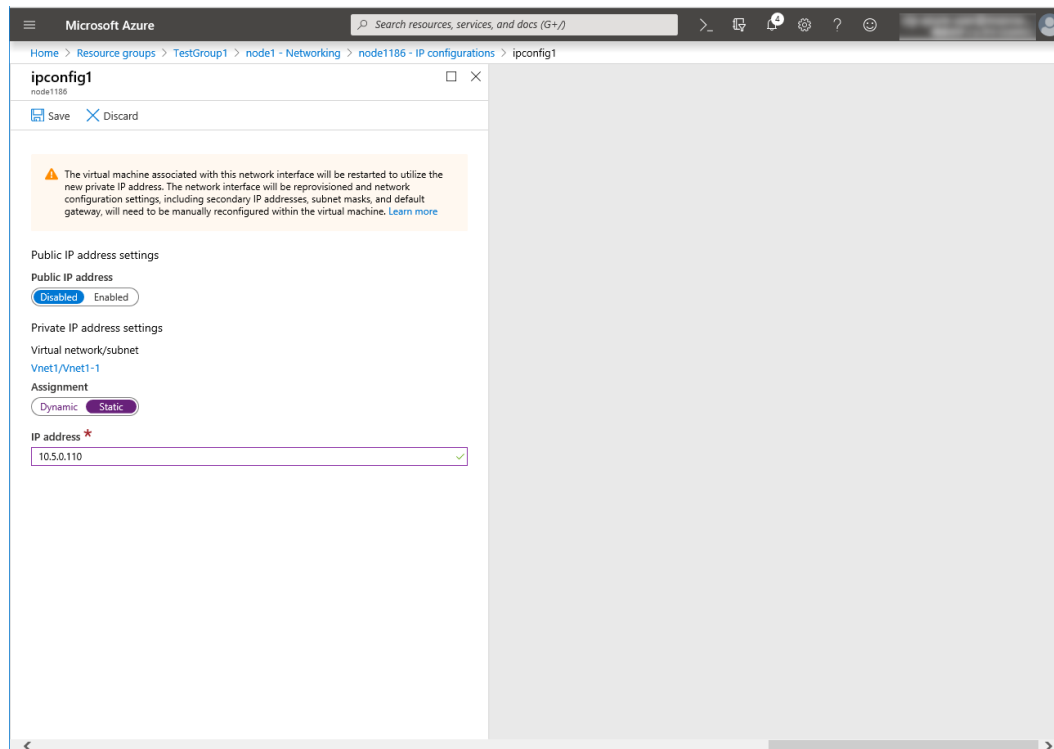


5. Select a network interface displayed in the list. The network interface name is generated automatically.

6. Select IP configurations.



- Only ipconfig1 is displayed in the list. Select it.
- 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 node1 is 10.5.0.110. The IP address of node2 is 10.5.0.111.



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

5) Configuring virtual machines

Log in to the created node1 and node2 and specify the settings following the procedure below. Set a partition for the mirror disk resource. Create a file system in the added disk. Secure an area in the added disk by using the fdisk command and then create a file system. For details about the partition for the mirror disk resource, see "Settings after configuring hardware" in "Partition settings for Mirror disk resource (when using Replicator)" in "Determining a system configuration" in the Installation and Configuration Guide

- Check the partition list. In the following example, the last line shows the added disk.

```
$ cat /proc/partitions
major minor #blocks name

 2         0          4 fd0
 8         0    31457280 sda
 8         1     512000 sda1
 8         2    30944256 sda2
 8        16    73400320 sdb
 8        17    73398272 sdb1
 8        32    20971520 sdc
```

- Create a cluster partition and data partition in the added disk by using the fdisk command. Allocate 1 GB (1*1024*1024*1024 bytes) or more to a cluster partition. (If the size is specified as just 1 GB,

the actual size will be larger than 1 GB depending on the disk geometry difference. This is not a problem.) Also, do not create a file system in a cluster partition.

- If you select **Execute initial mkfs** when creating the cluster configuration data by using Cluster WebUI, EXPRESSCLUSTER creates a file system automatically. Note that existing data in the partition will be lost.

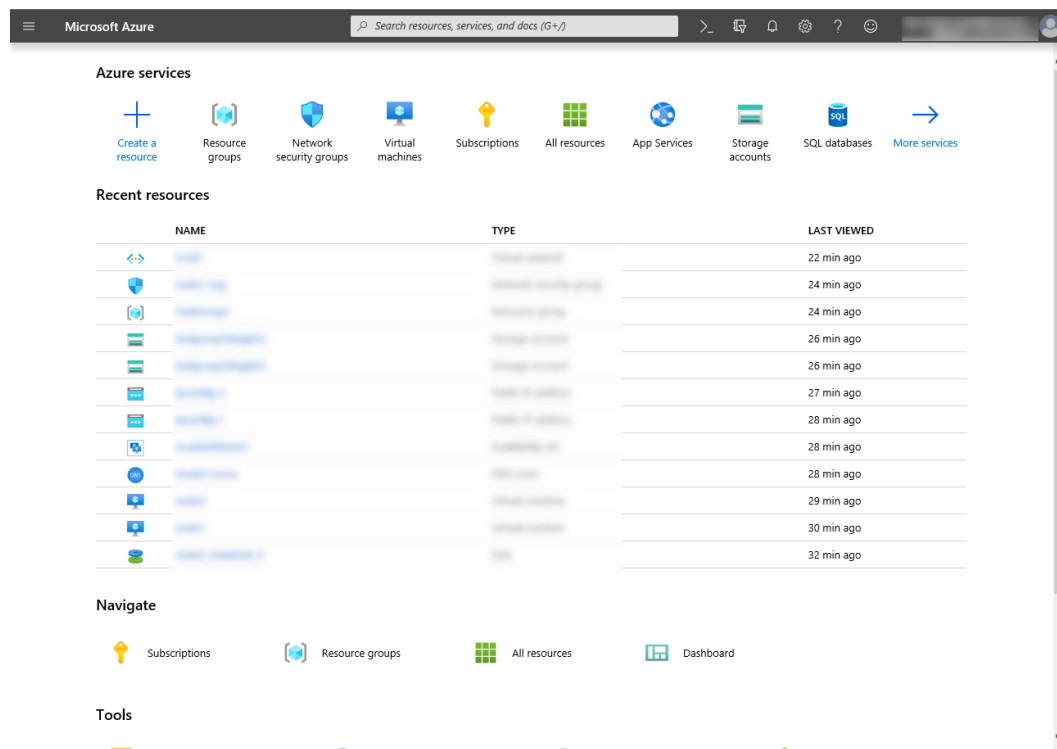
For DSR, add a Loopback Adapter in each node configuring a cluster.

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

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



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

EXPRESSCLUSTER X 5.2 HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2

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

Home > 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 * [dropdown]

Resource group * [TestGroup1] [Create new](#)

Instance details

Name * [TestLoadBalancer] ✓

Region * [(Asia Pacific) Japan East] ✓

Type * Internal Public

SKU * Basic Standard

Configure virtual network.

Virtual network * [Vnet1] ✓

Subnet * [Vnet1-1 (10.5.0.0/24)] ✓ [Manage subnet configuration](#)

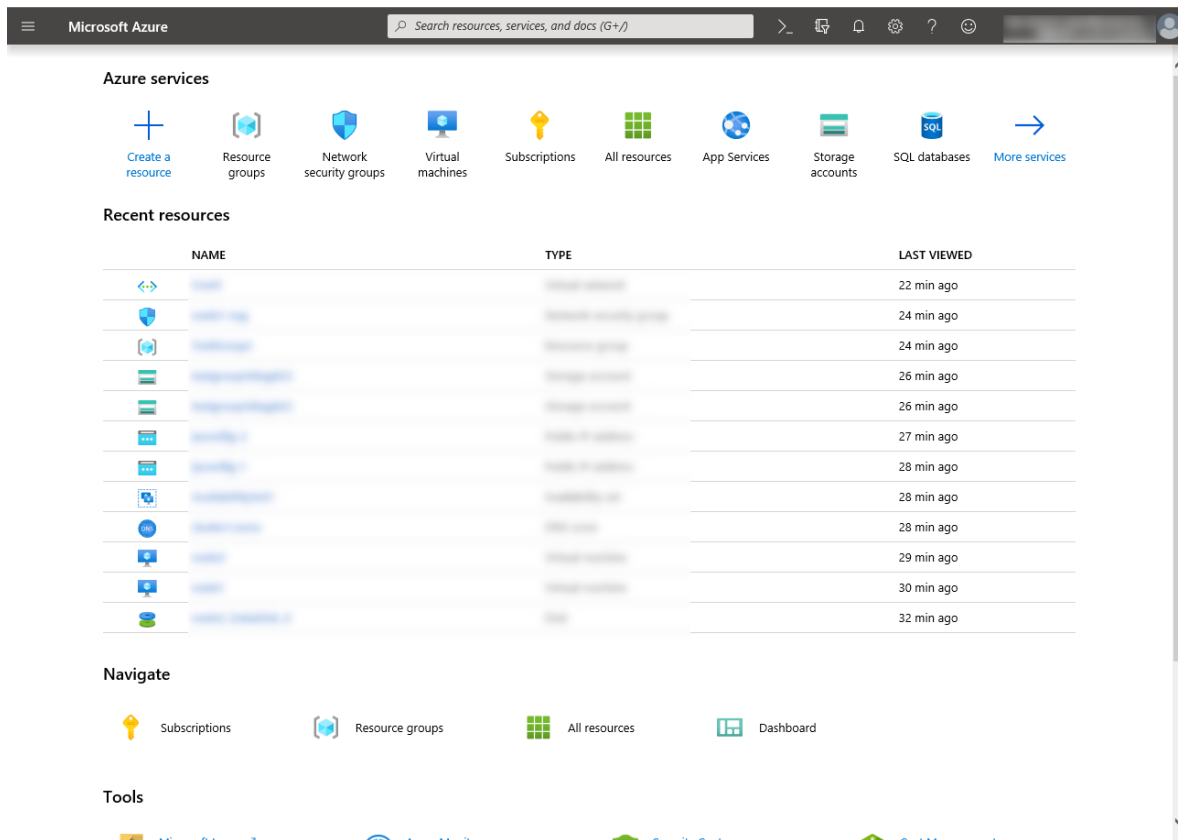
IP address assignment * Static Dynamic

Private IP address * [10.5.0.200] ✓

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

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

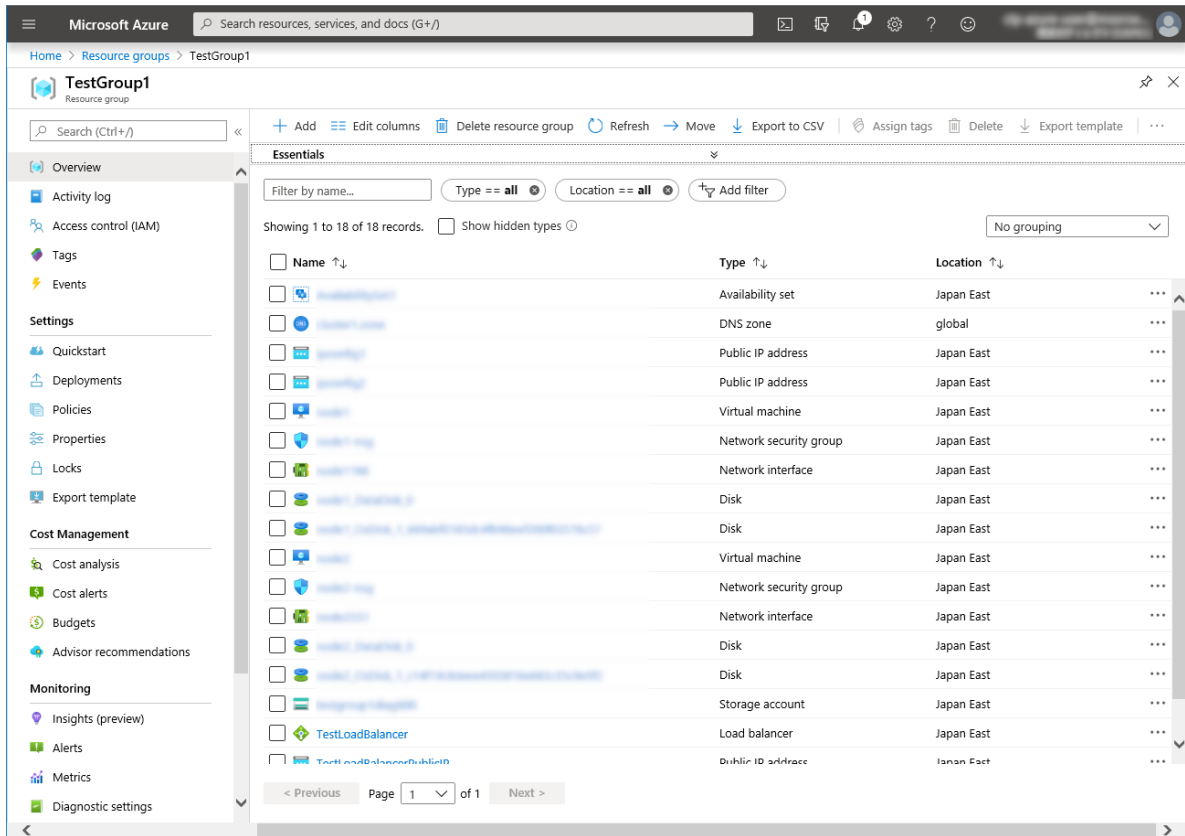
1. Associate a virtual machine registered to the availability set to the load balancer. After the load balancer has been deployed, select the **Resource groups** icon on the upper part of the window.



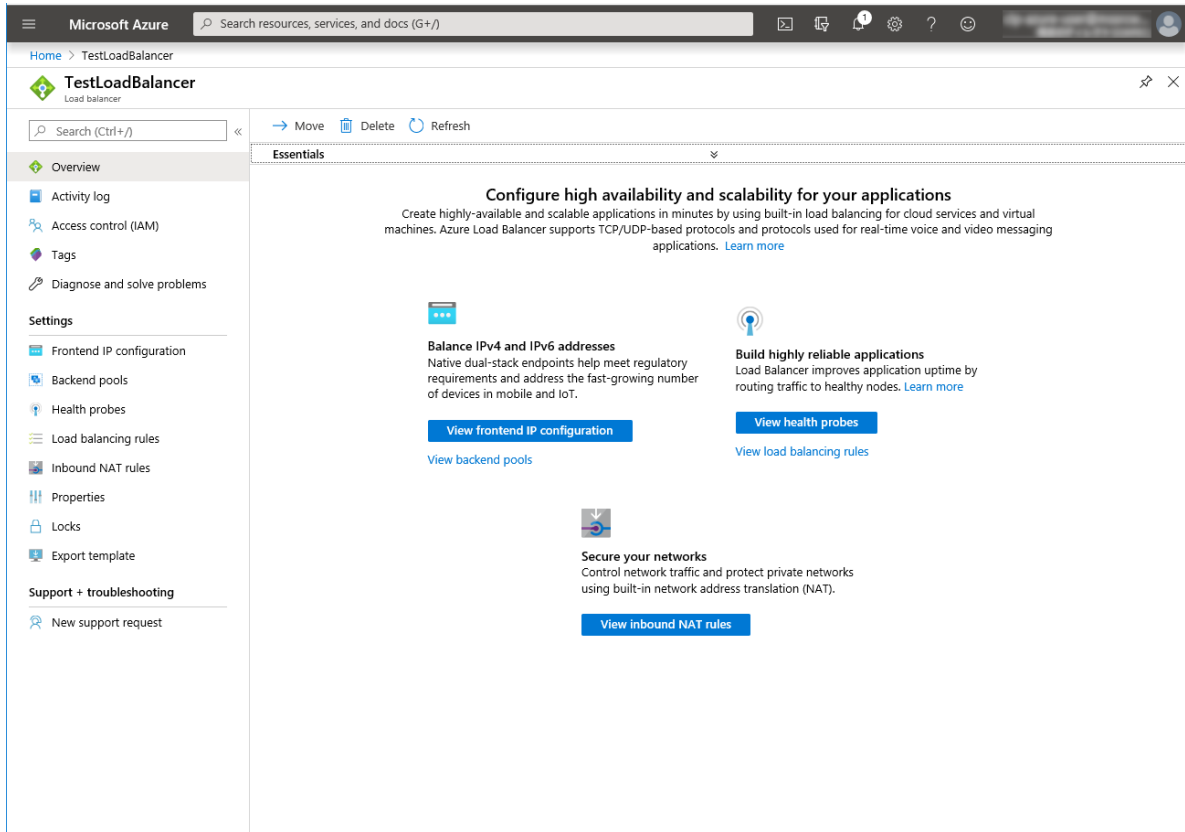
2. Select the resource group to which the created load balancer belongs from the resource group list.
3. The summary of the selected resource group is displayed. Select the created load balancer from the item list.

EXPRESSCLUSTER X 5.2

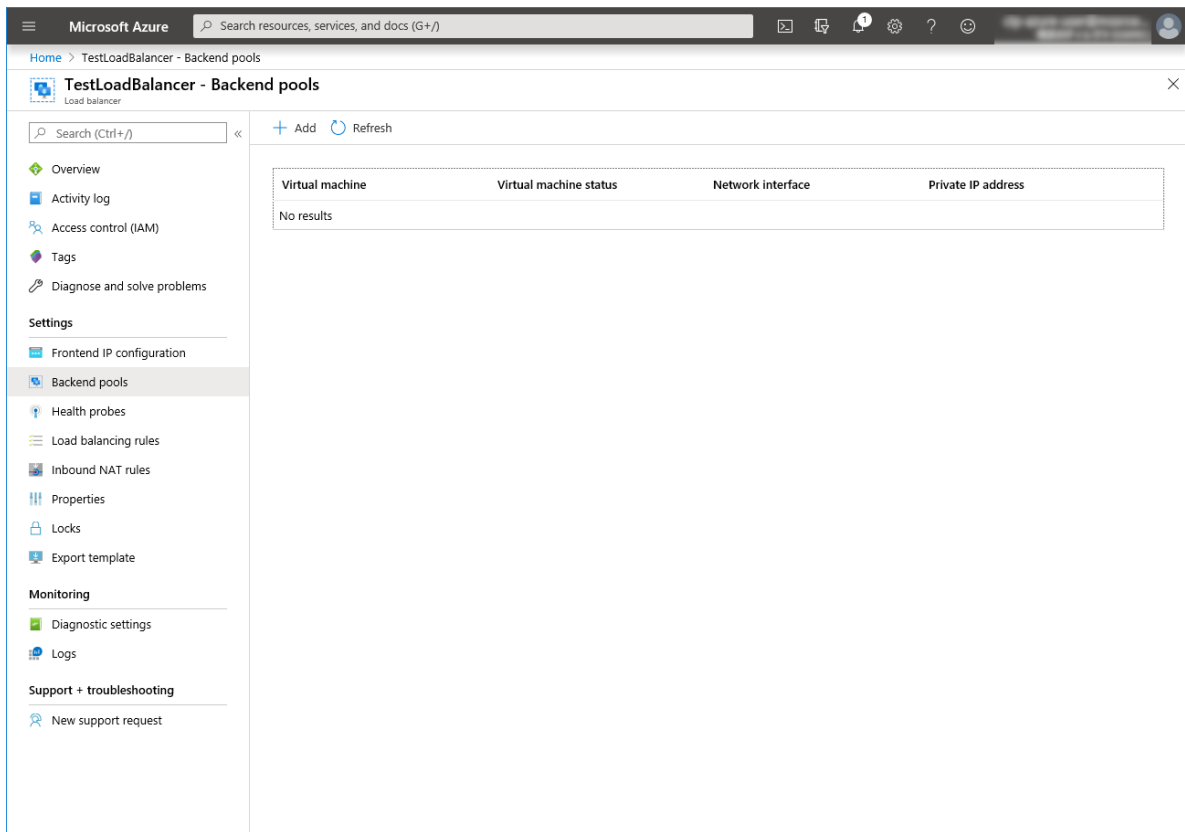
HA Cluster Configuration Guide for Microsoft Azure (Linux), Release 2



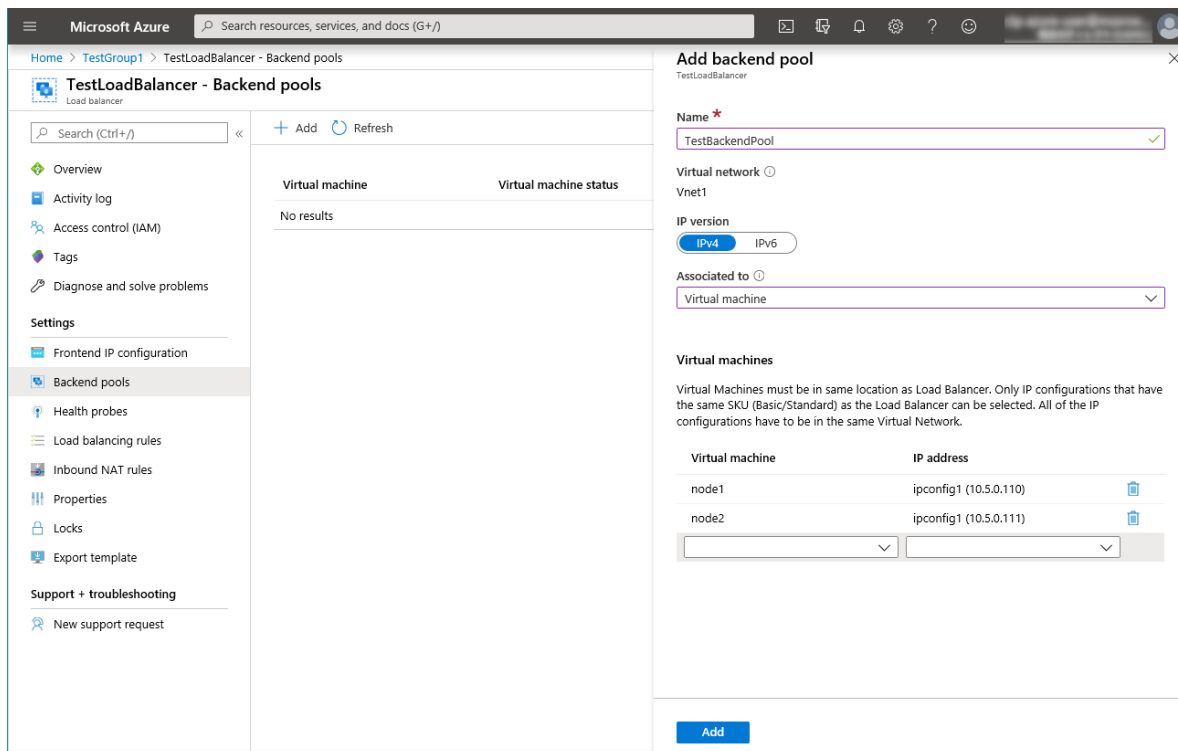
4. Select **Backend pools**.



5. Click **Add**.

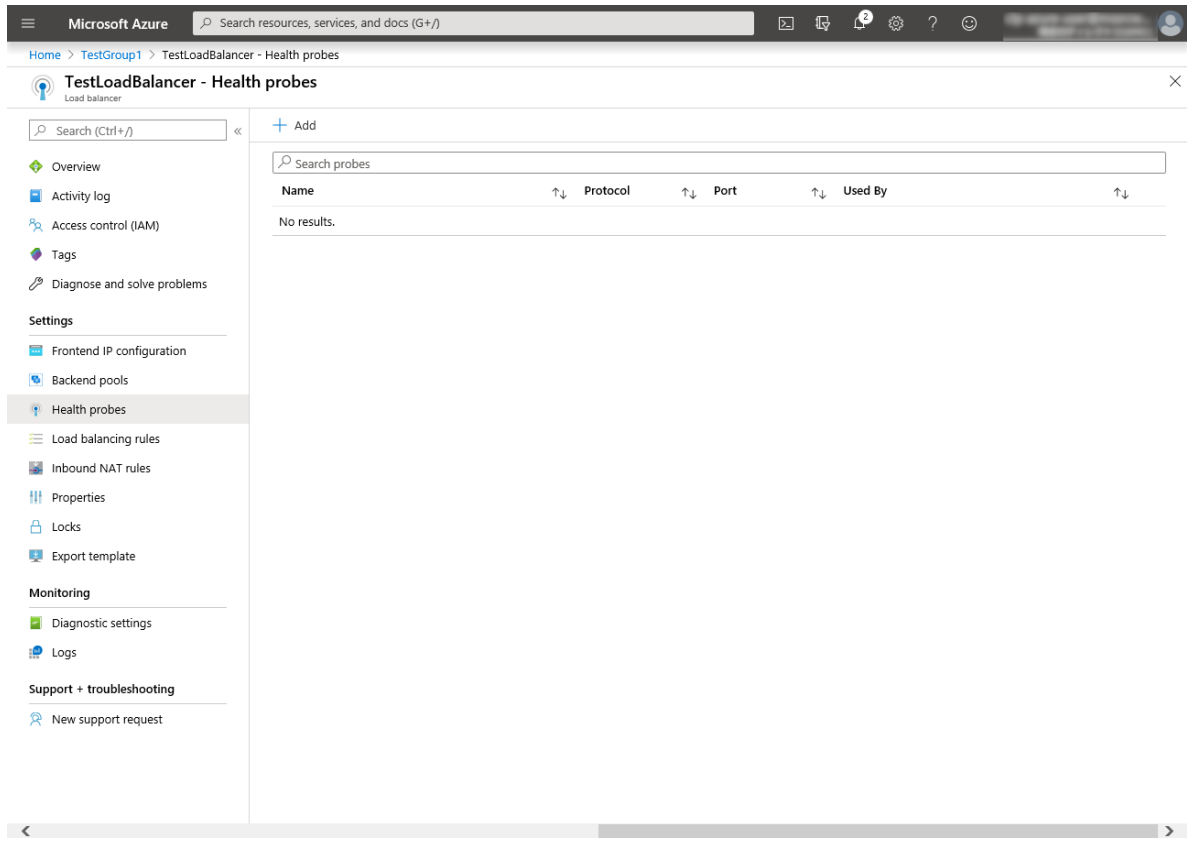


6. **Add backend pool** is displayed. Specify **Name**.
7. Select **Virtual machine** for **Associated to**.
8. Specify **Virtual machine** and **IP address** for the virtual machine you want to associate. Repeat this procedure for the rest of such virtual machines.
9. Then click **Add**.

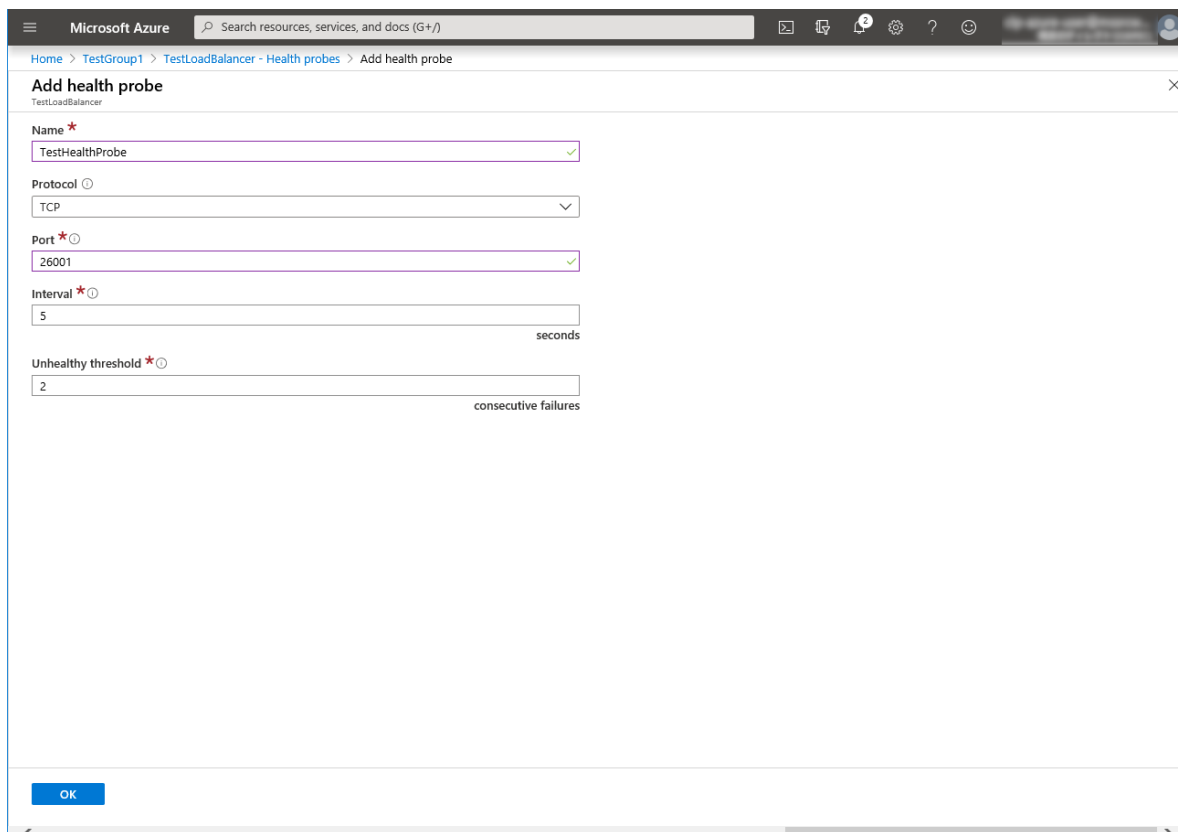


8) Configuring a load balancer (configuring a health probe)

1. Select **Health probes**.



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



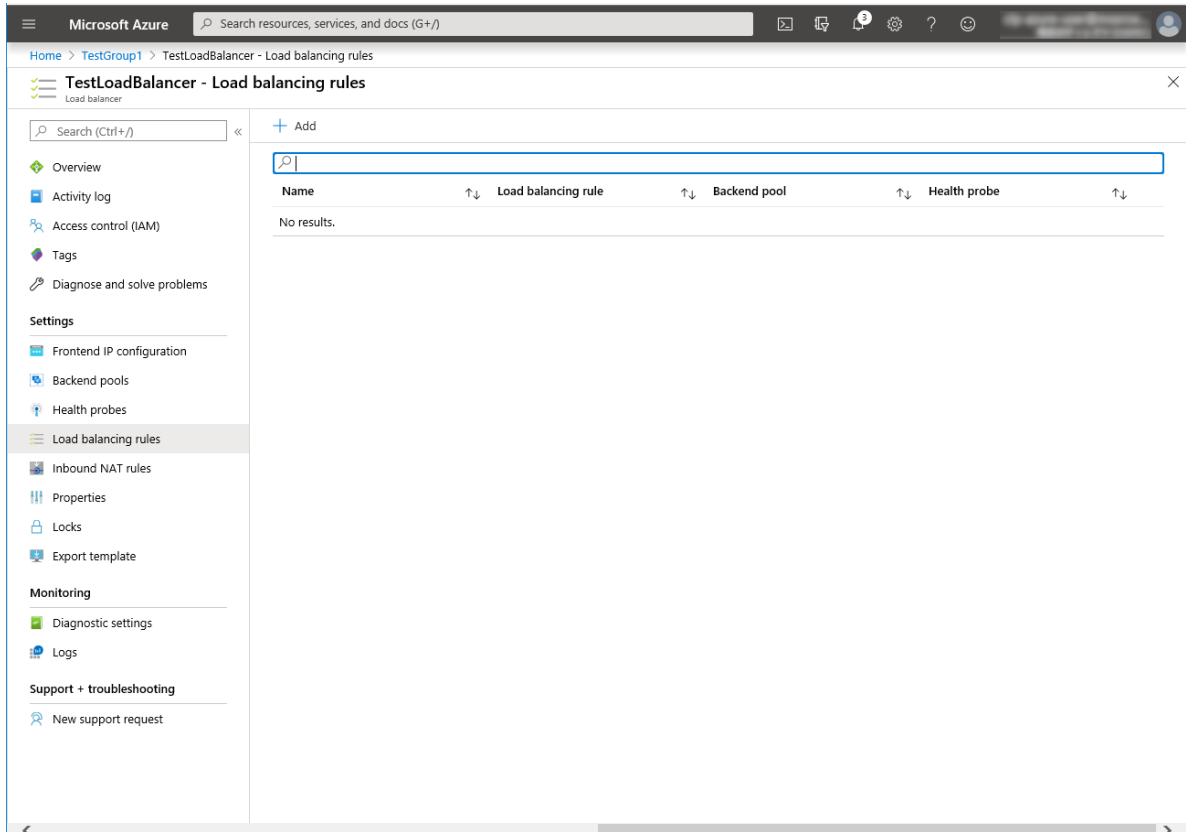
The screenshot shows the 'Add health probe' configuration window in the Microsoft Azure portal. The window title is 'Add health probe' and it is part of the 'TestLoadBalancer' resource. The configuration fields are as follows:

- Name ***: TestHealthProbe
- Protocol**: TCP
- Port ***: 26001
- Interval ***: 5 seconds
- Unhealthy threshold ***: 2 consecutive failures

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

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**.
For DSR, specify **Port** and **Backend port** to same port number, enable to **Floating IP(Direct Server Return)**, and click **OK**.
(Specify the port number used to connect to the application (example.80).)

The screenshot shows the 'Add load balancing rule' dialog in the Microsoft Azure portal. The fields are as follows:

- Name: TestLoadBalancingRule
- IP Version: IPv4
- Frontend IP address: 10.5.0.200 (LoadBalancerFrontEnd)
- Protocol: TCP
- Port: 80
- Backend port: 8080
- Backend pool: TestBackendPool
- Health probe: TestHealthProbe (TCP:26001)
- Session persistence: None
- Idle timeout (minutes): 4
- Floating IP (direct server return): Disabled

- 10) **Adjusting the OS startup time, checking the network setting, checking the root file system, checking the firewall setting, synchronizing the server time, and checking the SELinux setting.**

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:

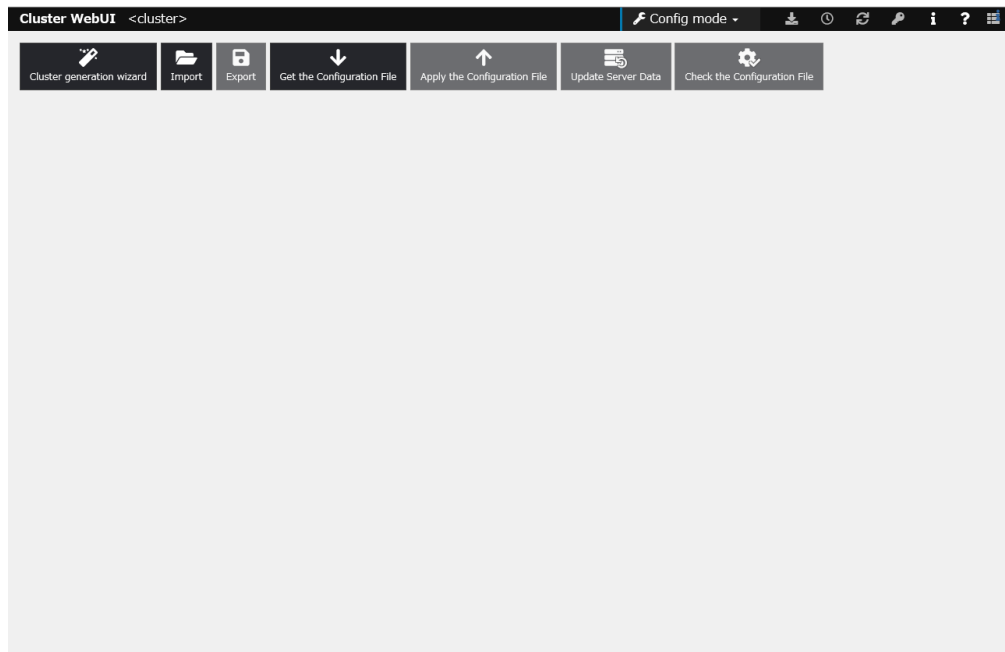
- Mirror disk resource
- Azure probe port resource
- Azure probe port monitor resource
- Azure load balance monitor resource
- PING network partition resolution resource (for NP resolution)

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

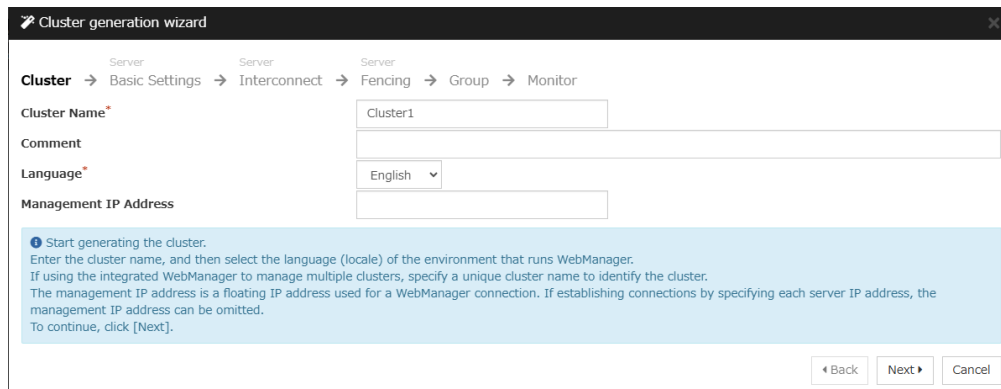
1) Creating a cluster

Start the Cluster generation wizard to create a cluster.

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

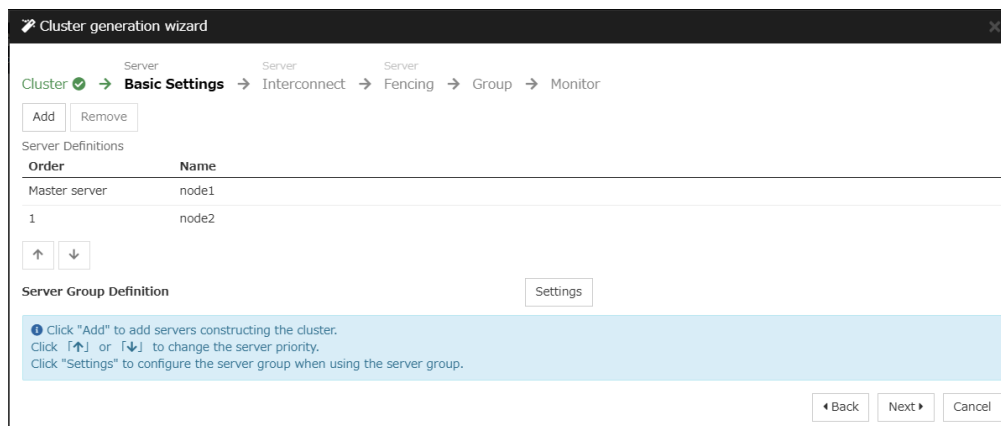


2. **Cluster of Cluster generation wizard** is displayed.
Enter a desired name in **Cluster Name**.
Select an appropriate language in **Language**. Click **Next**.



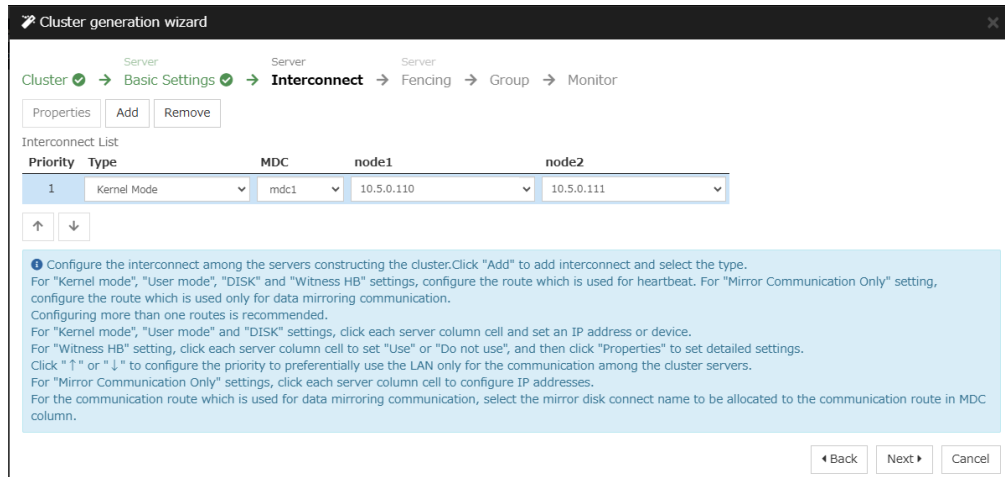
3. **Basic Settings** is displayed.

The instance connected to Cluster WebUI is displayed as a registered master server. Click **Add** to add the remaining instances (by specifying the private IP address of each instance). Click **Next**.



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

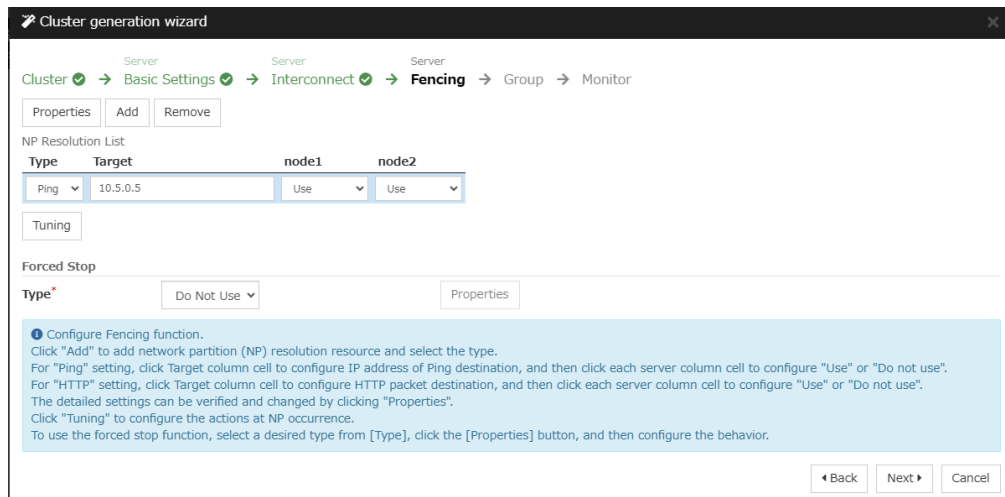
Specify the IP addresses (IP address of each instance) to be used for interconnect. In addition, select mdc1 for **MDC** as a communication path of a mirror disk resource to be created later. Click **Next**.



5. The **Fencing** 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 **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 network. Click a cell of each server column and select **Use** or **Not use**.

Click **Next**.



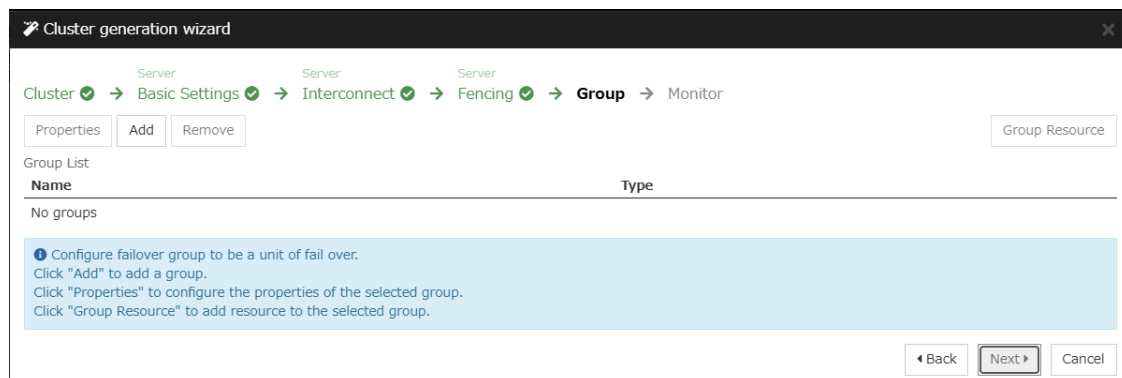
2) **Adding a group resource**

- Defining a group

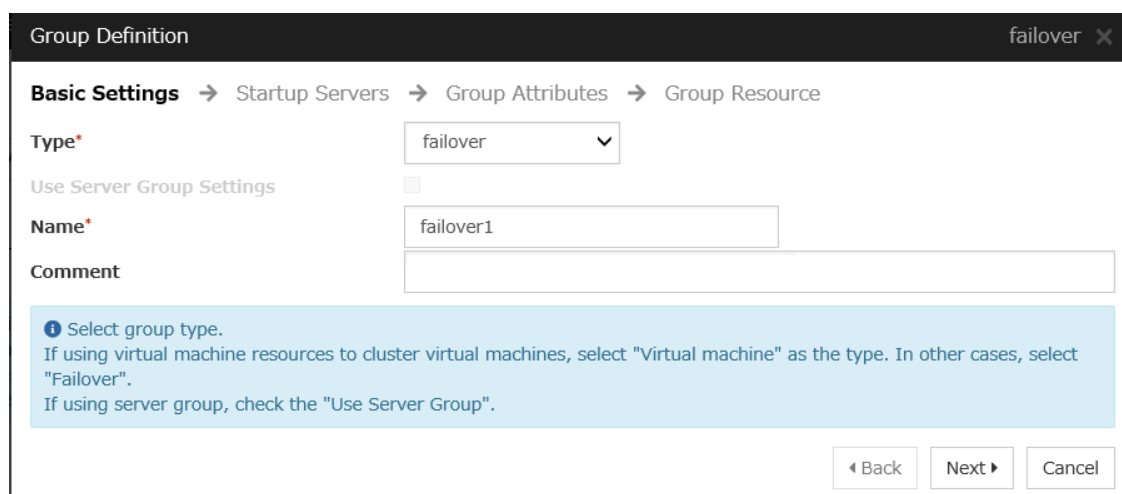
Create a failover group.

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

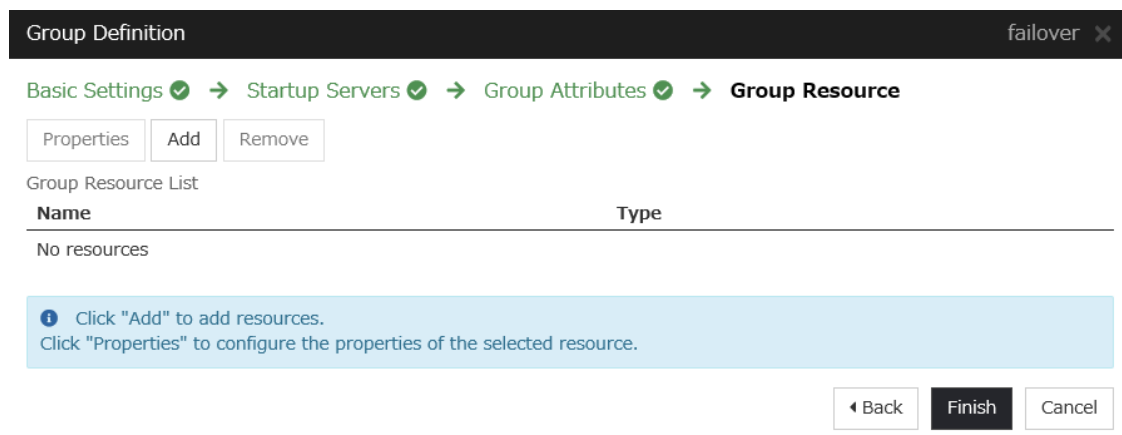
Click **Add**.



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 "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*

Name*

Comment

i 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.
Enter the device name of the partition created in "5) Configuring virtual machines" in **Data Partition Device Name** and **Cluster Partition Device Name**. Specify **Mount Point** and **File System**. Click **Finish** to finish setting.

Resource Definition of Group | failover1 md X

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

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

Mirror Partition Device Name*

Mount Point*

Data Partition Device Name*

Cluster Partition Device Name*

File System*

Mirror Disk Connect

- 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**.

Resource Definition of Group | failover1 azurepp x

Info → Dependency → Recovery Operation → Details

Type*

Name*

Comment

i 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 displayed. Click **Next**.
5. For **Probeport**, enter the value specified for **Port** when configuring a load balancer (configuring health probe).

Resource Definition of Group | failover1 azurepp x

Info ✓ → Dependency ✓ → Recovery Operation ✓ → Details

Probeport*

6. Click **Finish**.

- EXEC resource(for DSR)

EXPRESSCLUSTER provides a mechanism to add / remove front-end ip address as the load balancer switches. For details about the EXEC resources", see "Understanding EXEC 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 (EXEC resource) from the **Type** box and enter the group name (exec1) in the **Name** box.
3. Click **Next**.

4. The **Dependency** window is displayed. Click **Next** without specifying anything.
5. The **Recovery Operation** window displayed. Click **Next**.
6. The **Details** window displayed. Select the start.sh. Click **Edit**.
The following script is a sample script. Customize it to change your environment.

(Example: sample script of start.sh)

```
# Server1
SERVER1_NAME="server1" # hostname
SERVER1_NIC="lo" # Interface name for local loopback

# Server2
SERVER2_NAME="server2" # hostname
SERVER2_NIC="lo" # Interface name for local loopback

# VIP Address
VIP=10.5.0.200 # Load balancer front-end IP address
NETMASK=255.255.255.255 # Front-end IP address netmask

# HostName
CURRENT_HOSTNAME=`hostname`

if [ $CURRENT_HOSTNAME = $SERVER1_NAME ]; then
    NIC=$SERVER1_NIC
elif [ $CURRENT_HOSTNAME = $SERVER2_NAME ]; then
    NIC=$SERVER2_NIC
else
    echo "SERVER is not found."
    exit 1
fi

# Add IP Address
ip addr add $VIP/$NETMASK brd + dev $NIC
RET=$?
if [ $RET = 0 ]; then
    exit 0
else
    echo "Failure to add IP Address"
    exit 1
fi
```

7. The **Details** window displayed. Select the stop.sh. Click **Edit**.
The following script is a sample script. Customize it to change your environment.

(Example: sample script of stop.sh)

```
# Server1
SERVER1_NAME="server1" # hostname
SERVER1_NIC="lo" # Interface name for local loopback

# Server2
SERVER2_NAME="server2" # hostname
SERVER2_NIC="lo" # Interface name for local loopback

# VIP Address
VIP=10.5.0.200 # Load balancer front-end IP address
NETMASK=255.255.255.255 # Front-end IP address netmask
```

(continues on next page)

(continued from previous page)

```
# HostName
CURRENT_HOSTNAME=`hostname`

if [ $CURRENT_HOSTNAME = $SERVER1_NAME ]; then
    NIC=$SERVER1_NIC
elif [ $CURRENT_HOSTNAME = $SERVER2_NAME ]; then
    NIC=$SERVER2_NIC
else
    echo "SERVER is not found."
    exit 1
fi
# Del IP Address
ip addr del $VIP/$NETMASK brd + dev $NIC
RET=$?
if [ $RET = 0 ]; then
    exit 0
else
    echo "Failure to del IP Address"
    exit 1
fi
```

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

6.4 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 (node1). In the **Status** tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node1 is **Normal**.
When using DSR, perform packet capture and confirm that communication is being performed with the ip address of the client and the front-end IP address of the load balancer.
2. Change **Operation Mode** to **Verification Mode** from the WebManager pull-down menu.
3. In the **Status** tab on the Cluster WebUI, click the **Enable dummy failure** icon of azureppw1 of Monitors.
4. When the time specified for **Interval** elapses, the failover group (failover1) enters an error status and fails over to node2. In the **Status** tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node2 is **Normal**.
Also, confirm that access to the frontend IP and port of the Azure load balancer is normal after the failover.
When using DSR, perform packet capture and confirm that communication is being performed with the ip address of the client and the front-end IP address of the load balancer.

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.

Please refer the following for notes for EXPRESSCLUSTER on Azure:

EXPRESSCLUSTER X Getting Started Guide

- "Communication port number" in "Notes and Restrictions"

For an HA cluster using Azure DNS:

EXPRESSCLUSTER X Getting Started Guide

- "Azure DNS resources" in "Notes and Restrictions"
- "Setting up Azure DNS resources" in "*8. Notes*"

EXPRESSCLUSTER X Reference Guide

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

For an HA cluster using a load balancer:

EXPRESSCLUSTER X Getting Started Guide

- "Setting up Azure probe port resources" in "*8. Notes*"
- "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"

Maintenance for preserving Azure memory

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/linux/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.
- When changing **Shutdown Monitor Timeout** parameter on **Monitor** tab in **Cluster Properties** from the default value (Use Heartbeat Timeout), please set the parameter less than **Heartbeat Timeout**.

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"

- "Monitor tab"

Disk device name to be specified for EXPRESSCLUSTER

In the Microsoft Azure environment, a device name (e.g., /dev/sdb1) may be changed during the operation.

Therefore, it is recommended to use the symbolic link set by the Azure feature or to specify the logical volume of LVM, for the device name to be set for mirror disk resources.

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

Note on using Azure DNS

To set up EXPRESSCLUSTER to work with Microsoft Azure, a Microsoft Azure organizational account is required.

An account other than the organizational account cannot be used because an interactive login is required when executing the Azure CLI.

Security settings when creating a virtual machine on Azure

Secure Boot is enabled by default security settings when creating a virtual machine on Azure.

Therefore, when using EXPRESSCLUSTER, please create a virtual machine with Secure Boot disabled.

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.
- Linux is a registered trademark of Linus Torvalds in the United States and other countries.
- 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 15, 2024	New Guide
2nd	Nov 29, 2024	Corrected typographical errors and other mistakes.

© Copyright NEC Corporation 2024. All rights reserved.