

EXPRESSCLUSTER® X 4.0

HA Cluster Configuration Guide for Microsoft Azure (Linux)

March 28, 2019
3rd Edition



Revision History

Edition	Revised Date	Description
1st	Apr 17, 2018	New guide
2nd	Jul 26, 2018	Add notes on Heartbeat Timeout following memory preserving maintenance of Azure. 7.1.2 Notes on EXPRESSCLUSTER 7.2.2 Notes on EXPRESSCLUSTER
3rd	Mar 28, 2019	Modify the following "Configuring virtual machines". 3.2 Configuring Microsoft Azure 4.2 Configuring Microsoft Azure 5.2 Configuring Microsoft Azure

© Copyright NEC Corporation 2018. All rights reserved.

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.

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.

Contents

Preface	V
Who Should Use This Guide	v
Scope of application	v
Conventions	vii
Contacting NEC	viii
Chapter 1 Overview	9
1.1 Functional overview	9
1.2 Basic configuration	10
1.3 Network partition resolution	17
1.4 Differences between on-premises and Microsoft Azure	19
Chapter 2 Operating Environments	24
2.1 HA cluster using Azure DNS	24
2.2 HA cluster using a load balancer	24
Chapter 3 Cluster Creation Procedure (for an HA Cluster Using Azure DNS)	25
3.1 Creation example	25
3.2 Configuring Microsoft Azure	28
3.3 Configuring the EXPRESSCLUSTER settings	55
3.4 Verifying the created environment	82
Chapter 4 Cluster Creation Procedure (for an HA Cluster Using an Internet Facing Load Balancer)	83
4.1 Creation example	83
4.2 Configuring Microsoft Azure	86
4.3 Configuring the EXPRESSCLUSTER settings	120
4.4 Verifying the created environment	149
Chapter 5 Cluster Creation Procedure (for an HA Cluster Using an Internal Load Balancer)	150
5.1 Creation example	150
5.2 Configuring Microsoft Azure	153
5.3 Configuring the EXPRESSCLUSTER settings	182
5.4 Verifying the created environment	194
Chapter 6 Error Messages	195
Chapter 7 Notes and Restrictions	196
7.1 HA cluster using Azure DNS	196
7.1.1 Notes on Microsoft Azure	196
7.1.2 Notes on EXPRESSCLUSTER	196
7.2 HA cluster using a load balancer	197
7.2.1 Notes on Microsoft Azure	197
7.2.2 Notes on EXPRESSCLUSTER	197

Preface

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.

Scope of application

This guide covers the following product versions.

- EXPRESSCLUSTER X 4.0 for Linux (Internal version: 4.0.0-1)
- CentOS 6.9
- CentOS 7.4
- Microsoft Azure portal: Environment as of February 15, 2018
- Azure CLI 1.0 (for CentOS 6.9)
- Azure CLI 2.0 (for CentOS 7.4)

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

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

How This Guide is Organized

Chapter 1	Overview: Describes the functional overview.
Chapter 2	Operating Environments: Describes the tested operating environment of this function.
Chapter 3	Cluster Creation Procedure: Describes the procedure to create an HA cluster using Azure DNS.
Chapter 4	Cluster Creation Procedure: Describes the procedure to create an HA cluster using an Internet facing load balancer.
Chapter 5	Cluster Creation Procedure: Describes the procedure to create an HA cluster using an internal load balancer.
Chapter 6	Error Messages: Describes the error messages and solutions.
Chapter 7	Notes and Restrictions: Describes the notes and restrictions on creating and operating a cluster.

EXPRESSCLUSTER X Documentation Set

The EXPRESSCLUSTER manuals consist of the four guides below. 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, supported operating environments, updates, and known problems.

EXPRESSCLUSTER X Installation and Configuration Guide

This guide is intended for system engineers who install cluster systems using EXPRESSCLUSTER and for system administrators who maintain and operate installed cluster systems, and it describes requirements from for installing a cluster system using EXPRESSCLUSTER to for preparing to start operation. This guide follows the actual procedure for installing a cluster system to describe how to design a cluster system using EXPRESSCLUSTER, how to install and set up EXPRESSCLUSTER, how to check the system after setting it up, and how to evaluate the system before starting operation.

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, maintenance-related information, and troubleshooting. The guide is supplement to the *EXPRESSCLUSTER X Installation and Configuration Guide*.

EXPRESSCLUSTER X Integrated WebManager Administrator's Guide

This guide is intended for system administrators who manage cluster system using EXPRESSCLUSTER with EXPRESSCLUSTER Integrated WebManager and for system engineers who introduce the Integrated WebManager. In this guide, details on required items for introducing the cluster system using the Integrated WebManager are explained in accordance with the actual procedures.

Conventions

In this guide, **Note**, **Important**, **Related Information** are used as follows:

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

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

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

The following conventions are used in this guide.

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

Contacting NEC

For the latest product information, visit our website below:

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

Chapter 1 Overview

1.1 Functional overview

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.

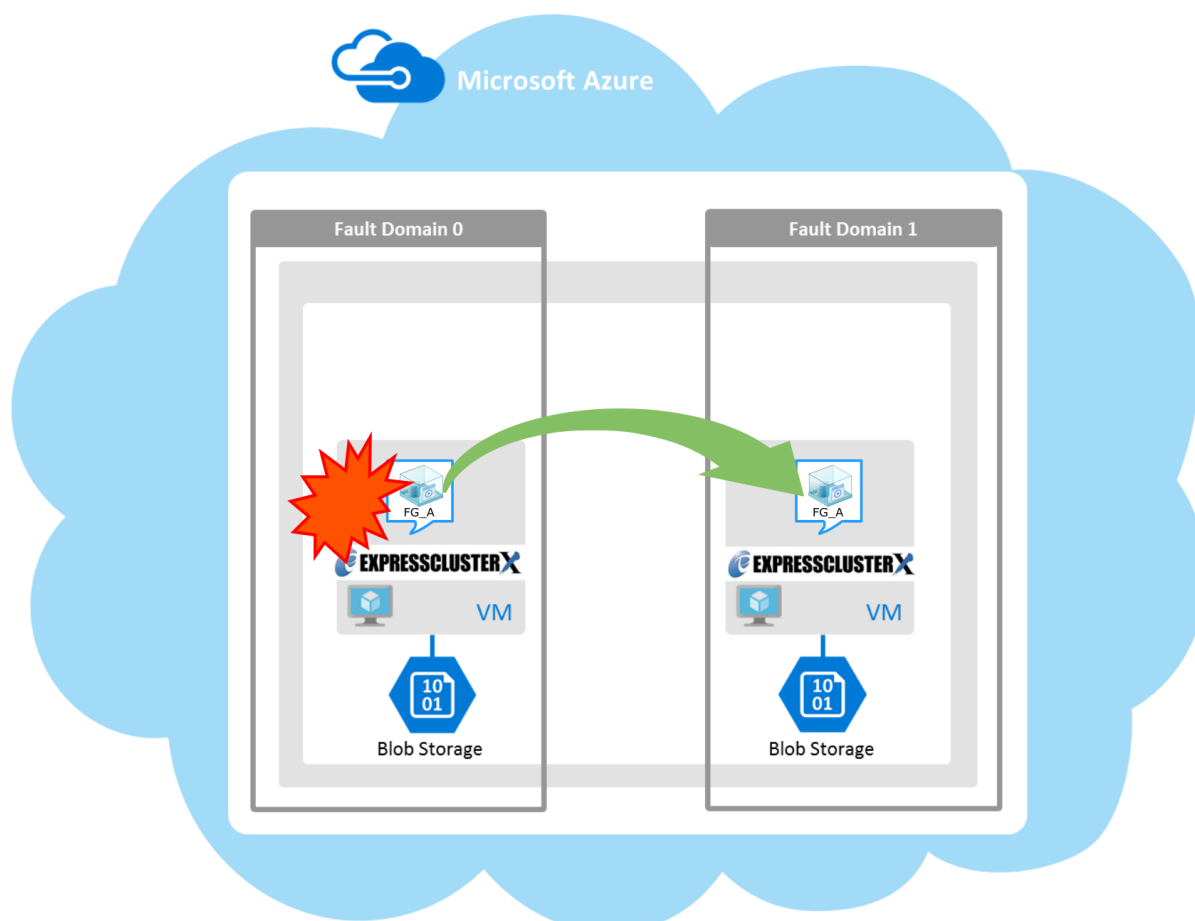


Figure 1-1 HA Cluster on a Cloud Service (Using Azure DNS)

Operational availability can be increased by clustering virtual machines (VMs in Figure 1-1) 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>

1.2 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 (A load balancer needs to be installed)	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/>

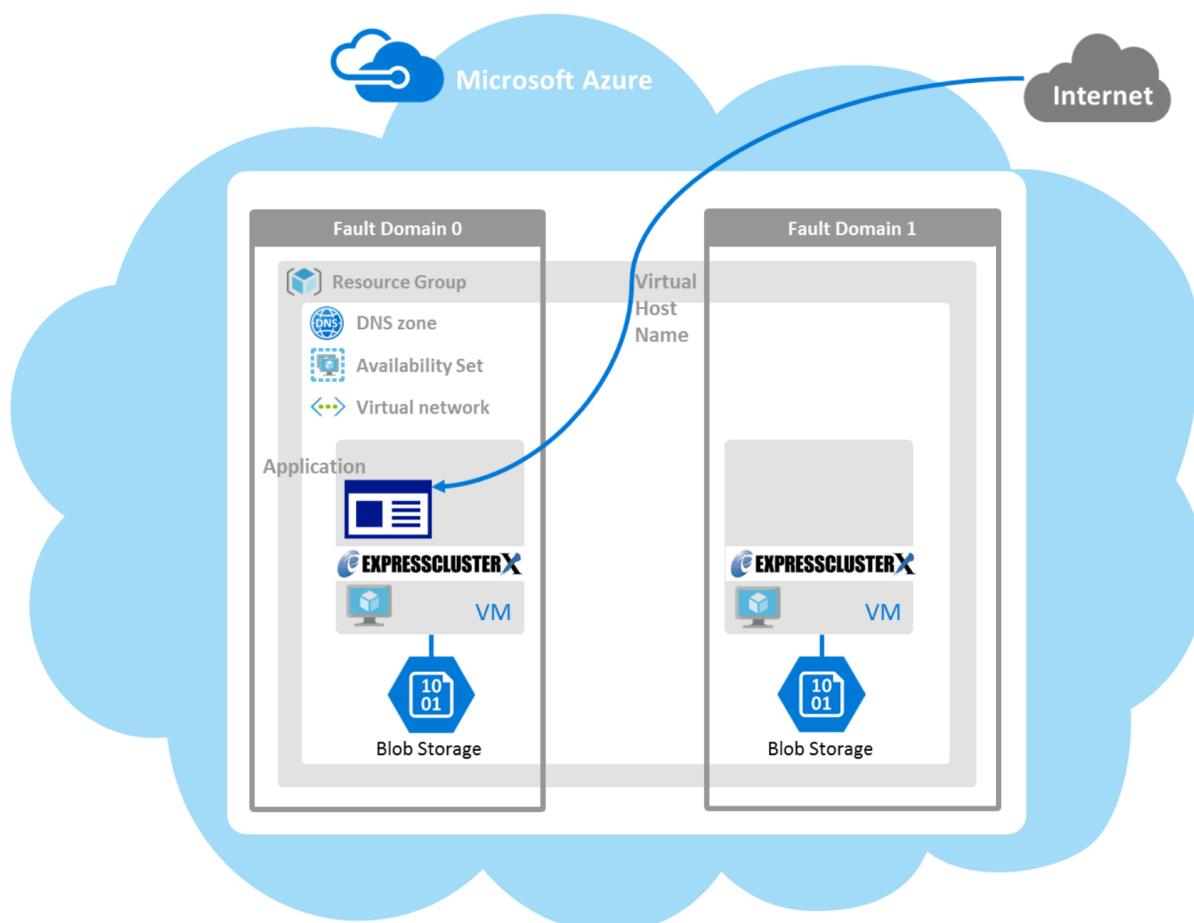


Figure 1-2 HA Cluster Using Azure DNS

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 1-2 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 record sets and DNS A records of the Azure DNS zone to find an IP address according to the DNS name.	Required
Azure DNS monitor resource	Checks the existence of a record set and monitors whether the name resolution is available in Azure DNS.	Required
IP monitor resource	Monitors whether communication with the Microsoft Azure Service Management API is possible, and also monitors health of communication with an external network.	When an Internet facing load balancer is used, required to monitor communication between clusters that are configured with virtual machines, and also to monitor health of communication with an internal network.
Custom monitor resource	Monitors communication between clusters that are configured with virtual machines, and also monitors health of communication with an internal network.	When an Internet facing load balancer is used, required to monitor whether communication with the Microsoft Azure Service Management API is possible, and also to monitor health of communication with an external network.
Multi-target monitor resource	Monitors the statuses of both the IP monitor resource and custom monitor resource. If the statuses of both monitor resources are abnormal, a script in which a process for network partition resolution (NP resolution) is described is executed.	When an Internet facing 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

For details about other resources and monitor resources, see the following:

- Chapter 4, "Group resource details" in the *Reference Guide*.
- Chapter 5, "Monitor resource details" in the *Reference Guide*.

HA cluster using a load balancer

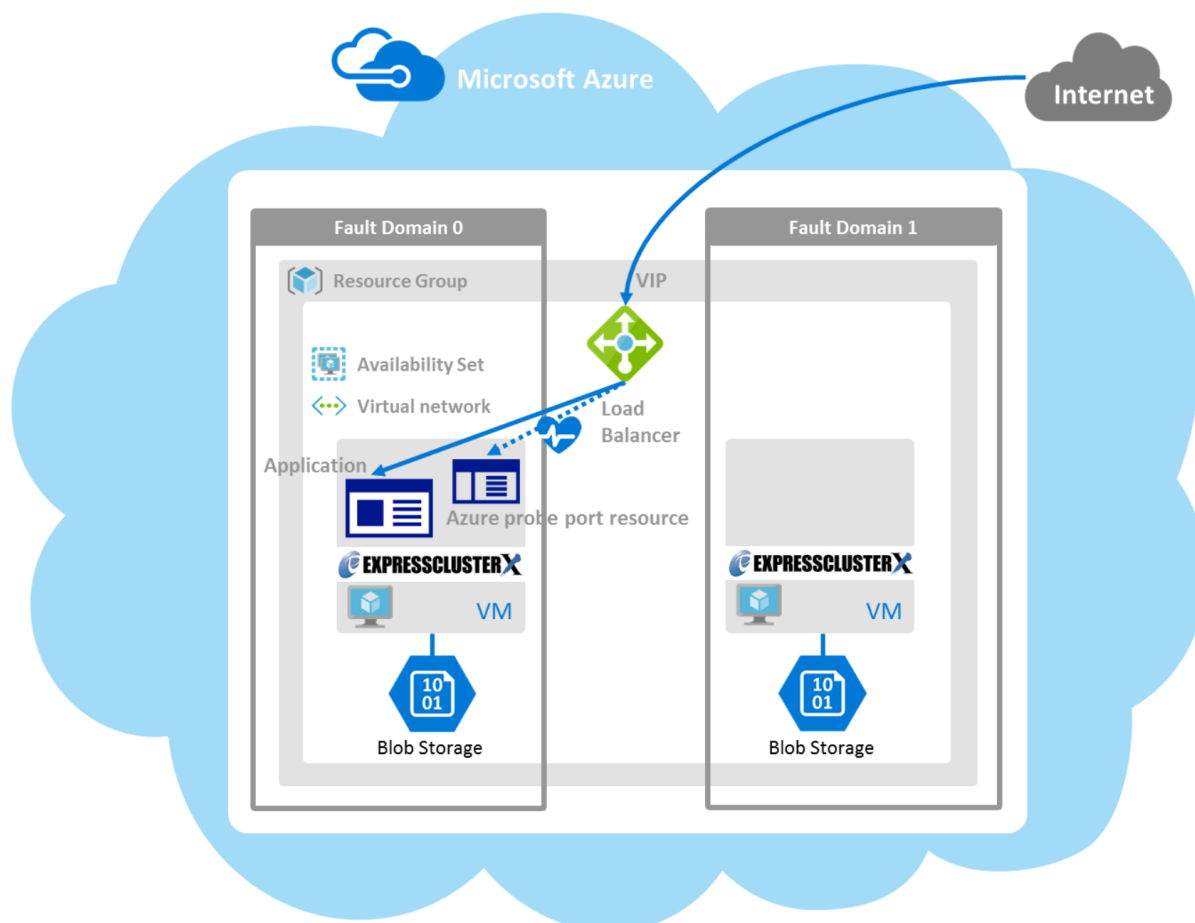


Figure 1-3 HA Cluster Using an Internet Facing Load Balancer

A client application can connect a virtual machine on an availability set in a Microsoft Azure environment to a cluster node by using a public virtual IP address (hereinafter referred to as VIP). By using a VIP, 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 1-3 is accessed by specifying a global IP address of the Microsoft Azure Load Balancer (Load Balancer in Figure 1-3).

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.

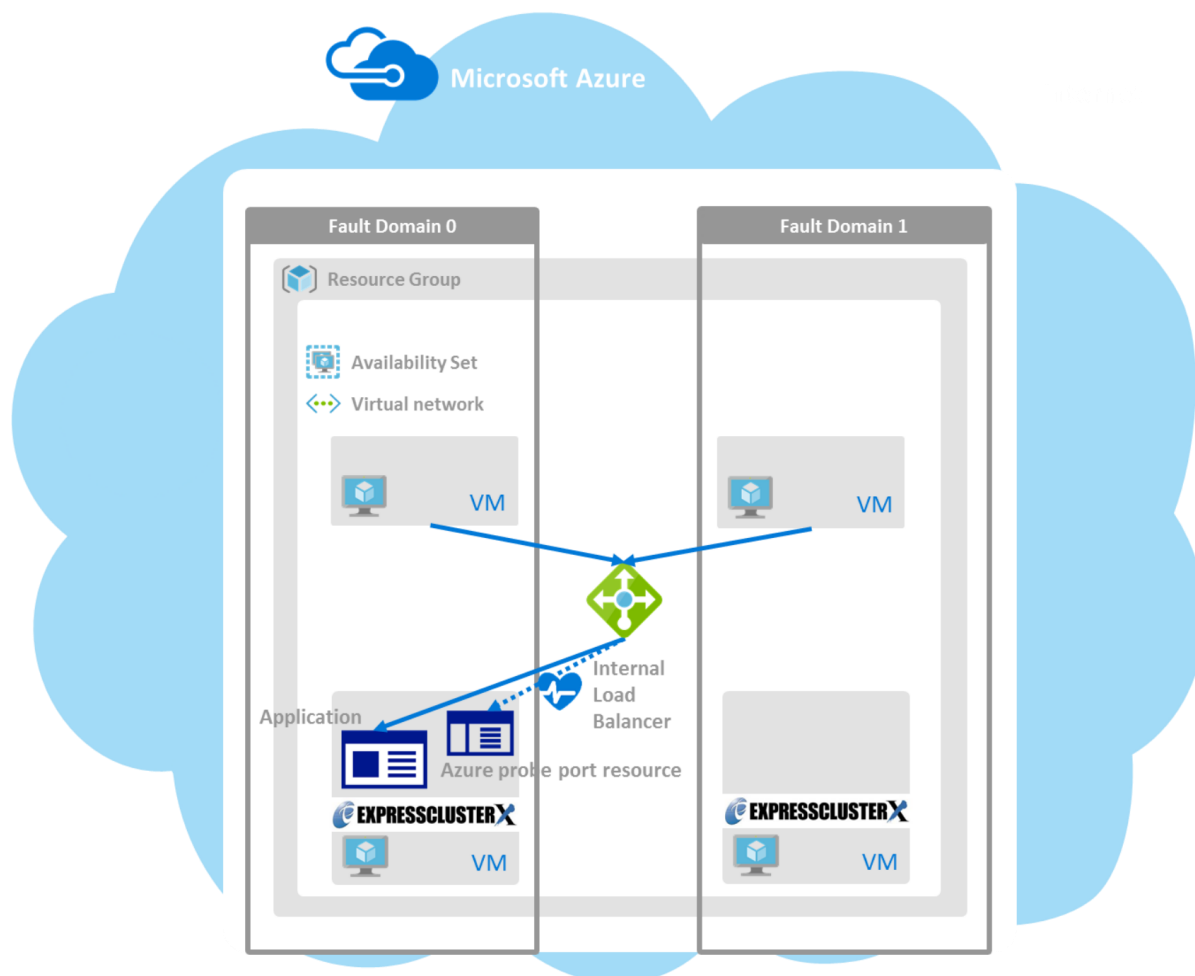


Figure 1-4 HA Cluster Using the Internal Load Balancer

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	Internet facing load balancer	See " Chapter 4 Cluster Creation Procedure (for an HA Cluster Using an Internet Facing Load Balancer)" in this guide.
Publishing operations within the Microsoft Azure network	Internal load balancer (ILB)	See " Chapter 5 Cluster Creation Procedure (for an HA Cluster Using an Internal Load Balancer)" in this guide.

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

Resource or monitor resource type	Description	Setting
Azure probe port resource	Provides a mechanism to wait for alive monitoring from a load balancer on a specific port of a node in which operations are running.	Required
Azure probe port monitor resource	Performs alive monitoring of a probe port control process, which starts upon activation of the Azure probe port resource, for a node in which the Azure probe port resource is running.	Required
Azure load balance monitor resource	Monitors whether a port with the same number as a probe port is open for a node in which the Azure probe port resource is not running.	Required
IP monitor resource	Monitors whether communication with the Microsoft Azure Service Management API is possible, and also monitors health of communication with an external network.	When an Internet facing load balancer is used, required to monitor communication between clusters that are configured with virtual machines, and also to monitor health of communication with an external network.
Custom monitor resource	Monitors communication between clusters that are configured with virtual machines, and also monitors health of communication with an internal network.	When an Internet facing load balancer is used, required to monitor whether communication with the Microsoft Azure Service Management API is possible, and also to monitor health of communication with an external network.
Multi-target monitor resource	Monitors the statuses of both the IP monitor resource and custom monitor resource. If the statuses of both monitor resources are abnormal, a script in which a process for network partition resolution (NP resolution) is described is executed.	When an Internet facing 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

For details about other resources and monitor resources, see the following:

- Chapter 4, "Group resource details" in the *Reference Guide*.
- Chapter 5, "Monitor resource details" in the *Reference Guide*.

1.3 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	<ul style="list-style-type: none"> Custom monitor resource clpazure_port_checker command
	each cluster server	Ping	<ul style="list-style-type: none"> IP monitor resource
Inside the Microsoft Azure Virtual network	Servers, excluding a cluster server, that exist within the Microsoft Azure network(*)	Ping	<ul style="list-style-type: none"> PING network partition resolution resource

For details about NP resolution, see the following:

- Chapter 7, “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).

How to judge the network partition status

EXPRESSCLUSTER provides the clpazure_port_checker command to judge the network partition 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 "3.3 Configuring the EXPRESSCLUSTER settings" and "5.3 Configuring the EXPRESSCLUSTER settings."

Options	-h <i>hostname</i>	Specify the determining server as <i>hostname</i> (by using an FQDN name or IP address). This option cannot be omitted.
	-p <i>port</i>	Specify the determining port number as <i>port</i> (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)

1.4 Differences between on-premises and Microsoft Azure

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

Function	On-premise	Microsoft Azure
Creating a shared disk type cluster	Y	N
Creating a mirror disk type cluster	Y	Y
Creating a hybrid disk type cluster	Y	N
Using the floating IP resource	Y	N
Using the virtual IP resource	Y	N
Using the Azure probe port resource	N	Y
Using the Azure DNS resource	N	Y

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.

Step No.	Procedure	On-premise	Microsoft Azure
Before installing EXPRESSCLUSTER			
1	Creating a resource group	Not required	See "3.2 Configuring Microsoft Azure" in this guide.
2	Creating a virtual network	Not required	See "3.2 Configuring Microsoft Azure" in this guide.
3	Creating a virtual machine	Not required	See "3.2 Configuring Microsoft Azure" in this guide.
4	Setting a private IP address	Not required	See "3.2 Configuring Microsoft Azure" in this guide.
5	Adding Blob storage	Not required	See "3.2 Configuring Microsoft Azure" in this guide.
6	Creating a DNS zone	Not required	See "3.2 Configuring Microsoft Azure" in this guide.
7	Setting up the DNS server	See the manual provided with an OS or DNS server such as <i>Red Hat Enterprise Linux 7 Network Guide</i> .	Not required
8	Setting a partition for the mirror disk resource	See the following: <ul style="list-style-type: none"> "Settings after configuring hardware" in Chapter 1, "Determining a system configuration" in the <i>Installation and Configuration Guide</i> "Understanding mirror disk resources" in Chapter 4, "Group resource details" in the <i>Reference Guide</i>. 	See "3.2 Configuring Microsoft Azure" in this guide.

Step No.	Procedure	On-premise	Microsoft Azure
9	Adjusting the OS startup time	See "Settings after configuring hardware" in Chapter 1, "Determining a system configuration" in the <i>Installation and Configuration Guide</i> .	Same as "On-premise"
10	Checking the network setting		
11	Checking the root file system		
12	Checking the firewall setting		
13	Synchronizing the server time		
14	Checking the SELinux setting		
15	Installing the Azure CLI	Not required	See "3.2 Configuring Microsoft Azure" in this guide.
16	Registering the service principal	Not required	See "3.2 Configuring Microsoft Azure" in this guide.
17	Installing EXPRESSCLUSTER	See Chapter 3, "Installing EXPRESSCLUSTER" in the <i>Installation and Configuration Guide</i> .	Same as "On-premise"
After installing EXPRESSCLUSTER			
18	Registering the EXPRESSCLUSTER license	See Chapter 4, "Registering the license" in the <i>Installation and Configuration Guide</i> .	Same as "On-premise"
19	Creating a cluster: Setting the heartbeat method	See "Creating the configuration data of a 2-node cluster" in Chapter 5, "Creating the cluster configuration data" in the <i>Installation and Configuration Guide</i> .	The COM heartbeat, BMC heartbeat, and disk heartbeat cannot be used.
20	Creating a cluster: Setting the NP resolution processing	<p>The network partition resolution resource is used. See the following:</p> <ul style="list-style-type: none"> • "Creating the configuration data of a 2-node cluster" in Chapter 5, "Creating the cluster configuration data" in the <i>Installation and Configuration Guide</i>. • Chapter 7, "Network partition resolution resources details" in the <i>Reference Guide</i>. 	See "3.3 Configuring the EXPRESSCLUSTER settings" in this guide.
21	Creating a cluster: Creating a failover group and monitor resource	See "Creating the configuration data of a 2-node cluster" in Chapter 5, "Creating the cluster configuration data" in the <i>Installation and Configuration Guide</i> .	<p>In addition to the references for on-premises, see the following:</p> <ul style="list-style-type: none"> ➤ "Understanding Azure DNS resources" in Chapter 4, "Group resource details" in the <i>Reference Guide</i>. ➤ "Understanding Azure DNS monitor resources" in Chapter 5, "Monitor resource details" in the <i>Reference Guide</i>. ➤ "3.3 Configuring the EXPRESSCLUSTER settings" 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.

Step No.	Procedure	On-premise	Microsoft Azure
Before installing EXPRESSCLUSTER			
1	Creating a resource group	Not required	See either of the following depending on the load balancer to use: <ul style="list-style-type: none"> • "4.2 Configuring Microsoft Azure" in this guide • "5.2 Configuring Microsoft Azure" in this guide
2	Creating a virtual network	Not required	See either of the following depending on the load balancer to use: <ul style="list-style-type: none"> • "4.2 Configuring Microsoft Azure" in this guide • "5.2 Configuring Microsoft Azure" in this guide
3	Creating a virtual machine	Not required	See either of the following depending on the load balancer to use: <ul style="list-style-type: none"> • "4.2 Configuring Microsoft Azure" in this guide • "5.2 Configuring Microsoft Azure" in this guide
4	Setting a private IP address	Not required	See either of the following depending on the load balancer to use: <ul style="list-style-type: none"> • "4.2 Configuring Microsoft Azure" in this guide • "5.2 Configuring Microsoft Azure" in this guide
5	Adding Blob storage	Not required	See either of the following depending on the load balancer to use: <ul style="list-style-type: none"> • "4.2 Configuring Microsoft Azure" in this guide • "5.2 Configuring Microsoft Azure" in this guide
6	Setting a partition for the mirror disk resource	See the following: <ul style="list-style-type: none"> • "Settings after configuring hardware" in Chapter 1, "Determining a system configuration" in the <i>Installation and Configuration Guide</i>. • "Understanding mirror disk resources" in Chapter 4, "Group resource details" in the <i>Reference Guide</i>. 	See either of the following depending on the load balancer to use: <ul style="list-style-type: none"> • "4.2 Configuring Microsoft Azure" in this guide • "5.2 Configuring Microsoft Azure" in this guide
7	Creating and configuring a load balancer	Not required	See either of the following depending on the load balancer to use: <ul style="list-style-type: none"> • "4.2 Configuring Microsoft Azure" in this guide

Step No.	Procedure	On-premise	Microsoft Azure
			<ul style="list-style-type: none"> • "5.2 Configuring Microsoft Azure" in this guide
8	Setting the inbound security rules	Not required	See either of the following depending on the load balancer to use: <ul style="list-style-type: none"> • "4.2 Configuring Microsoft Azure" in this guide • "5.2 Configuring Microsoft Azure" in this guide
9	Adjusting the OS startup time	See "Settings after configuring hardware" in Chapter 1, "Determining a system configuration" in the <i>Installation and Configuration Guide</i> .	Same as "On-premise"
10	Checking the network setting		
11	Checking the root file system		
12	Checking the firewall setting		
13	Synchronizing the server time		
14	Checking the SELinux setting		
15	Installing EXPRESSCLUSTER	See Chapter 3, "Installing EXPRESSCLUSTER" in the <i>Installation and Configuration Guide</i> .	Same as "On-premise"
After installing EXPRESSCLUSTER			
16	Registering the EXPRESSCLUSTER license	See Chapter 4, "Registering the license" in the <i>Installation and Configuration Guide</i> .	Same as "On-premise"
17	Creating a cluster: Setting the heartbeat method	See "Creating the configuration data of a 2-node cluster" in Chapter 5, "Creating the cluster configuration data" in the <i>Installation and Configuration Guide</i> .	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: <ul style="list-style-type: none"> • "Creating the configuration data of a 2-node cluster" in Chapter 5, "Creating the cluster configuration data" in the <i>Installation and Configuration Guide</i>. • Chapter 7, "Network partition resolution resources details" in the <i>Reference Guide</i>. 	See either of the following depending on the load balancer to use: <ul style="list-style-type: none"> • See "4.3 Configuring the EXPRESSCLUSTER settings" in this guide. • See "5.3 Configuring the EXPRESSCLUSTER settings" in this guide.
19	Creating a cluster: Creating a failover group and monitor resource	See "Creating the configuration data of a 2-node cluster" in Chapter 5, "Creating the cluster configuration data" in the <i>Installation and Configuration Guide</i> .	See the following in addition to the description of "On-premise." <ul style="list-style-type: none"> • "Understanding Azure probe port resources" in Chapter 4, "Group resource details" in the <i>Reference Guide</i>. • "Understanding Azure probe port monitor resources" in Chapter 5, "Monitor resource

Step No.	Procedure	On-premise	Microsoft Azure
			<p>details" in the <i>Reference Guide</i>.</p> <ul style="list-style-type: none">• "Understanding Azure load balance monitor resources" in Chapter 5, "Monitor resource details" in the <i>Reference Guide</i>. <p>See either of the following depending on the load balancer to use:</p> <ul style="list-style-type: none">• See "4.3 Configuring the EXPRESSCLUSTER settings" in this guide.• See "5.3 Configuring the EXPRESSCLUSTER settings" in this guide.

Chapter 2 Operating Environments

2.1 HA cluster using Azure DNS

See the following:

- "Getting Started Guide" > "Chapter 3, Installation requirements for EXPRESSCLUSTER" > "Operation environment for Azure DNS resource and Azure DNS monitor resource"

x86_64

OS	CentOS 6.9 CentOS 7.4
EXPRESSCLUSTER	EXPRESSCLUSTER X 4.0 for Linux (Internal version: 4.0.0-1)
Microsoft Azure deployment model	Resource Manager
Location	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 1.0 (for CentOS 6.9) Azure CLI 2.0 (for CentOS 7.4)
Python	Not required because the Azure CLI 1.0 is used (for CentOS 6.9) 2.7 (for CentOS 7.4)

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, please use Azure CLI 1.0 in environment installed Python 2.6 or earlier.

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

Microsoft Azure document:

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

Python is bundled with Linux OS.

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/>

2.2 HA cluster using a load balancer

See the following:

- "Operation environment for Azure probe port resource, Azure probe port monitor resource, Azure load balance monitor resource" in Chapter 3, "Installation requirements for EXPRESSCLUSTER" in the *Getting Started Guide*.

Chapter 3 Cluster Creation Procedure (for an HA Cluster Using Azure DNS)

3.1 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	
Name	Vnet1
Resource group location	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 name	TestGroup1
Location	Japan East
DNS zone setting	
Name	cluster1.zone
Resource group	TestGroup1
Resource group location	Japan East
Record set	test-record1

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

Microsoft Azure settings (specify to each of node1 and node2)		
Setting item	Setting value	
	node1	node2
Virtual machine setting		
VM disk type	HDD	
User name	testlogin	
Password	PassWord_123	
Resource group name	TestGroup1	
Location	Japan East	
Storage account setting		
Name	clstorageacc1	
Performance	Standard	
Replication	Locally-redundant storage (LRS)	
Network security group setting		
Name	NetSecGroup1	
Availability set setting		
Name	AvailabilitySet1	
Update domains	5	
Fault domains	3	
Diagnostics storage account setting		
Name	clstorageaccdiag1	
Performance	Standard	
Replication	Locally-redundant storage (LRS)	
IP configuration setting		

Setting item	Setting value	
	node1	node2
IP address	10.5.0.110	10.5.0.111
Blob storage setting		
Name	Node1Blob	Node2Blob
Source type	New (empty disk)	
Account type	Standard (HDD)	
Size	20	

- EXPRESSCLUSTER settings (cluster properties)

Setting item	Setting value	
	node1	node2
Cluster Name	Cluster1	
Server Name	node1	node2
Timeout Tab: Heartbeat Timeout	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
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	http://azure-test
	Tenant ID	xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
	File Path of Service Principal	/root/examplecert.pem
	Thumbprint of Service Principal	xx
	Azure CLI File Path	/usr/bin/az

- EXPRESSCLUSTER settings (monitor resource)

Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	-	-
Azure DNS monitor resource	Name	azurednsw1
Custom monitor resource	Name	genw1
	Script created with this product	On
	Monitor Type	Synchronous

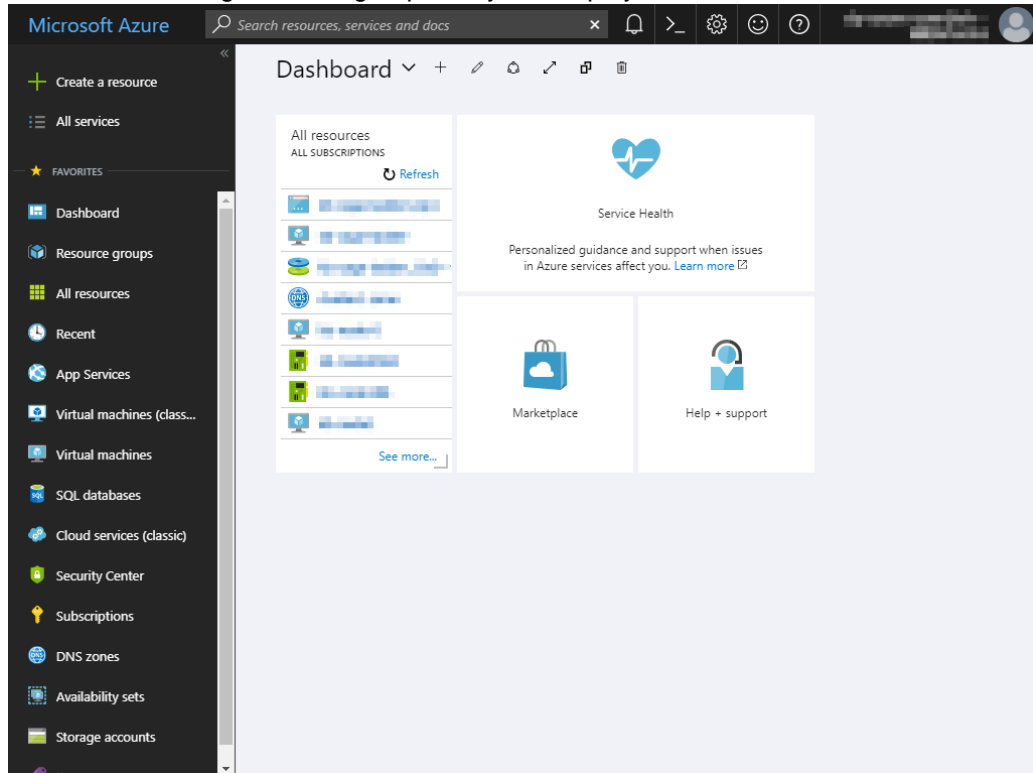
Monitor resource name	Setting item	Setting value
	Normal Return Value	0
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
IP monitor resource	Name	ipw1
	Server to monitor	node1
	IP Address	10.5.0.111
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
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

3.2 Configuring Microsoft Azure

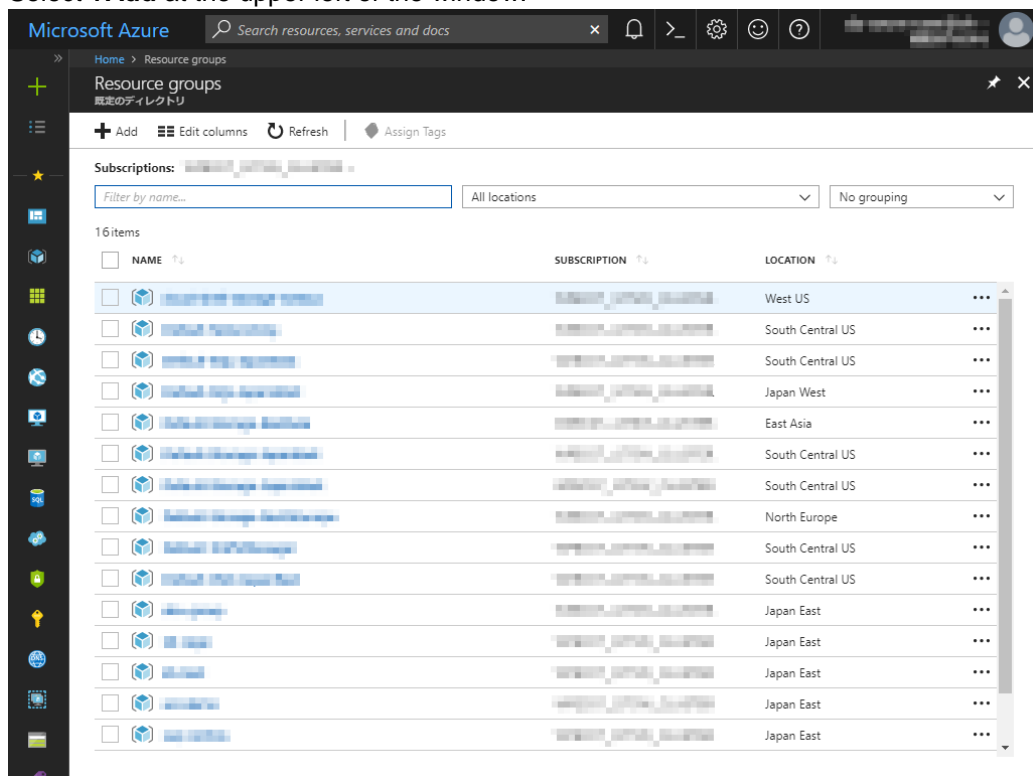
1) Creating a resource group

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

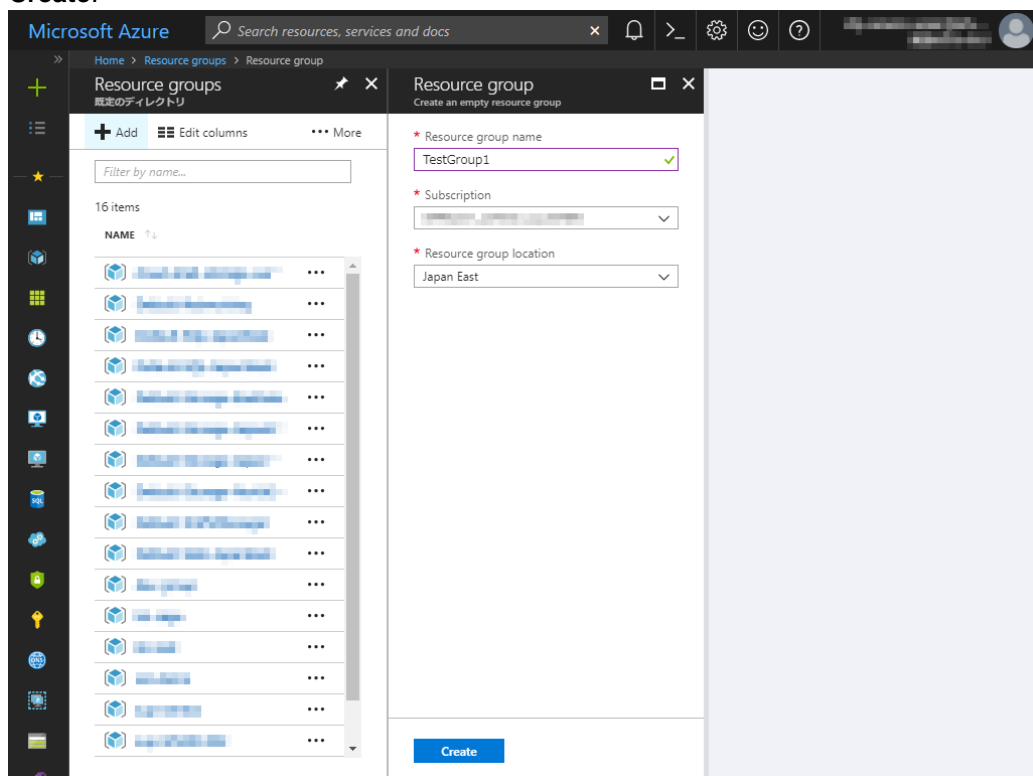
1. Select **Resource groups** or the resource group icon in the menu on the left side of the window. If there are existing resource groups, they are displayed in a list.



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



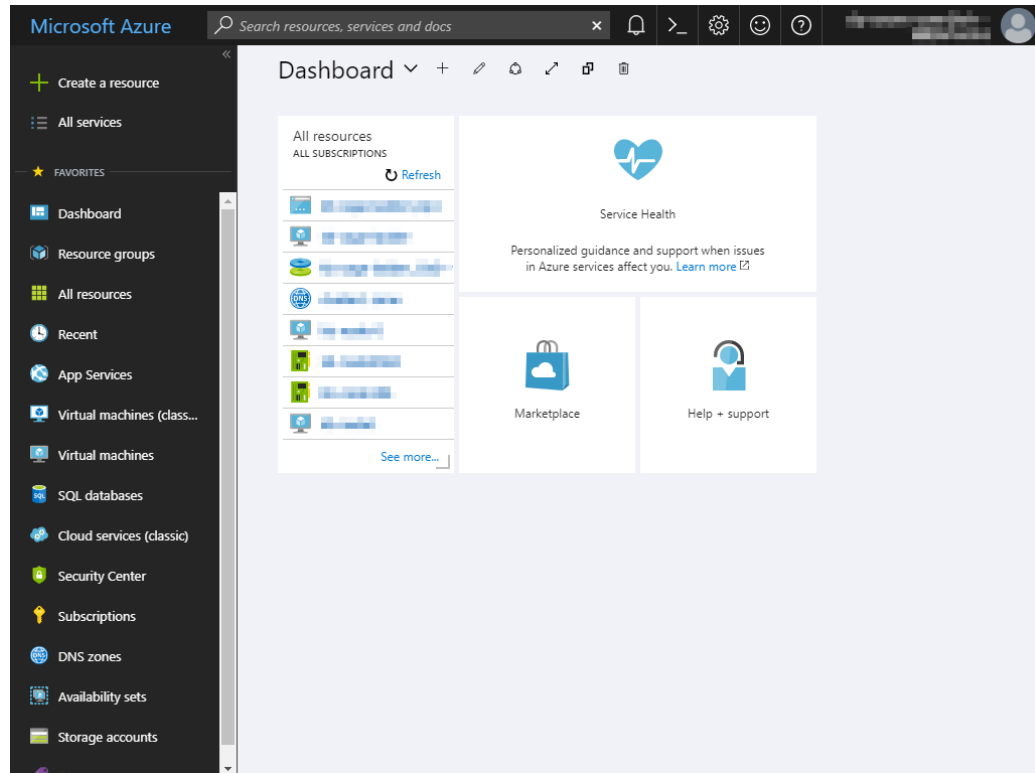
3. Specify **Resource group name**, **Subscription**, and **Resource group location**, and click **Create**.



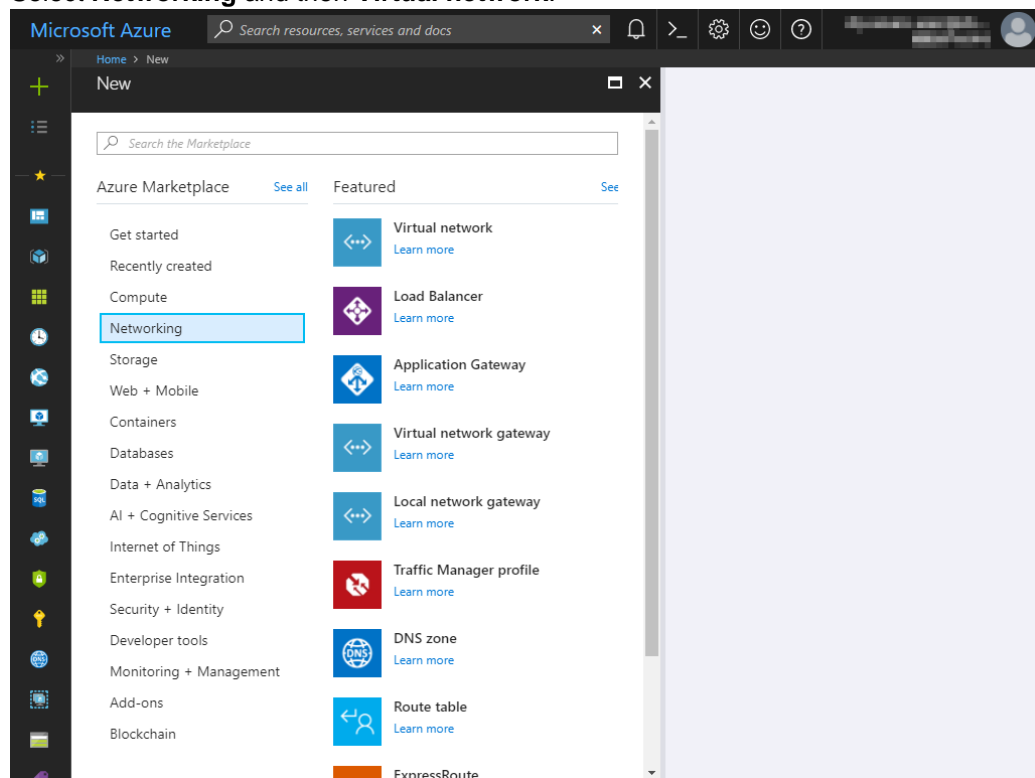
2) Creating a virtual network

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

1. Select **+Create a resource** or the **+** icon in the menu on the left side of the window.



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



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

The screenshot shows the 'Create virtual network' form in the Microsoft Azure portal. The form is titled 'Create virtual network' and is located under the 'Home > New > Create virtual network' breadcrumb. The form fields are as follows:

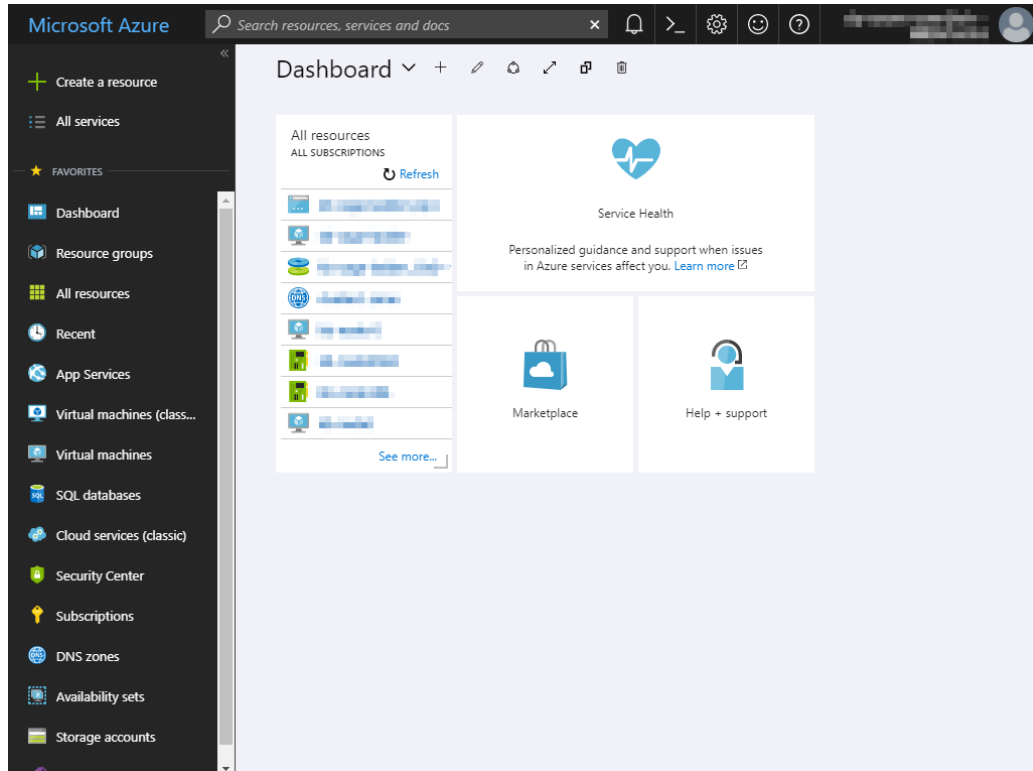
- Name:** Vnet1 (with a green checkmark)
- Address space:** 10.5.0.0/24 (with a green checkmark). Below the input, it says '10.5.0.0 - 10.5.0.255 (256 addresses)'.
- Subscription:** A dropdown menu showing a blurred subscription name.
- Resource group:** ☐ Create new ☒ Use existing. Below, a dropdown menu shows 'TestGroup1'.
- Location:** A dropdown menu showing 'Japan East'.
- Subnet:**
 - Name:** Vnet1-1 (with a green checkmark)
 - Address range:** 10.5.0.0/24 (with a green checkmark). Below the input, it says '10.5.0.0 - 10.5.0.255 (256 addresses)'.
- Service endpoints:** ☒ Disabled ☐ Enabled
- Pin to dashboard:** ☐
- Create:** A blue button.
- Automation options:** A link.

3) Creating a virtual machine

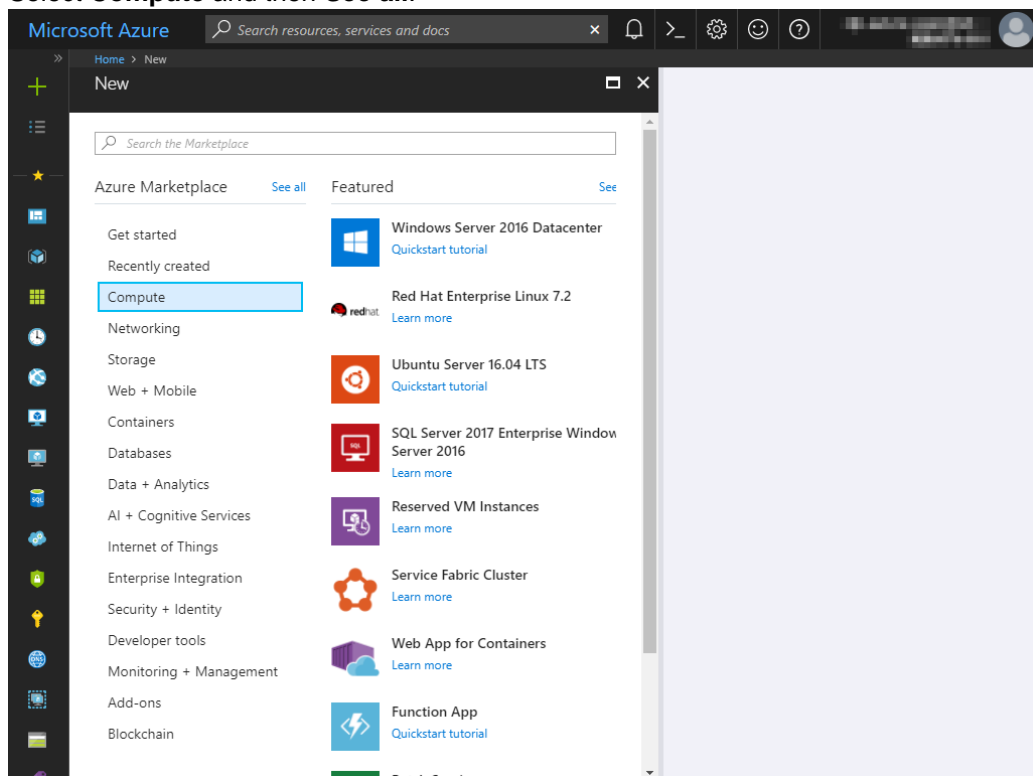
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create virtual machines and disks following the steps below.

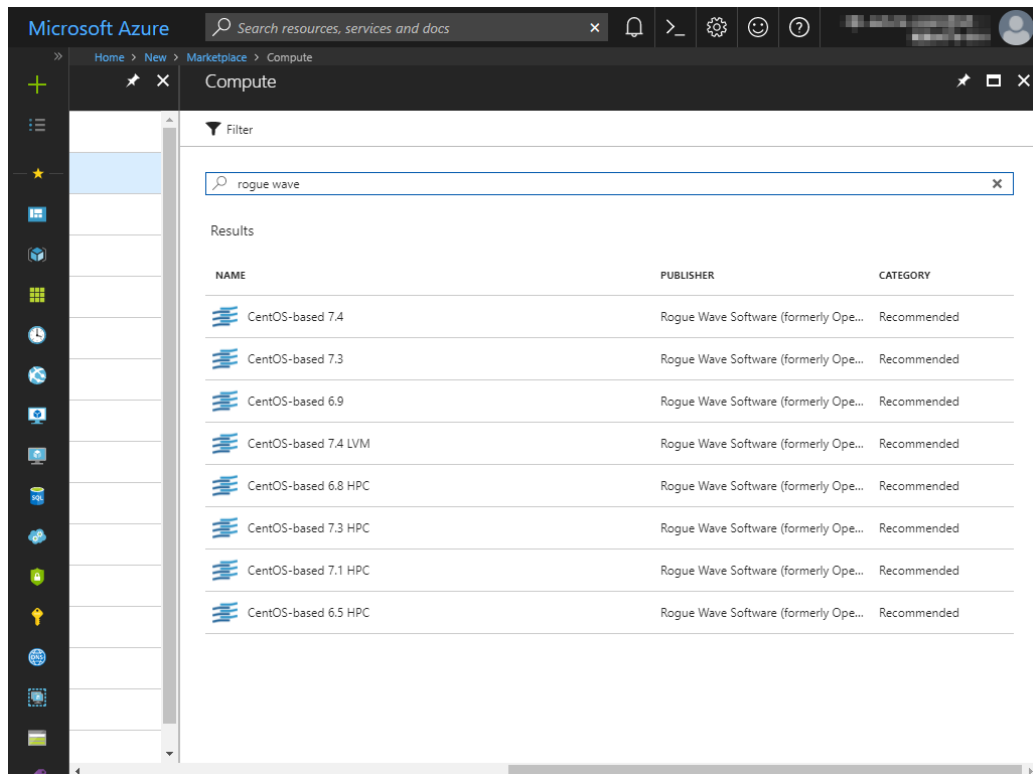
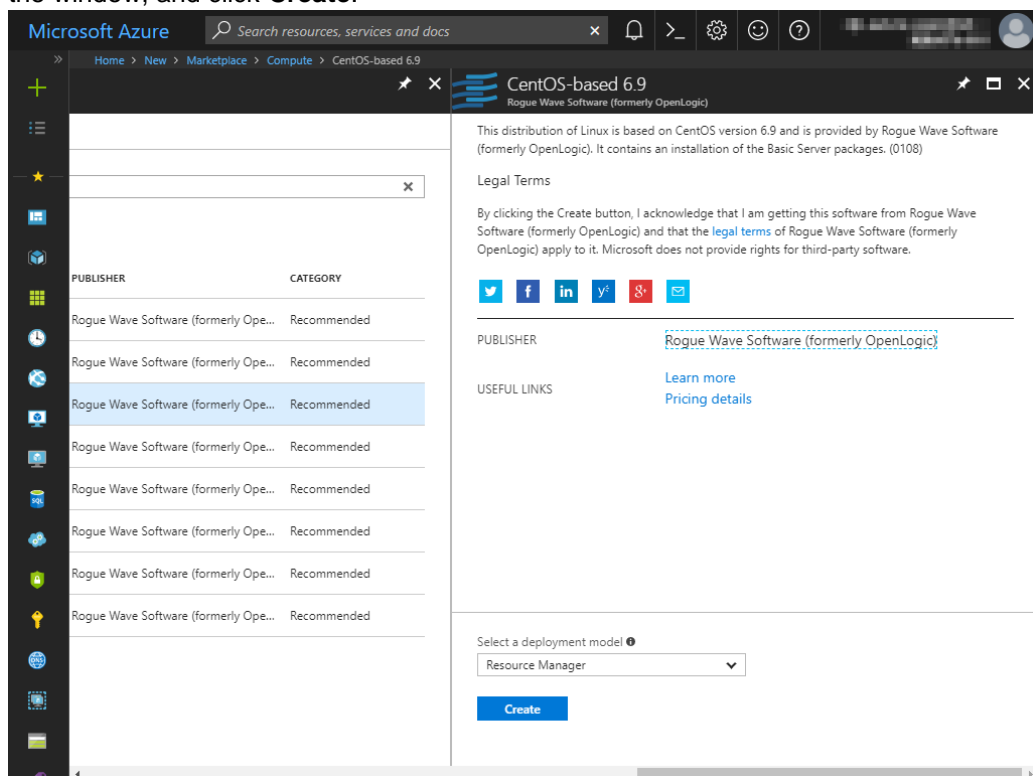
Create as many virtual machines as required to create a cluster. Create node1 and then node2.

1. Select **+Create a resource** or the **+** icon in the menu on the left side of the window.



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



3. Select **CentOS-based 6.9** or **CentOS-based 7.4**.4. Confirm that **Resource Manager** is selected for **Select a deployment model** at the bottom of the window, and click **Create**.

- The **Basics** blade is displayed. Specify **Name**, **VM disk type**, **User name**, **Password**, **Confirm password**, **Subscription**, **Resource group name**, and **Location**, and click **OK**. For **Name**, specify node1 for node1 and node2 for node2.

Microsoft Azure Search resources, services and docs

Home > New > Marketplace > Compute > CentOS-based 6.9 > Create virtual machine > Basics

Create virtual machine Basics

- Basics Configure basic settings
- Size Choose virtual machine size
- Settings Configure optional features
- Summary CentOS-based 6.9

* Name node1 ✓

VM disk type HDD

* User name testlogin

* Authentication type SSH public key Password

* Password

* Confirm password

Subscription

* Resource group Create new Use existing TestGroup1

* Location Japan East

OK

- The **Choose a size** blade is displayed. Select the size appropriate for the usage purpose of the virtual machines from the list and click **Select**. In this guide, **A1 Standard** is selected.

Microsoft Azure Search resources, services and docs

Home > New > Marketplace > Compute > CentOS-based 6.9 > Create virtual machine > Choose a size

Create virtual machine Choose a size

Browse the available sizes and their features

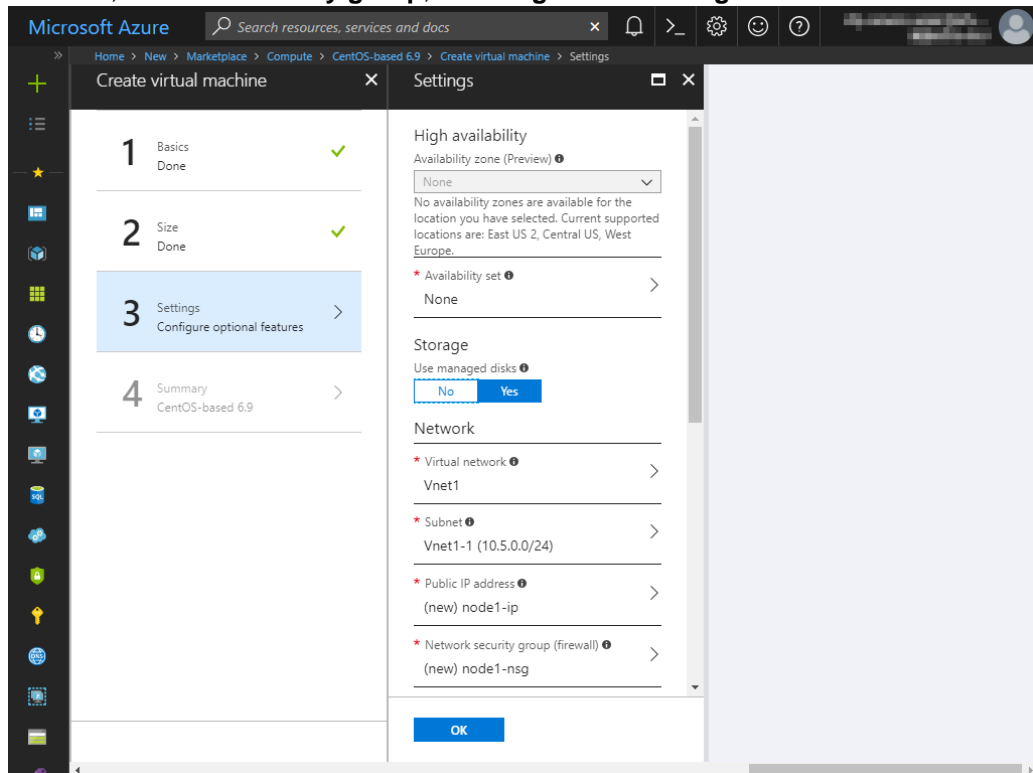
Supported disk type HDD Minimum vCPUs 1 Minimum memory (GiB) 0

★ Recommended | View all

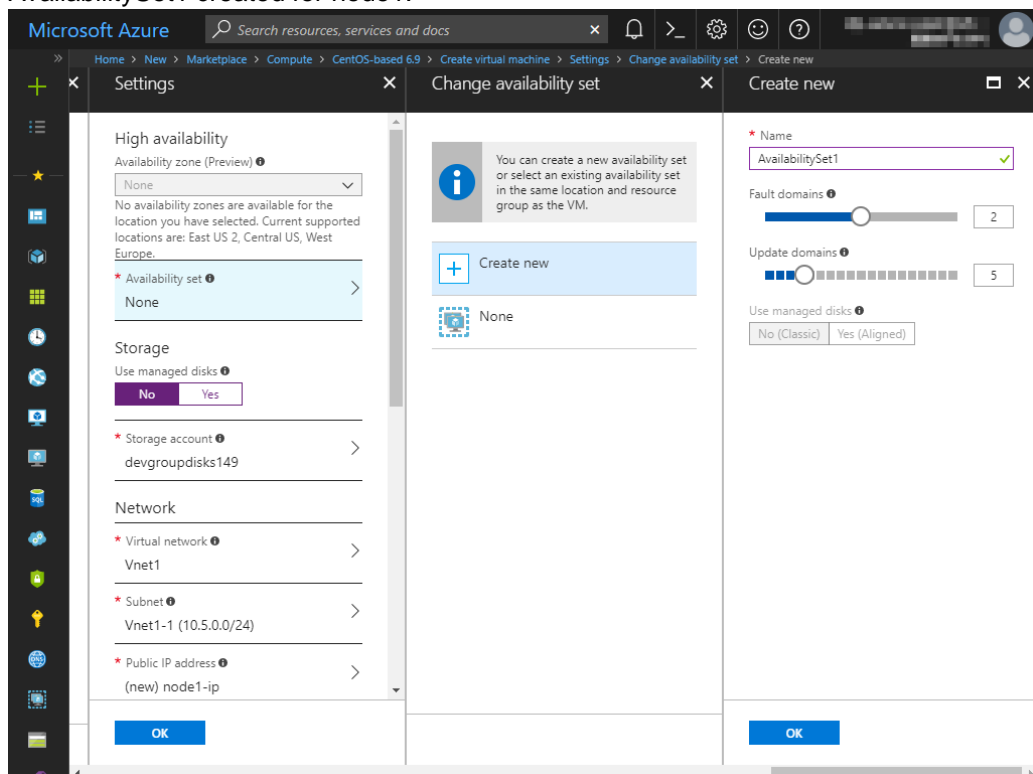
D1_V2 Standard	D1 Standard	A1 Standard
1 vCPU	1 vCPU	1 vCPU
3.5 GB	3.5 GB	1.75 GB
4 Data disks	4 Data disks	2 Data disks
2x500 Max IOPS	2x500 Max IOPS	2x500 Max IOPS
50 GB Local SSD	50 GB Local SSD	Load balancing
Load balancing	Load balancing	
7,015.92 JPY/MONTH (ESTIMATED)	7,343.28 JPY/MONTH (ESTIMATED)	3,935.76 JPY/MONTH (ESTIMATED)

Select

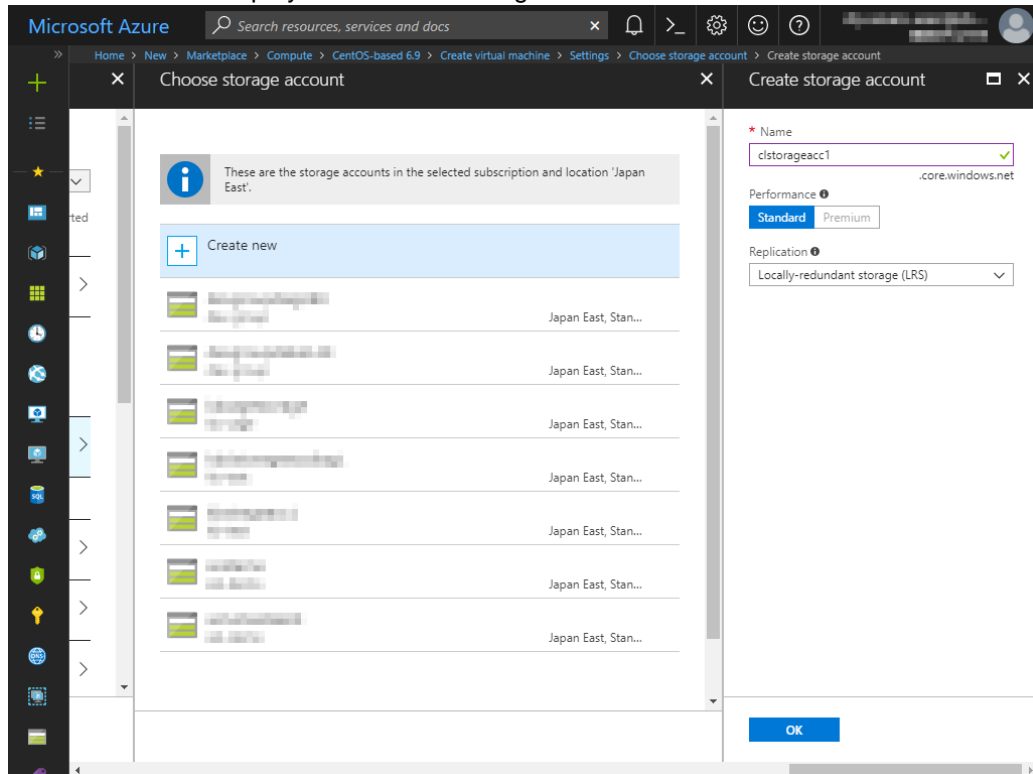
7. The **Settings** blade is displayed. Specify **Availability set**, **Storage account**, **Public IP address**, **Network security group**, and **Diagnostics storage account**.



8. Select **No** for **Use managed disks** for **Storage**.
9. Return to the **Settings** blade and select **Availability set**. For node1, the **Change availability set** blade is displayed. Select **Create new**. Specify **Name**, **Fault domains**, and **Update domains**, and click **OK**. For node2, the **Change availability set** blade is displayed. Select AvailabilitySet1 created for node1.

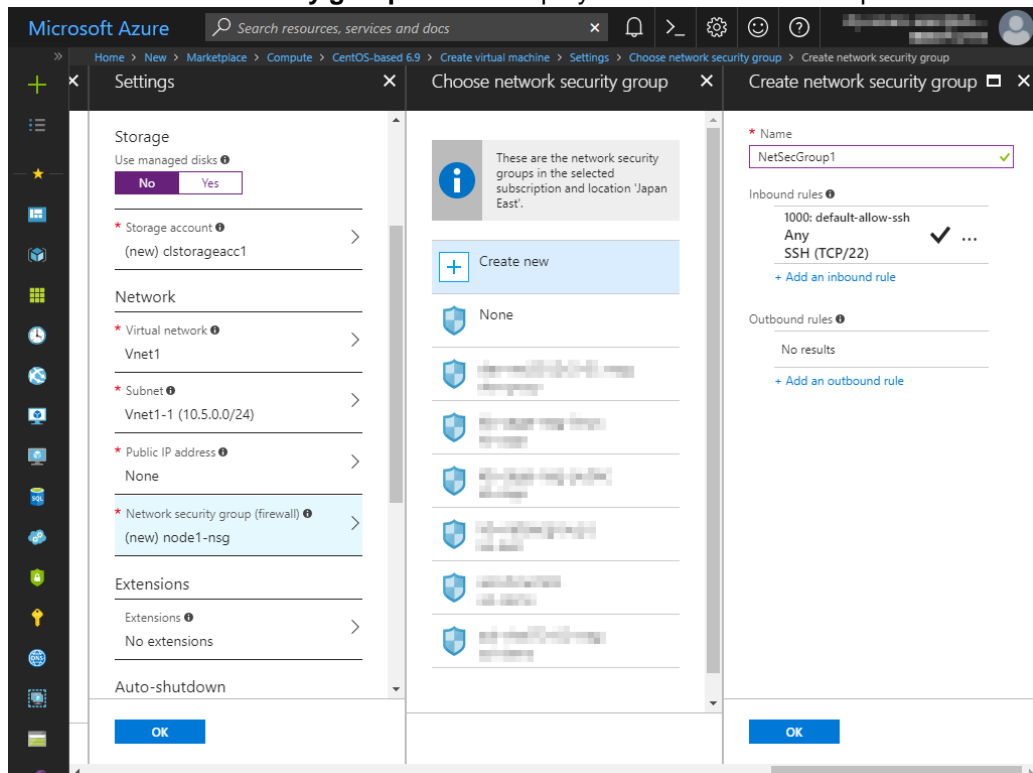


10. Select **Storage account**. For node1, the **Create storage account** blade is displayed. Specify **Name**, **Performance**, and **Replication**, and click **OK**. For node2, the **Choose storage account** blade is displayed. Select "clstorageacc1" created for node1.

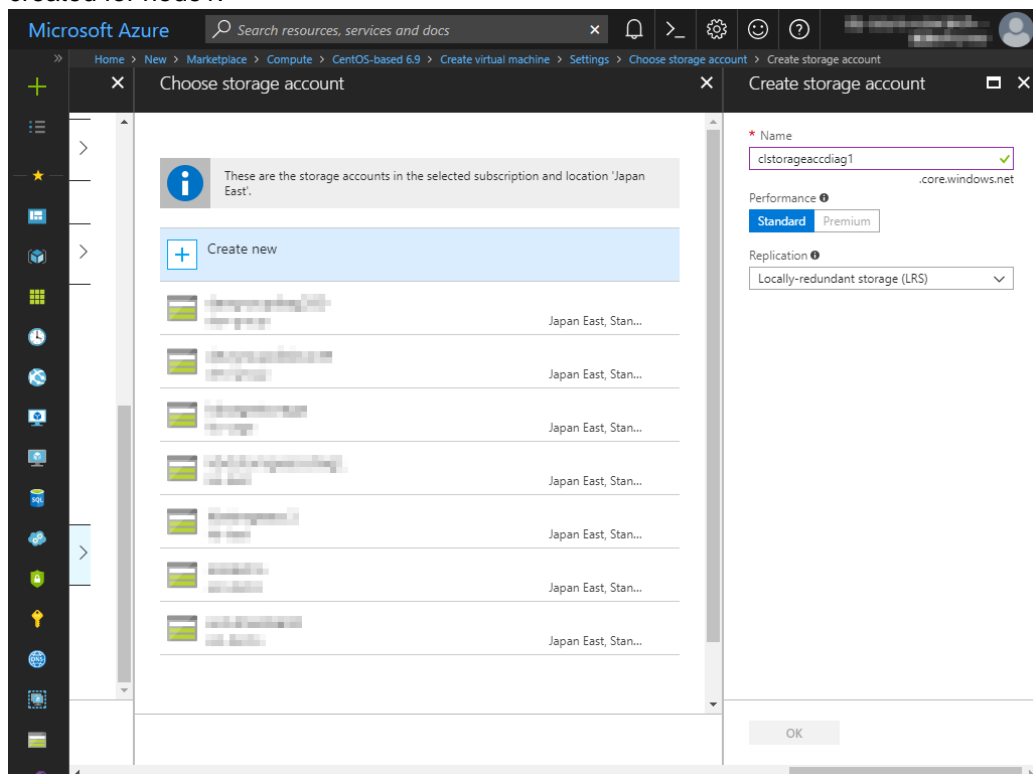


11. Return to the **Settings** blade and select **Public IP address**.
12. The **Choose public IP address** blade is displayed. Select **None**. Ignore the **Create public IP address** blade.

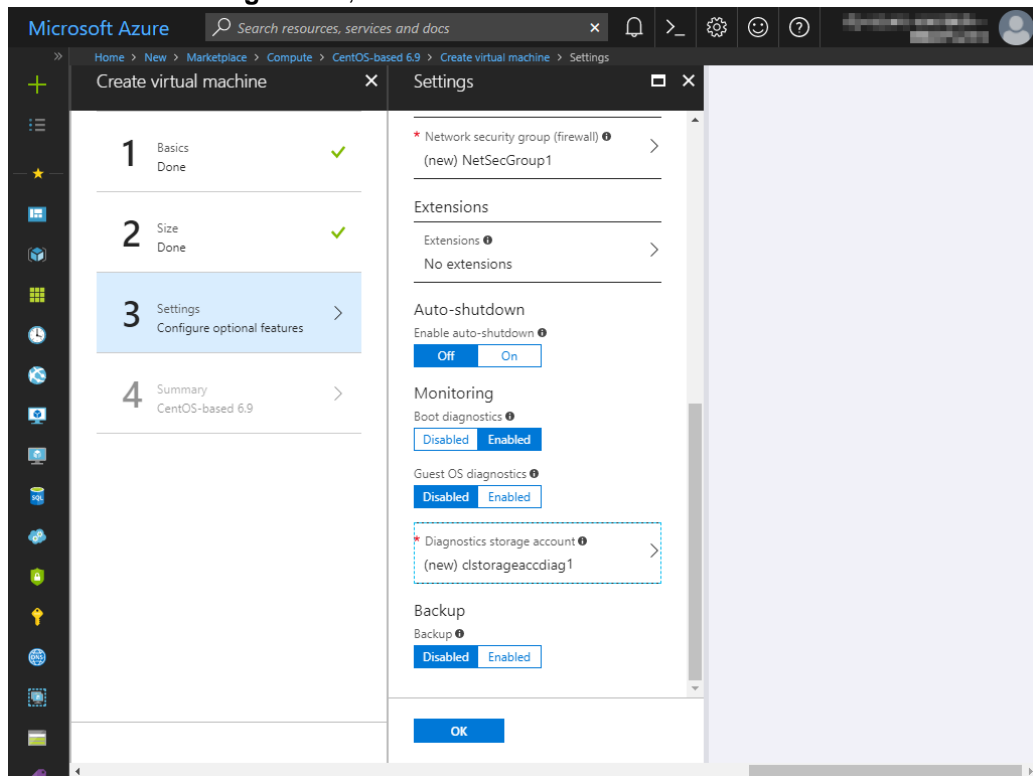
13. Return to the **Settings** blade and select **Network security group**. For node1, the **Create network security group** blade is displayed. Specify **Name**, and click **OK**. For node2, the **Choose network security group** blade is displayed. Select NetSecGroup1 created for node1.



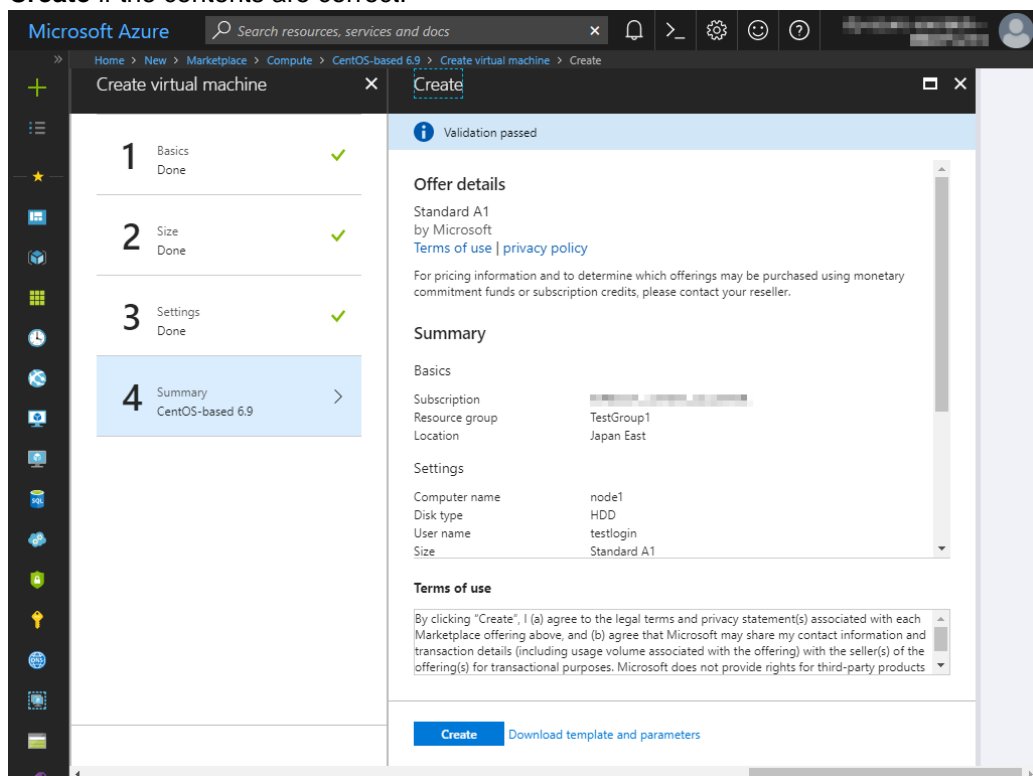
14. Return to the **Settings** blade and select **Diagnostics storage account**. For node1, the **Create storage account** blade is displayed. Specify **Name**, **Performance**, and **Replication**, and click **OK**. For node2, the **Choose storage account** blade is displayed. Select clstorageacctdiag1 created for node1.



15. Return to the **Settings** blade, and click **OK**.



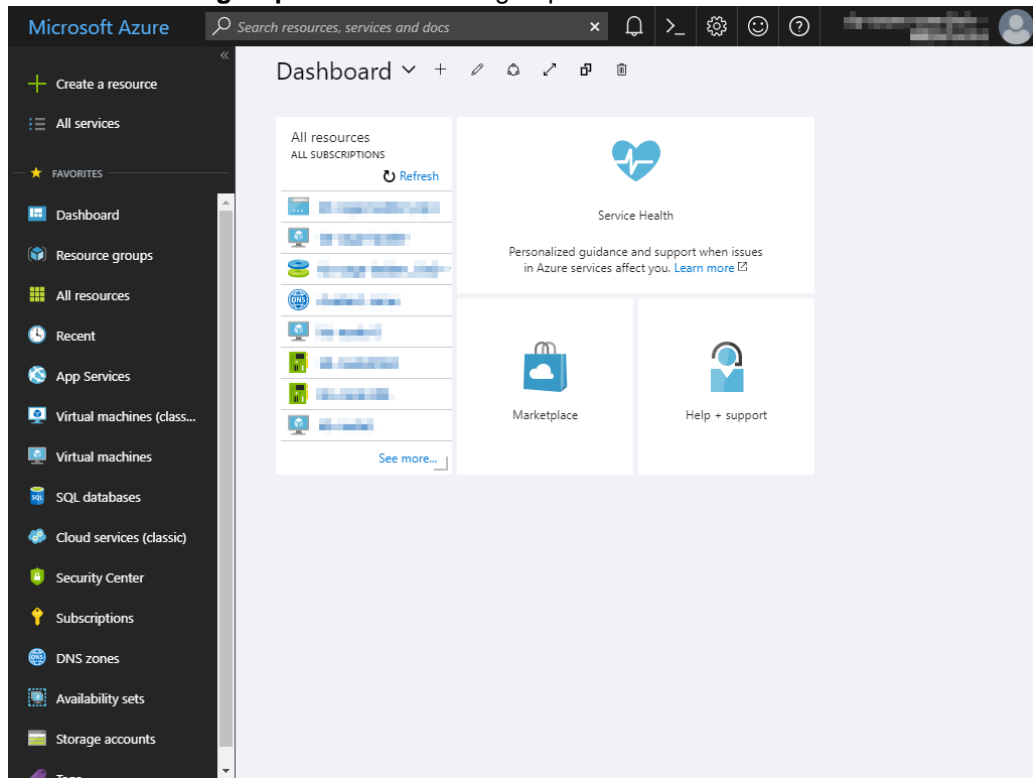
16. The **Create** blade is displayed. Check the contents displayed on the **Create** blade and click **Create** if the contents are correct.



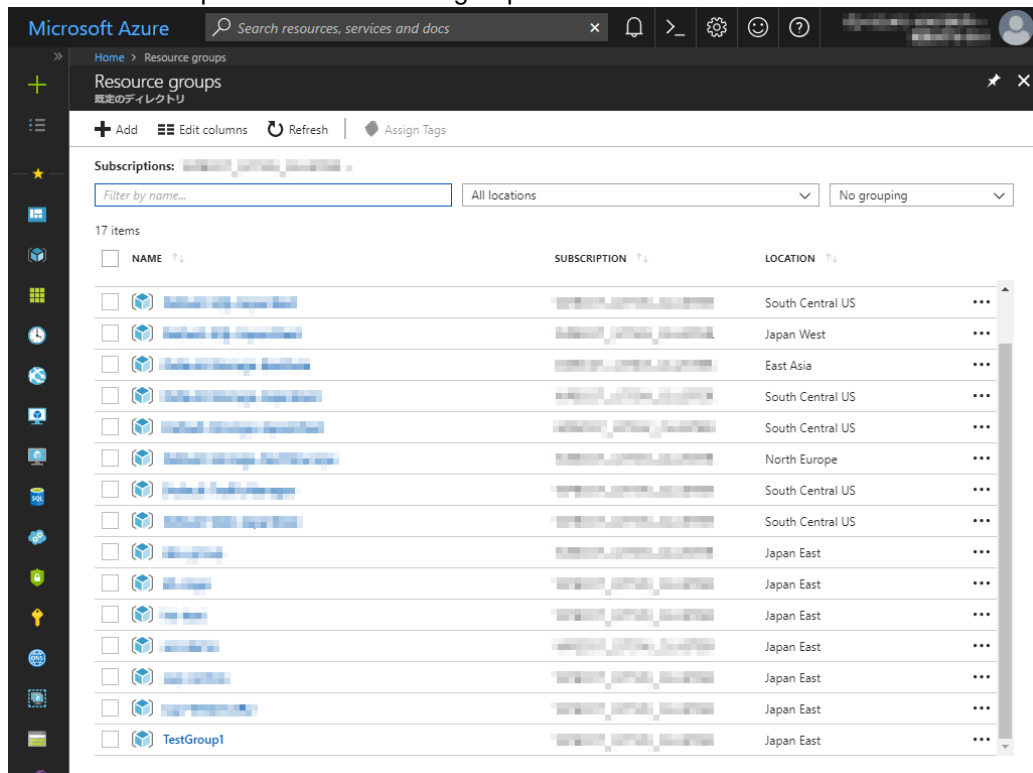
4) Setting a private IP address

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 **Resource groups** or the resource group icon in the menu on the left side 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.

Microsoft Azure

Home > Resource groups > TestGroup1

TestGroup1
Resource group

Subscription (change) [Subscription ID] Deployments: 3 Succeeded

Filter by name... All types All locations No

9 items Show all resources

NAME	TYPE	LOCATION
AvailabilitySet1	Availability set	Japan East
clstorageacct1	Storage account	Japan East
clstorageacctdiag1	Storage account	Japan East
NetSecGroup1	Network security group	Japan East
node1	Virtual machine	Japan East
node1435	Network interface	Japan East
node2	Virtual machine	Japan East
node2680	Network interface	Japan East
Vnet1	Virtual network	Japan East

4. Select **Networking**.

Microsoft Azure

Home > Resource groups > TestGroup1 > node1 - Networking

node1 - Networking
Virtual machine

Attach network interface Detach network interface

Network Interface: node1435 Effective security rules Topology

Virtual network/subnet: Vnet1/Vnet1-1 Public IP: None Private IP: 10.5.0.4

INBOUND PORT RULES

Network security group NetSecGroup1 (attached to network interface: node1435)
Impacts 0 subnets, 2 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATI...	ACTION
1000	default-allow-ssh	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNet...	VirtualNet...	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

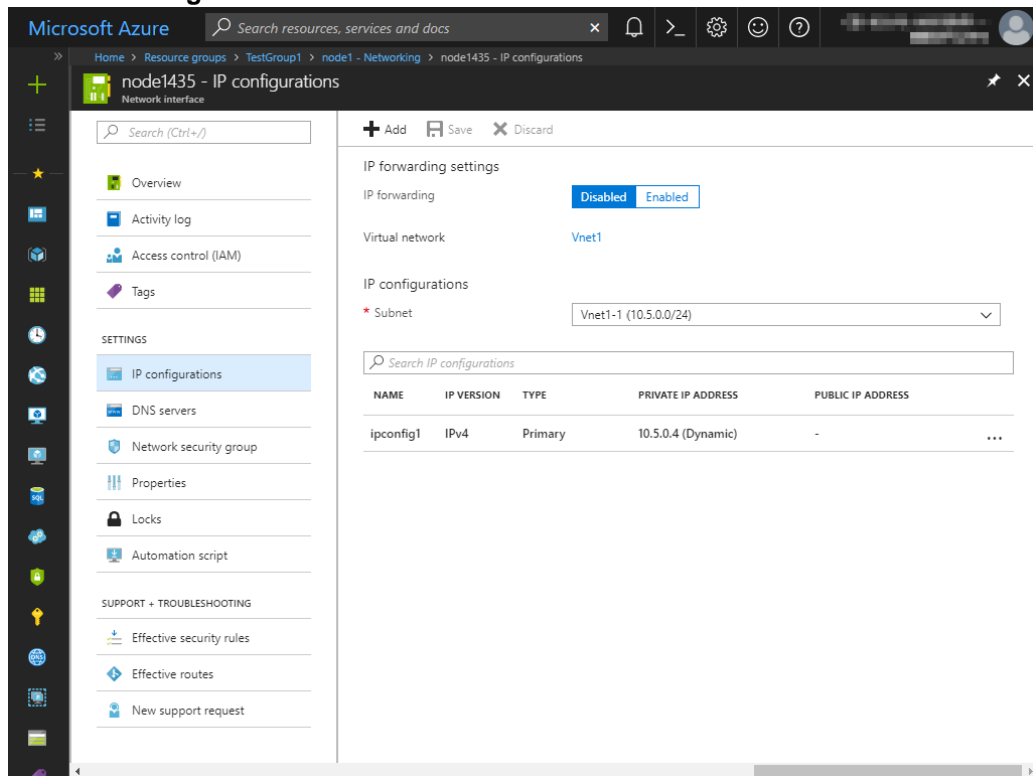
OUTBOUND PORT RULES

Network security group NetSecGroup1 (attached to network interface: node1435)
Impacts 0 subnets, 2 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATI...	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNet...	VirtualNet...	Allow
65001	AllowInternetOutBou...	Any	Any	Any	Internet	Allow

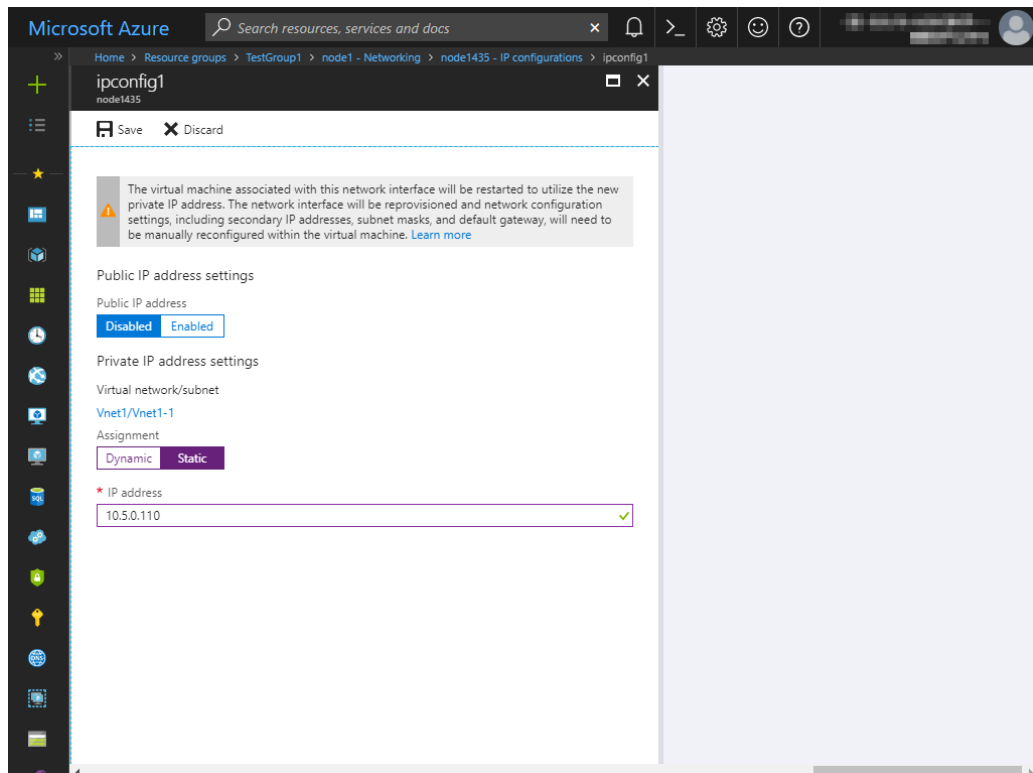
5. Select a network interface displayed in the list. The network interface name is generated automatically.

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.

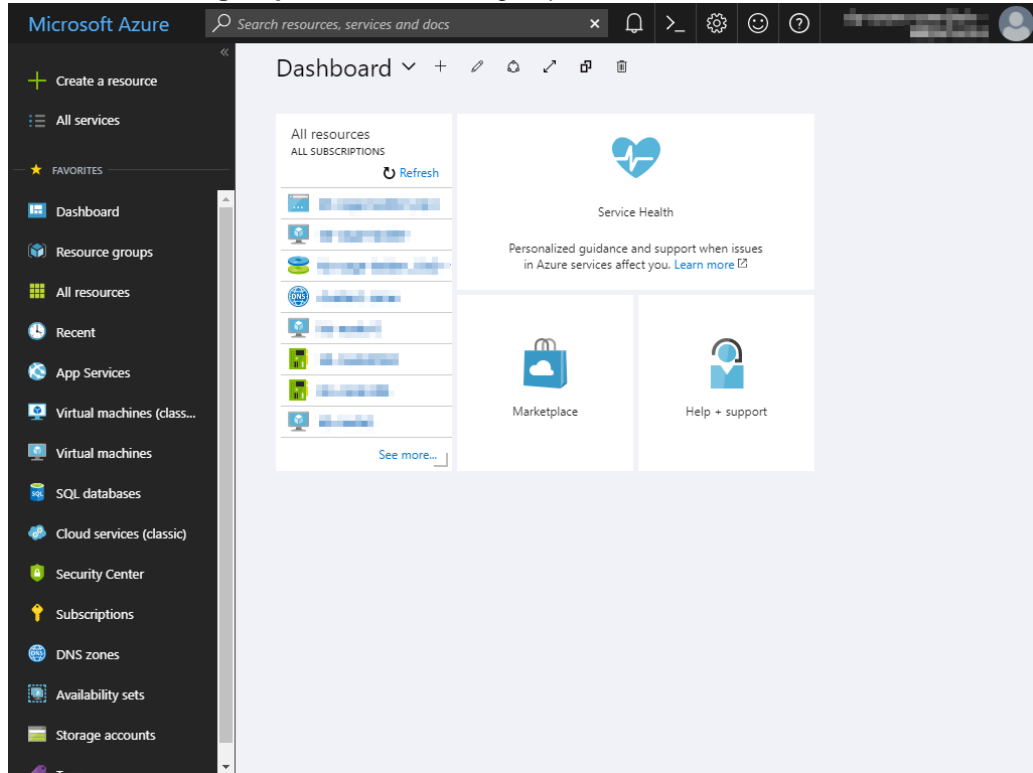


9. The virtual machines restart automatically so that new private IP addresses can be used.

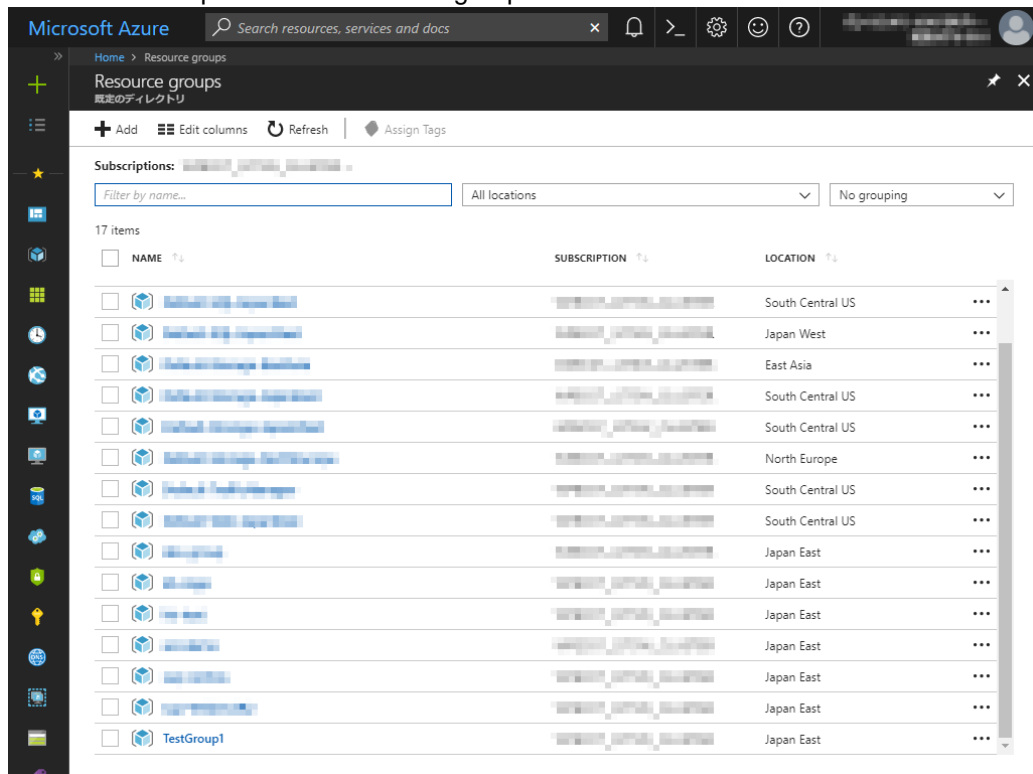
5) Adding Blob storage

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and add Blob storage to be used for a mirror disk (cluster partition or data partition). Change the settings of node1 and then node2.

1. Select **Resource groups** or the resource group icon in the menu on the left side of the window.



2. Select TestGroup1 from the resource group list.



3. The summary of TestGroup1 is displayed. Select virtual machine node1 or node2 to which to add Blob storage from the item list and select **Disk**.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1

TestGroup1 Resource group

Subscription (change) Deployments 3 Succeeded

Subscription ID

Filter by name... All types All locations No

9 items Show all resources

NAME	TYPE	LOCATION
AvailabilitySet1	Availability set	Japan East
clstorageacct1	Storage account	Japan East
clstorageacctdiag1	Storage account	Japan East
NetSecGroup1	Network security group	Japan East
node1	Virtual machine	Japan East
node1435	Network interface	Japan East
node2	Virtual machine	Japan East
node2680	Network interface	Japan East
Vnet1	Virtual network	Japan East

4. Select **+Add data disk**.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1 > node1 - Disks

node1 - Disks Virtual machine

OS disk

NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRIPTION	HOS
node1	30 GiB	Standard_LRS	Not enabled	Rea

Data disks

None

+ Add data disk

5. The **Attach unmanaged disk** blade is displayed. Click **Browse** right to the **Storage container** text box. For **Name** and **Storage blob name**, the automatically generated default values are entered.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1 > node1 - Disks > Attach unmanaged disk

Attach unmanaged disk

* Name
node1-20180215-104728 ✓

* Source type
New (empty disk) ▾

* Account type
Standard (HDD) ▾

* Size (GiB)
1023

ESTIMATED PERFORMANCE
IOPS limit 500
Throughput limit (MB/s) 60

* Storage container
 [Browse](#)

* Storage blob name
node1-20180215-104728.vhd ✓

OK

6. Select clstorageacc1 from the storage account list.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1 > node1 - Disks > Attach unmanaged disk > Storage accounts

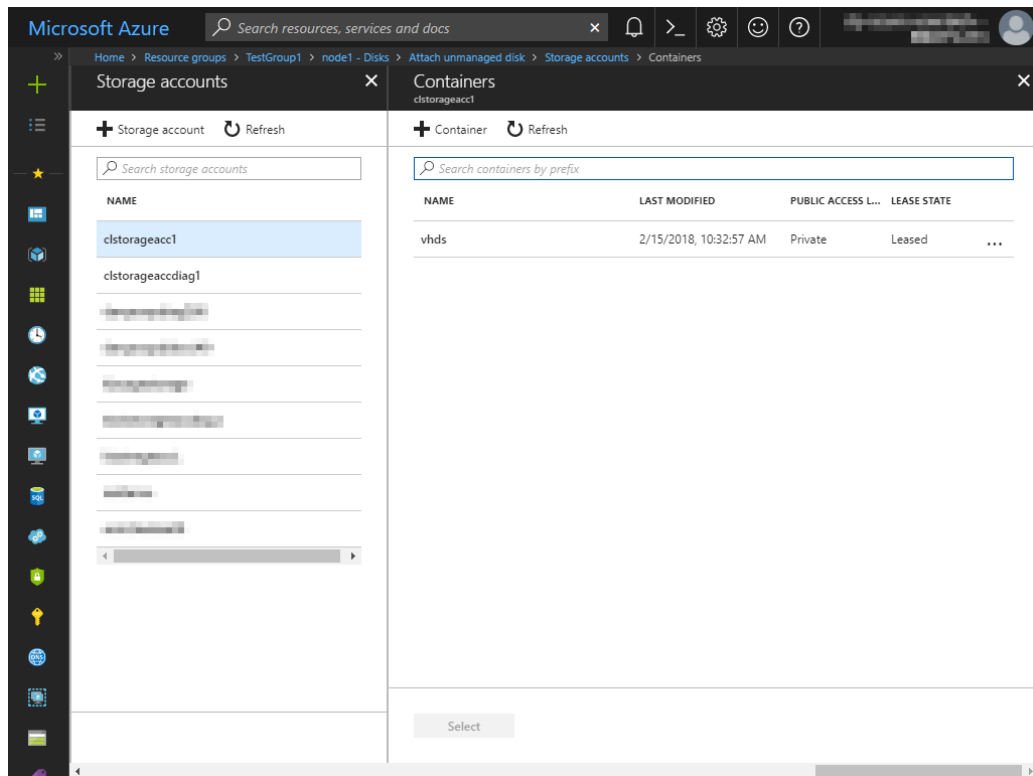
Storage accounts

+ Storage account Refresh

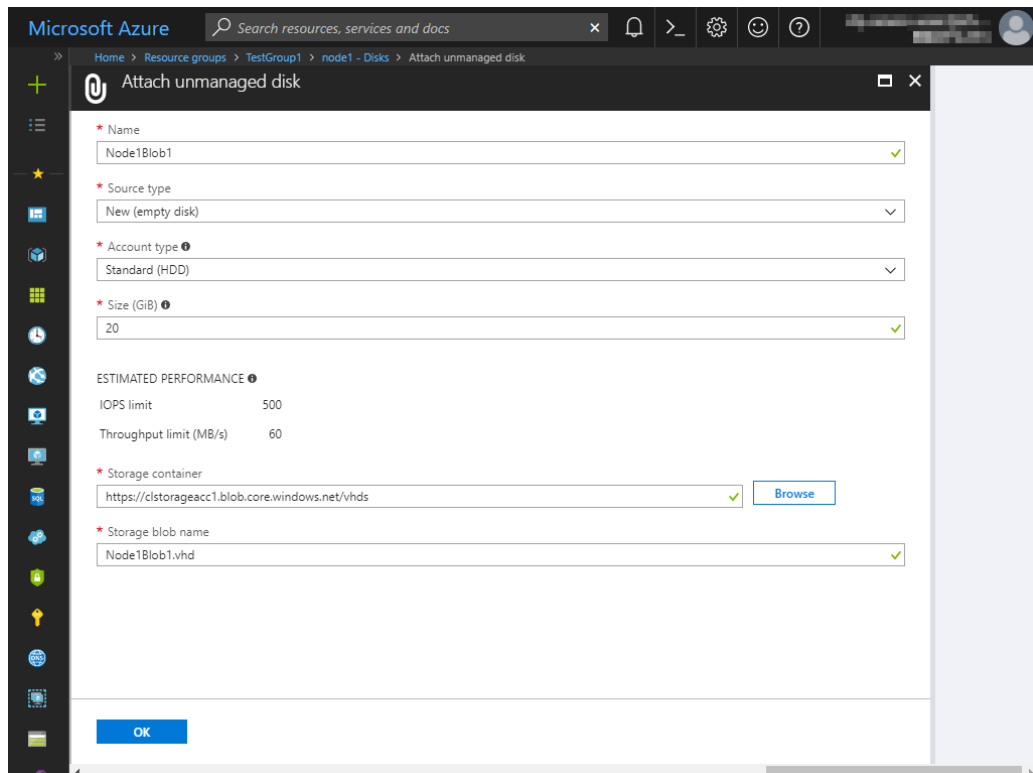
Search storage accounts

NAME	TYPE	RESOURCE GROUP
clstorageacc1	Standard-LRS	TestGroup1
clstorageaccdiag1	Standard-LRS	TestGroup1
clstorageaccdiag2	Standard-LRS	TestGroup1
clstorageaccdiag3	Standard-LRS	TestGroup1
clstorageaccdiag4	Standard-LRS	TestGroup1
clstorageaccdiag5	Standard-LRS	TestGroup1
clstorageaccdiag6	Standard-LRS	TestGroup1
clstorageaccdiag7	Standard-LRS	TestGroup1
clstorageaccdiag8	Standard-LRS	TestGroup1
clstorageaccdiag9	Standard-LRS	TestGroup1

7. Select vhds from the container list and click **Select**.



8. The **Attach unmanaged disk** blade is displayed again. Specify **Name**, **Source type**, **Account type**, **Size**, and **Storage blob name**, and click **OK**. For **Name**, specify Node1Blob for node1 and Node2Blob for node2. For **Storage blob name**, specify Node1Blob.vhd for node1 and Node2Blob.vhd for node2.



9. Click **Save**.

Microsoft Azure Search resources, services and docs

Home > node1 - Disks

node1 - Disks
Virtual machine

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

SETTINGS

Networking

Disks

Size

Extensions

Availability set

Configuration

Properties

Locks

Automation script

OPERATIONS

Save Discard

OS disk

NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOS
node1	30 GiB	Standard_LRS	Not enabled	Re

Data disks

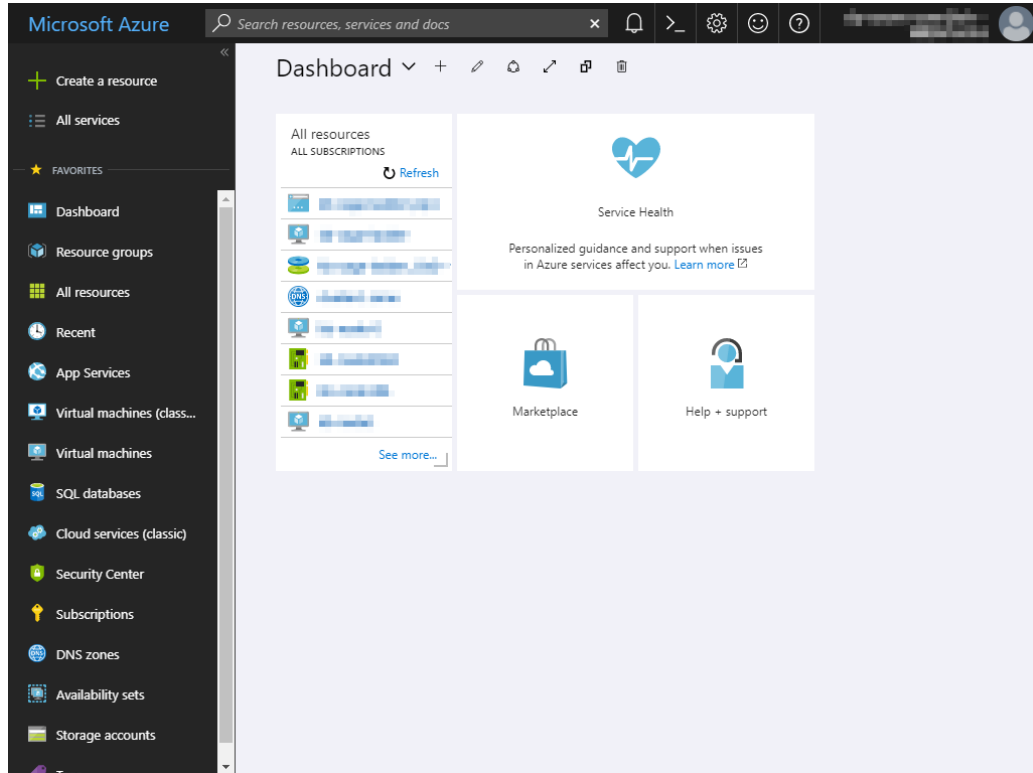
LUN	NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOS
0	Node1Blob1	20 GiB	Standard_LRS	Not enabled	Ni

+ Add data disk

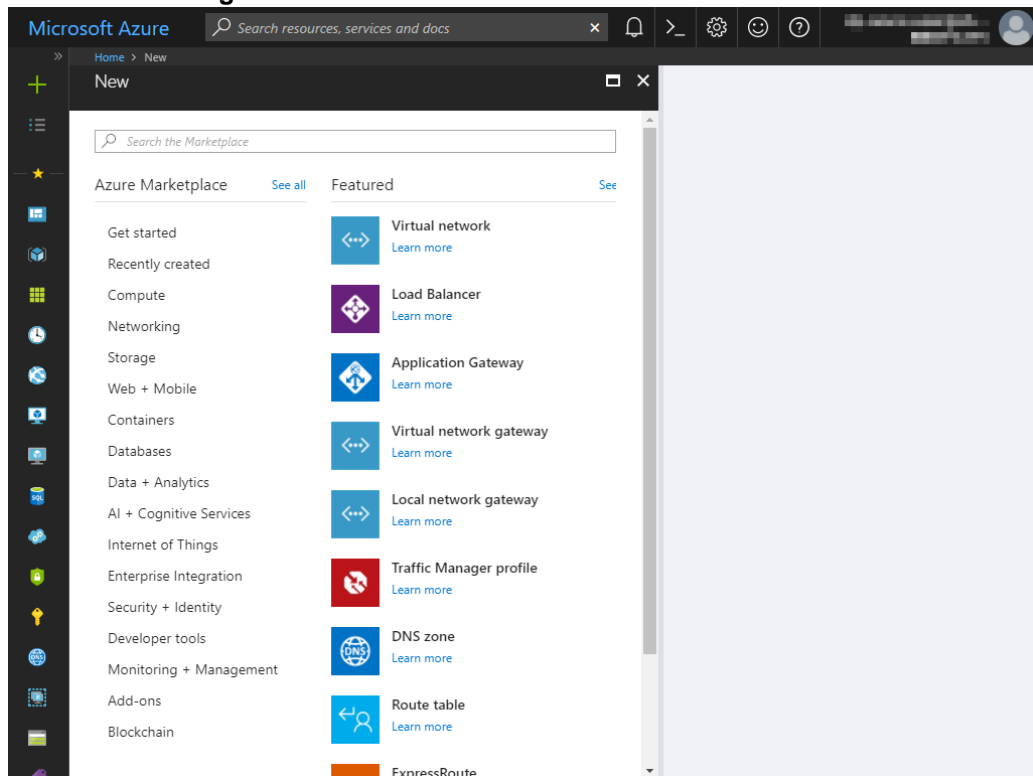
6) Creating a DNS zone

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

1. Select **+Create a resource** or the **+** icon in the menu on the left side of the window.



2. Select **Networking** and then **DNS zone**.





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


Microsoft Azure Search resources, services and docs



Home > New > Create DNS zone

Create DNS zone

* Name  cluster1.zone ✓

* Subscription 

* Resource group
 ☐ Create new ☒ Use existing
 TestGroup1 

* Resource group location  Japan East 

☐ Pin to dashboard

Create Automation options

7) 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 Blob storage.
 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 Chapter 1, "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

8 16 73400320 sdb
8 17 73398272 sdb1
8 0 31459328 sda
8 1 31456256 sda1
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. The following is an example of creating one partition including all areas of /dev/sdc.

```
$ sudo fdisk /dev/sdc
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0xe3c83b13.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
```

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

The device presents a logical sector size that is smaller than the physical sector size. Aligning to a physical sector (or optimal I/O) size boundary is recommended, or performance may be impacted.

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to switch off the mode (command 'c') and change display units to sectors (command 'u').

```
Command (m for help): n
Command action
  e extended
  p primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-2610, default 1):
Using default value 1
```

```
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610): +1G
```

```
Command (m for help): p
```

```
Disk /dev/sdc: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0xe29ed566
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sdc1		1	132	1060256+	83	Linux

Partition 1 does not end on cylinder boundary.
Partition 1 does not start on physical sector boundary.

Command (m for help): n
Command action
e extended
p primary partition (1-4)
p
Partition number (1-4): 2
First cylinder (132-2610, default 132):
Using default value 132
Last cylinder, +cylinders or +size{K,M,G} (132-2610, default 2610):
Using default value 2610
Command (m for help): p

Disk /dev/sdc: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0xe29ed566

Device	Boot	Start	End	Blocks	Id	System
/dev/sdc1		1	132	1060256+	83	Linux
Partition 1 does not end on cylinder boundary.						
Partition 1 does not start on physical sector boundary.						
/dev/sdc2		132	2610	19904537	83	Linux

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.

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

8) 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 Chapter 1, "Determining a system configuration" in the *Installation and Configuration Guide*.

9) 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 1.0: <https://docs.microsoft.com/en-us/azure/cli-install-nodejs>

Install Azure CLI 2.0:

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

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.

For the Azure CLI 1.0

```
$ sudo sh
```

```
# curl --silent --location https://rpm.nodesource.com/setup_4.x | bash -
```

```
# yum install -y nodejs
```

```
# npm install azure-cli -g
```

```
# exit
```

For the Azure CLI 2.0

```
$ sudo yum check-update; sudo yum install -y gcc libffi-devel python-devel openssl-devel
```

```
$ curl -L https://aka.ms/InstallAzureCli | bash -
```

```
$ exec -i $SHELL
```

10) 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.

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

Log in with Azure CLI 2.0: <https://docs.microsoft.com/en-us/azure/xplat-cli-connect>

Create an Azure service principal with Azure CLI 2.0:

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

For the Azure CLI 1.0 (Note that Open SSL must be installed.)

1. Create a certificate.

```
$ openssl req -x509 -days 3650 -newkey rsa:2048 -out cert.pem -nodes  
-subj '/CN=exampleapp'  
$ cat privkey.pem > /root/examplecert.pem
```

2. Acquire a thumbprint. Write down the displayed thumbprint because it is necessary to set it in the Azure environment configuration file.

```
$ openssl x509 -in /root/examplecert.pem -fingerprint -noout | sed  
's/SHA1 Fingerprint=//g' | sed 's/://g'  
98520C685C9BF50486A3ED78EBD539xxxxxxxxxx
```

3. Log in with an organizational account.

```
$ azure login -u <account_name> -p <password>
```

4. Create and register a service principal. Write down the displayed UUID (1st line under Service Principal Names) because it is necessary to set it in the Azure environment configuration file.

```
$ azure ad sp create -n exampleapp --cert-value "$(tail -n+2 cert.pem  
| head -n-1 | tr -d '\n')"  
info:      Executing command ad sp create  
+ Creating application exampleapp  
+ Creating service principal for application xxxxxxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxx  
data:      Object Id:                xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx  
data:      Display Name:              exampleapp  
data:      Service Principal Names:  
data:      xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx  
data:      http://exampleapp  
info:      ad sp create command OK
```

5. Check the tenant. Write down the displayed Tenant ID because it is necessary to set it in the Azure environment configuration file.

```
$ azure account show  
info:      Executing command account show  
data:      Name                      : Visual Studio Professional  
data:      ID                          : xxxxxxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxx  
data:      State                       : Enabled  
data:      Tenant ID                   : xxxxxxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxx  
data:      Is Default                   : true  
data:      Environment                  : AzureCloud  
data:      Has Certificate                : No  
data:      Has Access Token               : Yes  
data:      User name                     : xxxxxx@xxxxxxxxxx.xxxxx.com  
data:
```

6. Grant the service principal access permissions to the subscription.

```
$ azure role assignment create --objectId {Object Id in step 4} -o  
Contributor -c /subscriptions/{subscription Id}
```

7. Log out.

```
$ azure logout -u <account-name>
```

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


```
$ azure login --service-principal --tenant {Tenant ID} -u {UUID} --
certificate-file /root/examplecert.pem --thumbprint {thumbprint}
info:      Executing command login
|info:      Added subscription Visual Studio Professional
info:      Setting subscription "Visual Studio Professional" as default
+
info:      login command OK
```
9. Log out.


```
$ azure logout -u <UUID>
```

For the Azure CLI 2.0

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 environment configuration file. In the following example, a service principal is created in `/root/examplecert.pem`.


```
$ az ad sp create-for-rbac --create-cert
{
  "appId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
  "displayName": "azure-test",
  "fileWithCertAndPrivateKey": " /root/examplecert.pem",
  "name": "http://azure-test",
  "password": null,
  "tenant": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```
3. Log out.


```
$ az logout --u <account_name>
```
4. Check whether login to Microsoft Azure using the created service principal is possible.


```
$ az login --service-principal -u <name_value_in_step_2> --tenant
<tenant_value_in_step_2> -p
<fileWithCertAndPrivateKey_value_in_step_2>
The following is displayed upon successful sign-in.
[
  {
    "cloudName": "AzureCloud",
    "id": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "isDefault": true,
    "state": "Enabled",
    "tenantId": "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
    "user": {
      "name": "http://azure-test",
      "type": "servicePrincipal"
    }
  }
]
```
5. Log out.


```
$ az logout --username <name_value_in_step_4>
```

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

For the Azure CLI 1.0

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

For the Azure CLI 2.0
Microsoft.Network/dnsZones/A/write
Microsoft.Network/dnsZones/A/delete
Microsoft.Network/dnsZones/NS/read

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*.

3.3 Configuring the EXPRESSCLUSTER settings

Configure the following on the WebManager cluster generation wizard.

For the WebManager setup and connection procedures, see Chapter 5, "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)
- Multi target monitor resource (for NP resolution)
- Multi target monitor resource (for NP resolution)

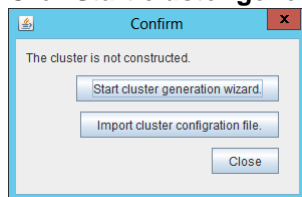
For the settings of other resources and monitor resources, see the *Installation and Configuration Guide* and the *Reference Guide*.

1) Creating a cluster

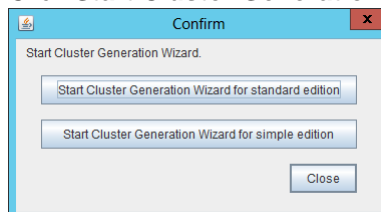
Start the cluster generation wizard to create a cluster.

◆ Creating a cluster

1. Access WebManager. Then, the following dialog box is displayed.
Click **Start cluster generation wizard**.



2. The following dialog box is displayed.
Click **Start Cluster Generation Wizard for standard edition**.



3. The **Cluster Definition** page is displayed.
Enter a desired name in **Cluster Name**.
Select an appropriate language in **Language**. After the setting is applied, the display language of WebManager is changed to the selected language.

The screenshot shows the 'Cluster Definition' page of the 'Cluster Generation Wizard'. On the left, a 'Steps' sidebar lists 'Cluster', 'Server', 'Basic Settings', 'Interconnect', 'NP Resolution', 'Group', and 'Monitor'. The 'Cluster' step is selected. The main area contains the following fields:

- Cluster Name:** A text box containing 'Cluster1'.
- Comment:** An empty text box.
- Language:** A dropdown menu showing 'English'.
- Management IP Address:** An empty text box.

Below these fields is a 'Description' section with the following text:

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

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

4. The **Server Definition** page is displayed.
The instance connected to WebManager is displayed as a registered master server.
Click **Add** to add the remaining instances (by specifying the private IP address of each instance).

The screenshot shows the 'Server Definition' page of the 'Cluster Generation Wizard'. The 'Steps' sidebar on the left is the same as in the previous screenshot, but 'Server' is now selected. The main area contains the following elements:

- Server Definition List:** A table with two columns: 'Order' and 'Name'. It contains two rows: 'Master Server' with 'node1' and '1' with 'node2'.
- Buttons:** 'Add' and 'Remove' buttons are to the right of the table. 'Up' and 'Down' buttons are below the table.
- Server Group:** A section with a 'Server Group Definition' text box and a 'Settings' button to its right.
- Description:** A section with the following text:
Click "Add" to add servers constructing the cluster.
Click "Up" or "Down" to change the server priority.
Click "Settings" to configure the server group when using the server group.

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

5. Click **Next**.

6. The **Interconnect** page 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.

Cluster Generation Wizard

Steps

- Cluster
- Server
- Basic Settings
- Interconnect
- NP Resolution
- Group
- Monitor

Interconnect

Priority	Type	MDC	node1	node2
1	Kernel Mode	mdc1	10.5.0.110	10.5.0.111

Buttons: Add, Remove, Properties, Up, Down

Description

Configure the interconnect among the servers constructing the cluster. Click "Add" to add interconnect and select the type. For "Kernel mode", "User mode", "BMC", "DISK" and "COM" settings, configure the route which is used for heartbeat. For "Mirror Communication Only" setting, configure the route which is used only for data mirroring communication. Configuring more than one routes is recommended. Click "Up" or "Down" to configure the priority. For "Mirror Communication Only" settings, click each server column cell to configure IP addresses. For the communication route which is used for data mirroring communication, select the mirror disk connect name to be allocated to the communication route in MDC column.

Buttons: < Back, Next >, Cancel

7. Click **Next**.
8. The **NP Resolution** page is displayed.
Note that NP resolution is not configured on this page. 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**." Click **Next**.

Cluster Generation Wizard

Steps

- Cluster
- Server
- Basic Settings
- Interconnect
- NP Resolution
- Group
- Monitor

NP Resolution

Type	Ping Target	node1	node2
------	-------------	-------	-------

Buttons: Add, Remove, Properties, Tuning

Description

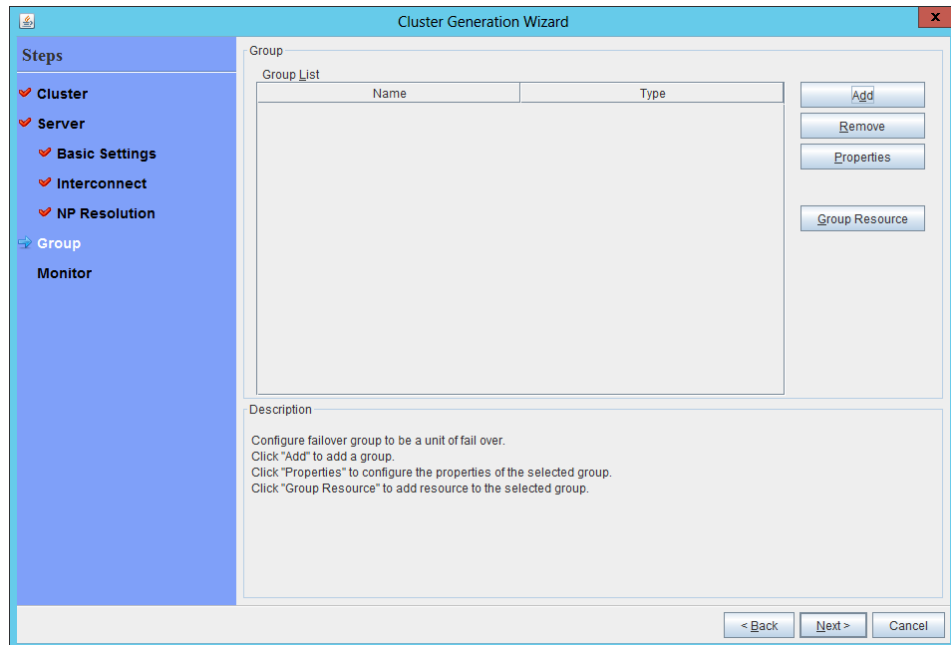
Configure network partition (NP) resolution function. In case Ping method NP resolution, click "Add" to add Ping NP resolution resource and click Ping target column cell to configure IP address of Ping destination. Click each server column cell to configure "Use" or "Do not use". The detailed settings can be verified and changed by clicking "Properties". Click "Tuning" to configure the actions at NP occurrence.

Buttons: < Back, Next >, Cancel

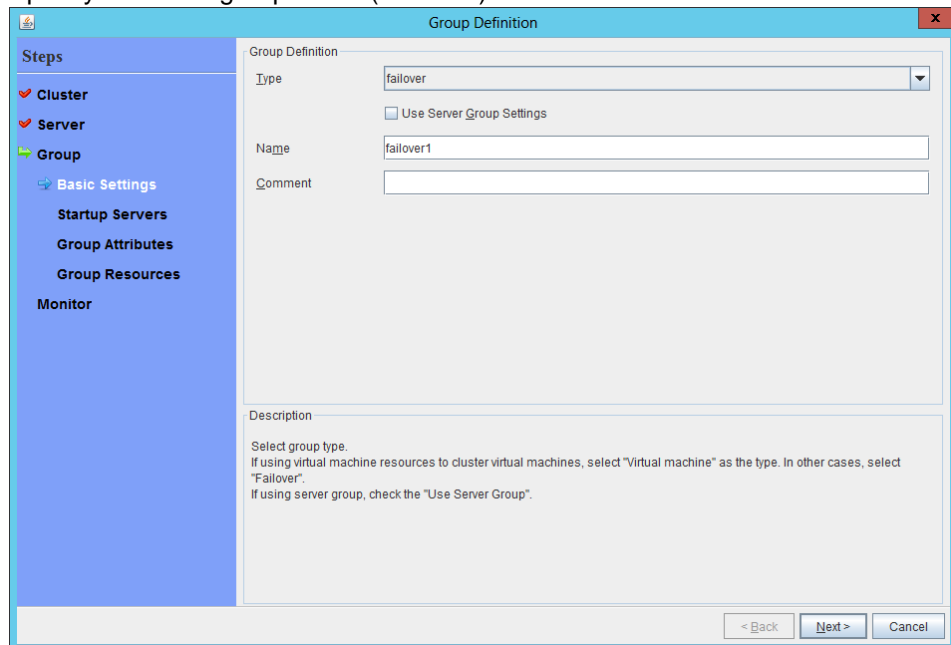
2) Adding a group resource

- ◆ Defining a group
Create a failover group.

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



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



3. Click **Next**.

4. The **Servers that can run the Group** page is displayed.
Click **Next** without specifying anything.

The screenshot shows the 'Group Definition(failover1)' dialog box. On the left is a 'Steps' sidebar with options: Cluster, Server, Group (selected), Basic Settings, Startup Servers, Group Attributes, Group Resources, and Monitor. The main area is titled 'Servers that can run the Group'. It contains a checkbox 'Failover is possible on all servers' which is checked. Below this are two lists: 'Servers that can run the Group' (empty) and 'Available Servers' (containing 'node1' and 'node2'). Between the lists are buttons: '< Add', 'Remove >', 'Up', and 'Down'. At the bottom right are buttons: '< Back', 'Next >', and 'Cancel'. A 'Description' section at the bottom provides instructions on server selection and priority.

5. The **Group Attribute Settings** page is displayed.
Click **Next** without specifying anything.

The screenshot shows the 'Group Definition(failover1)' dialog box, now on the 'Group Attribute Settings' page. The 'Steps' sidebar remains the same. The main area contains settings for 'Startup Attribute' (radio buttons for 'Auto Startup' and 'Manual Startup'), 'Failover Attribute' (radio buttons for 'Auto Failover' and 'Manual Failover'), and 'Failback Attribute' (radio buttons for 'Auto Failback' and 'Manual Failback'). Under 'Auto Failover', there are checkboxes for 'Use the startup server settings', 'Failover dynamically', 'Perform a Forced Failover', 'Prioritize failover policy in the server group', and 'Perform a Smart Failover'. There is also an 'Edit exclusion monitor' button. At the bottom right are buttons: '< Back', 'Next >', and 'Cancel'. A 'Description' section at the bottom provides instructions on configuring failover and failback.

6. The **Group Resource** page is displayed.
On this page, add a group resource following the procedure below.

The screenshot shows the 'Group Definition(failover1)' window. On the left is a 'Steps' sidebar with options: Cluster, Server, Group (selected), Basic Settings, Startup Servers, Group Attributes, Group Resources, and Monitor. The main area is titled 'Group Resource' and 'Group Resource List'. It contains a table with columns 'Name' and 'Type'. To the right of the table are buttons: 'Add', 'Remove', and 'Properties'. Below the table is a 'Description' section with instructions: 'Click "Add" to add resources. Click "Properties" to configure the properties of the selected resource.' At the bottom right are buttons: '< Back', 'Finish', and 'Cancel'.

- ◆ Mirror disk resource
Create a mirror disk resource.
For details, see "Understanding mirror disk resources" in Chapter 4, "Group resource details" in the *Reference Guide*.

1. Click **Add** on the **Group Resource List** page.
2. The **Resource Definition of Group** 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.

The screenshot shows the 'Resource Definition of Group(failover1)' window. The 'Steps' sidebar on the left has 'Group Resources' selected. The main area is titled 'Group Resource Definitions'. It features a 'Type' dropdown menu set to 'mirror disk resource', a 'Name' text box containing 'md', and an empty 'Comment' text box. A 'Get Licence Info' button is to the right of the comment box. Below these is a 'Description' section with the instruction: 'Select the type of group resource and enter its name.' At the bottom right are buttons: '< Back', 'Next >', and 'Cancel'.

3. Click **Next**.

4. The **Dependent Resources** page is displayed.
Click **Next** without specifying anything.

Resource Definition of Group(failover1)

☒ Follow the default dependency

Dependent Resources

Name	Resource type
--	
--	AWS Elastic I...
--	AWS virtual ip ...
--	Azure probe p...
--	floating ip res...
--	virtual ip reso...

Available Resources

Name

< Back Next > Cancel

5. The **Recovery Operation at Activation Failure Detection** and **Recovery Operation at Deactivation Failure Detection** page is displayed.
Click **Next**.

Resource Definition of Group(failover1)

Execute Script before or after Activation or Deactivation Settings

Recovery Operation at Activation Failure Detection

Retry Count 0 time

Failover Threshold 1 time

Final Action No operation (not activate next resource) ▾

☐ Execute Script before Final Action Settings

Recovery Operation at Deactivation Failure Detection

Retry Count at Deactivation Failure 0 time

Final Action Stop the cluster service and shutdown OS ▾

☐ Execute Script before Final Action Settings

< Back Next > Cancel

6. The **Details Settings** page is displayed.
Enter the device name of the partition created in "7) **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)

Steps

- Cluster
- Server
- Group
 - Basic Settings
 - Startup Servers
 - Group Attributes
 - Group Resources
 - Info
 - Dependency
 - Recovery Operation
 - Details
- Monitor

Common node1 node2

Mirror Partition Device Name /dev/nmp1

Mount Point /dev/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 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 Chapter 4, “Group resource details” in the *Reference Guide*.

1. Click **Add** on the **Group Resource List** page.
2. The **Resource Definition of Group** 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.

Resource Definition of Group(failover1)

Steps

- Cluster
- Server
- Group
- Basic Settings
- Startup Servers
- Group Attributes
- Group Resources
- Info
- Dependency
- Recovery Operation
- Details
- Monitor

Group Resource Definitions

Type: Azure DNS resource

Name: azuredns1

Comment:

Get Licence Info

Description

Select the type of group resource and enter its name.

< Back Next > Cancel

3. Click **Next**.
4. The **Dependent Resources** page is displayed. Click **Next** without specifying anything.

Resource Definition of Group(failover1)

Steps

- Cluster
- Server
- Group
- Basic Settings
- Startup Servers
- Group Attributes
- Group Resources
- Info
- Dependency
- Recovery Operation
- Details
- Monitor

☒ Follow the default dependency

Dependent Resources

Name	Resource type
------	---------------

< Add Remove >

Available Resources

Name

< Back Next > Cancel

- The **Recovery Operation at Activation Failure Detection** and **Recovery Operation at Deactivation Failure Detection** page is displayed. Click **Next**.

- 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, please input **Thumbprint of Service Principal**.

- Click **Finish**.

3) Adding a monitor resource

- ◆ Azure DNS monitor resource

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

For details about Azure DNS monitor resources, see "*Reference Guide*" > "Chapter 5, Monitor resource details" > "Understanding Azure DNS monitor resources."

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

- ◆ Custom monitor resource

Sets a script to monitor whether communication with 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 Chapter 5, "Monitor resource details" 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.

The screenshot shows the 'Monitor Resource Definition' window. On the left, a sidebar lists 'Steps' (Cluster, Server, Group, Monitor, Info) and under 'Monitor', it lists 'Monitor(common)', 'Monitor(special)', and 'Recovery Action'. The main panel has a title bar 'Monitor Resource Definition' and a close button. It contains three input fields: 'Type' (a dropdown menu showing 'custom monitor'), 'Name' (a text box containing 'genw1'), and 'Comment' (an empty text box). To the right of the 'Comment' field is a 'Get Licence Info' button. Below these fields is a 'Description' section with the text 'Select the type of monitor resource and enter its name.' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

3. Click **Next**.

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

The screenshot shows the 'Monitor Resource Definition' dialog box with the 'Monitor (common)' page selected in the left sidebar. The main area contains the following settings:

- 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:** (empty text box with a 'Browse' button)
- Nice Value:** A slider set to 0
- Choose servers that execute monitoring:** (empty text box with a 'Server' button)

At the bottom right, there are buttons for '< Back', 'Next >', and 'Cancel'.

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

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

Select **Synchronous** for **Monitor Type**.

The screenshot shows the 'Monitor Resource Definition' dialog box with the 'Monitor (special)' page selected in the left sidebar. The main area contains the following settings:

- ☐ User Application
- ☒ Script created with this product
- File:** genw.sh (with 'View', 'Edit', and 'Replace' buttons)
- Monitor Type:** ☒ Synchronous, ☐ Asynchronous
- Log Output Path:** (empty text box)
- ☐ Rotate Log
- Rotation Size:** 1000000 byte
- Normal Return Value:** 0

At the bottom right, there is a 'Viewer/Editor tool can be changed' label with a 'Change' button, and buttons for '< Back', 'Next >', and 'Cancel'.

6. Click **Next**.

7. The **Recovery Action** page 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' dialog box with the 'Recovery Action' tab selected. The left sidebar shows a tree view with 'Recovery Action' highlighted. The main area contains the following fields:

- Recovery Action:** A dropdown menu set to 'Execute only the final action'.
- Recovery Target:** A text box containing 'LocalServer' and a 'Browse' button.
- Recovery Script Execution Count:** A text box containing '0' and a 'time' unit.
- Execute Script before Reactivation:** An unchecked checkbox.
- Maximum Reactivation Count:** A text box containing '0' and a 'time' unit.
- Execute Script before Failover:** An unchecked checkbox.
- Execute migration before Failover:** An unchecked checkbox.
- Maximum Failover Count:** A text box containing '0' and a 'time' unit.
- Execute Script before Final Action:** An unchecked checkbox.
- Final Action:** A dropdown menu set to 'No operation'.

At the bottom right, there are buttons for '< Back', 'Finish', 'Cancel', and 'Script Settings'.

8. 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 Chapter 5, “Monitor resource details” in the *Reference Guide*.

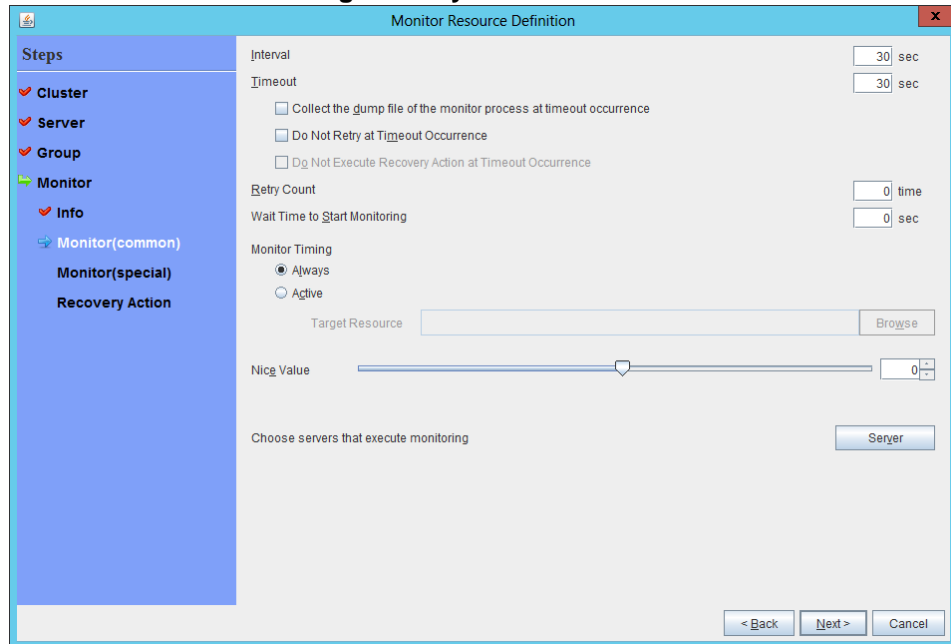
1. Click **Add** on the **Monitor Resource List** page.
2. Select the monitor resource type (ip monitor) from the **Type** box and enter the monitor resource name (ipw1) in the **Name** box.

The screenshot shows the 'Monitor Resource Definition' dialog box with the 'Info' tab selected. The left sidebar shows a tree view with 'Info' highlighted. The main area contains the following fields:

- Type:** A dropdown menu set to 'ip monitor'.
- Name:** A text box containing 'ipw1'.
- Comment:** An empty text box.
- Get Licence Info:** A button.
- Description:** A text box containing the text 'Select the type of monitor resource and enter its name.'

At the bottom right, there are buttons for '< Back', 'Next >', and 'Cancel'.

3. Click **Next**.
4. The **Monitor (common)** page is displayed.
Confirm that **Monitor Timing** is **Always**.

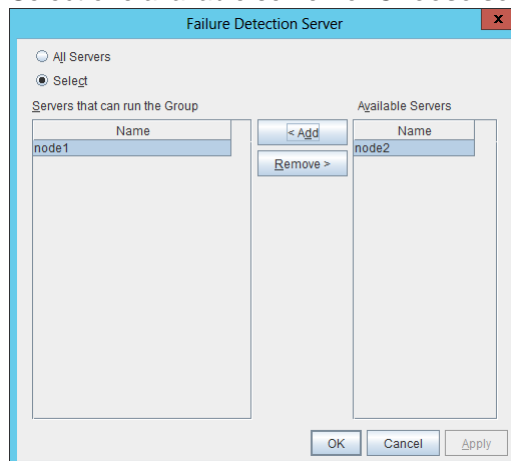


The **Monitor Resource Definition** dialog box is shown. On the left, the **Steps** pane lists: Cluster, Server, Group, Monitor, Info, Monitor(common), Monitor(special), and Recovery Action. The **Monitor(common)** step is selected. The main area contains the following settings:

- 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 text box] **Browse**
- Nice Value:** 0 (slider)
- Choose servers that execute monitoring:** **Server** button

At the bottom right are buttons: **< Back**, **Next >**, and **Cancel**.

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



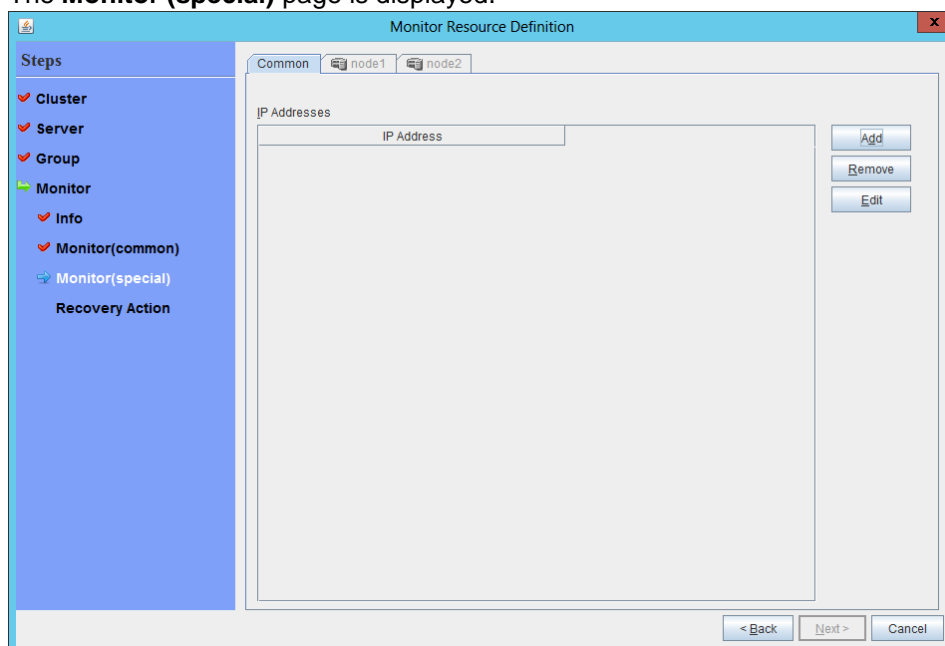
The **Failure Detection Server** dialog box is shown. It has two radio buttons: ☐ All Servers and ☒ Select. Below the radio buttons are two list boxes:

- Servers that can run the Group:** Contains 'node1'.
- Available Servers:** Contains 'node2'.

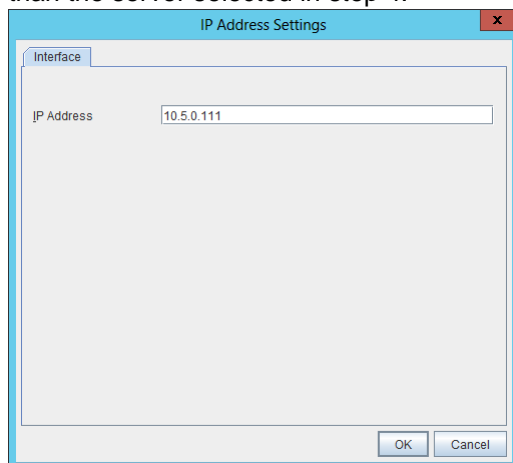
Between the list boxes are buttons: **< Add** and **Remove >**. At the bottom are buttons: **OK**, **Cancel**, and **Apply**.

Click **Next**.

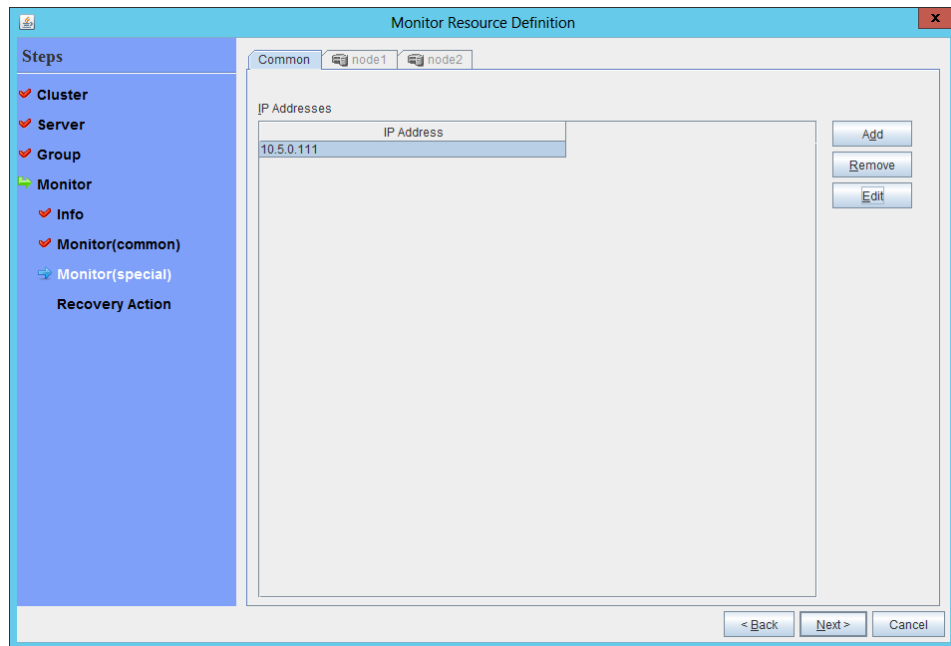
5. The **Monitor (special)** page is displayed.



On the **Common** tab, select **Add** of **IP Address** and set an IP address of a server other than the server selected in step 4.

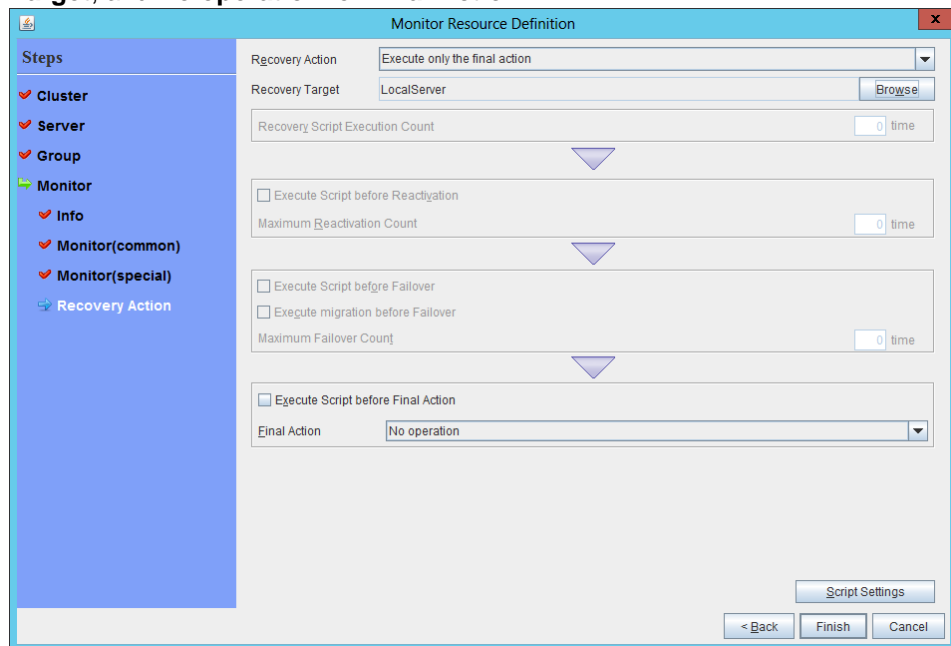


6. Click **Next**.



The 'Monitor Resource Definition' dialog box is shown with the 'Common' tab selected. The 'Steps' pane on the left lists 'Cluster', 'Server', 'Group', 'Monitor', 'Info', 'Monitor(common)', 'Monitor(special)', and 'Recovery Action'. The 'Monitor' step is highlighted. The main area shows 'IP Addresses' with a table containing one entry: '10.5.0.111'. To the right of the table are buttons for 'Add', 'Remove', and 'Edit'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

7. The **Recovery Action** page is displayed.
Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final Action**.



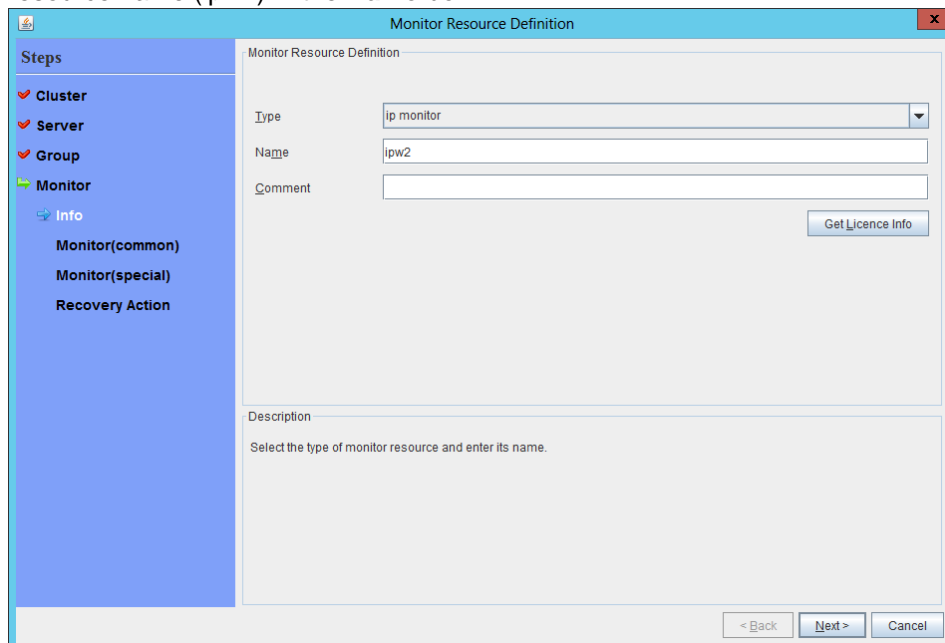
The 'Monitor Resource Definition' dialog box is shown with the 'Recovery Action' tab selected. The 'Steps' pane on the left lists 'Cluster', 'Server', 'Group', 'Monitor', 'Info', 'Monitor(common)', 'Monitor(special)', and 'Recovery Action'. The 'Recovery Action' step is highlighted. The main area contains the following settings:

- Recovery Action:** A dropdown menu set to 'Execute only the final action'.
- Recovery Target:** A text field containing 'LocalServer' and a 'Browse' button.
- Recovery Script Execution Count:** A text field containing '0' and a 'time' label.
- Execute Script before Reactivation:** An unchecked checkbox.
- Maximum Reactivation Count:** A text field containing '0' and a 'time' label.
- Execute Script before Failover:** An unchecked checkbox.
- Execute migration before Failover:** An unchecked checkbox.
- Maximum Failover Count:** A text field containing '0' and a 'time' label.
- Execute Script before Final Action:** An unchecked checkbox.
- Final Action:** A dropdown menu set to 'No operation'.

At the bottom right are 'Script Settings', '< Back', 'Finish', and 'Cancel' buttons.

8. Click **Finish** to finish setting.
9. Then, create a monitor resource on the other server. Click **Add** on the **Monitor Resource List** page.

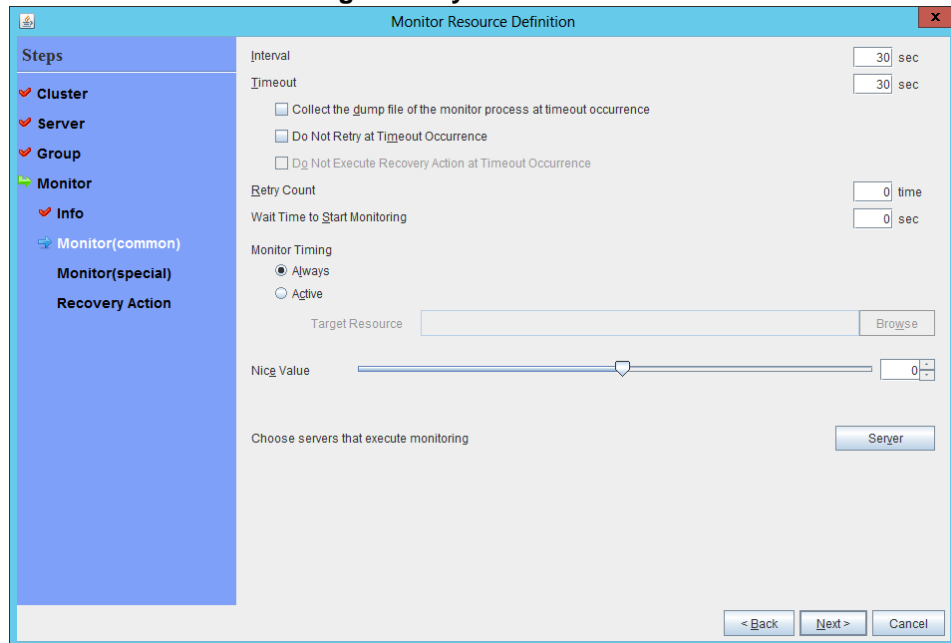
10. Select the monitor resource type (ip monitor) from the **Type** box and enter the monitor resource name (ipw2) in the **Name** box.



The image shows a 'Monitor Resource Definition' dialog box. On the left is a 'Steps' sidebar with a tree view containing 'Cluster', 'Server', 'Group', 'Monitor' (selected), and 'Info'. Under 'Monitor', there are sub-items: 'Monitor(common)', 'Monitor(special)', and 'Recovery Action'. The main area is titled 'Monitor Resource Definition' and contains three input fields: 'Type' (a dropdown menu with 'ip monitor' selected), 'Name' (a text box with 'ipw2' entered), and 'Comment' (an empty text box). To the right of the 'Comment' field is a 'Get Licence Info' button. Below these fields is a 'Description' section with the text 'Select the type of monitor resource and enter its name.' At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

11. Click **Next**.

12. The **Monitor (common)** page is displayed.
Confirm that **Monitor Timing** is **Always**.

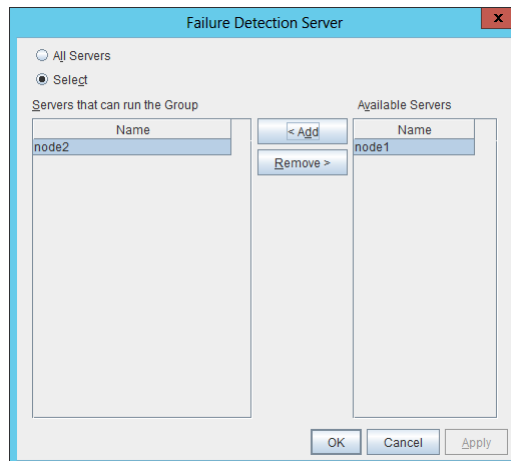


The **Monitor Resource Definition** dialog box is shown. The **Steps** pane on the left has **Monitor** selected, with sub-steps **Info**, **Monitor(common)**, **Monitor(special)**, and **Recovery Action**. The main area contains the following settings:

- 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 text box with a **Browse** button)
- Nice Value:** 0 (slider)
- Choose servers that execute monitoring:** (empty list with a **Server** button)

Navigation buttons at the bottom: **< Back**, **Next >**, and **Cancel**.

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



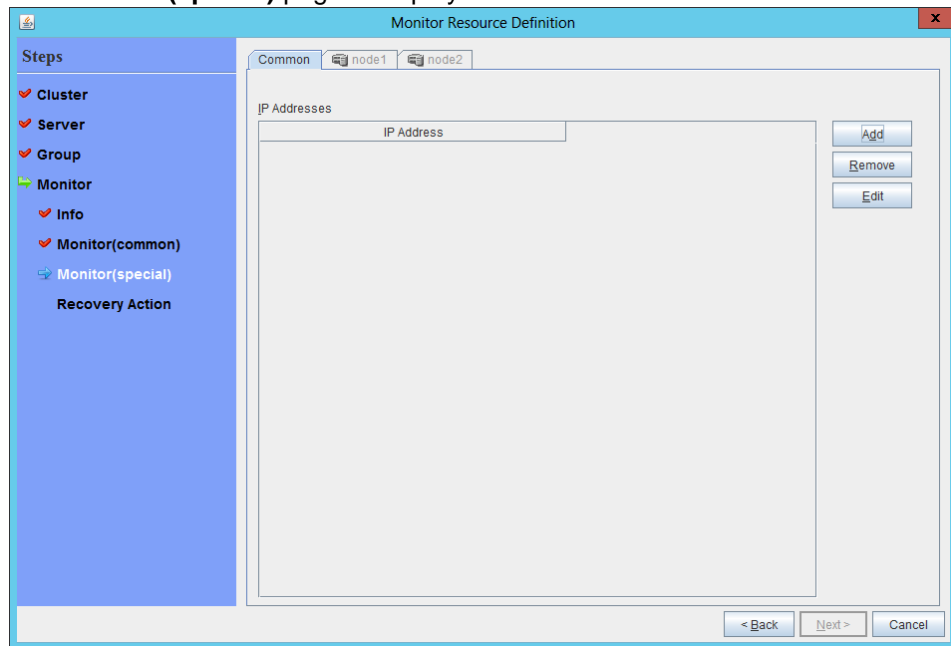
The **Failure Detection Server** dialog box is shown. It has two radio buttons: **All Servers** and **Select** (which is selected). Below the radio buttons are two list boxes:

- Servers that can run the Group:** Contains **node2**.
- Available Servers:** Contains **node1**.

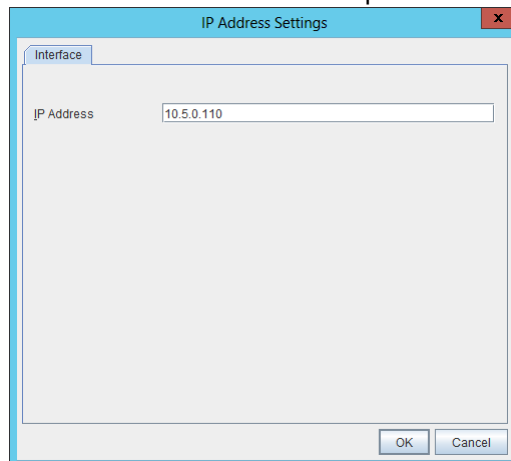
Between the list boxes are **< Add** and **Remove >** buttons. At the bottom are **OK**, **Cancel**, and **Apply** buttons.

Click **Next**.

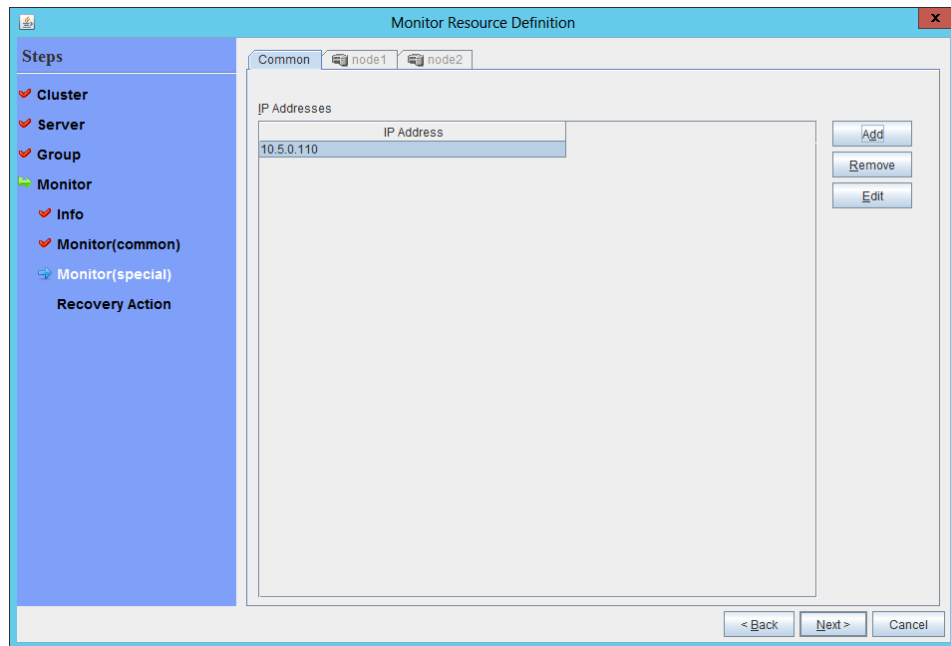
13. The **Monitor (special)** page is displayed.



On the **Common** tab, select **Add** of **IP Address** and set an IP address of a server other than the server selected in step 12.



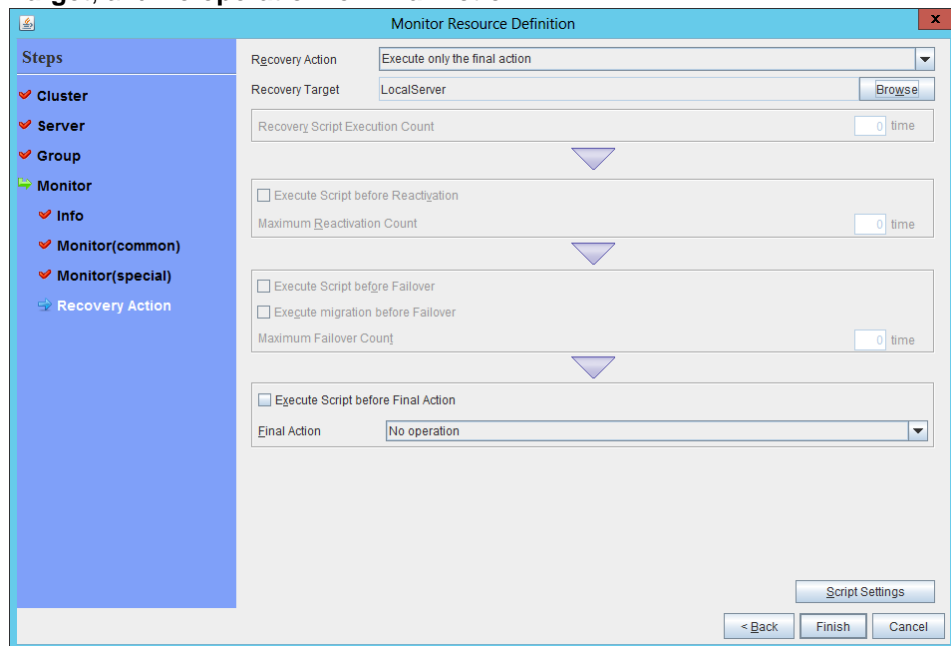
14. Click **Next**.



The 'Monitor Resource Definition' dialog box is shown with the 'Common' tab selected. The 'IP Addresses' section contains a table with one entry: '10.5.0.110'. To the right of the table are buttons for 'Add', 'Remove', and 'Edit'. At the bottom of the dialog are buttons for '< Back', 'Next >', and 'Cancel'.

IP Address
10.5.0.110

15. The **Recovery Action** page is displayed.
Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final Action**.



The 'Monitor Resource Definition' dialog box is shown with the 'Recovery Action' tab selected. The 'Recovery Action' dropdown is set to 'Execute only the final action'. The 'Recovery Target' is 'LocalServer'. The 'Recovery Script Execution Count' is '0' time. The 'Execute Script before Reactivation' checkbox is unchecked. The 'Maximum Reactivation Count' is '0' time. The 'Execute Script before Failover' checkbox is unchecked. The 'Execute migration before Failover' checkbox is unchecked. The 'Maximum Failover Count' is '0' time. The 'Execute Script before Final Action' checkbox is unchecked. The 'Final Action' dropdown is set to 'No operation'. At the bottom right are buttons for 'Script Settings', '< Back', 'Finish', and 'Cancel'.

16. 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 Chapter 5, “Monitor resource details” 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.

Monitor Resource Definition

Steps

- Cluster
- Server
- Group
- Monitor
 - Info
 - Monitor(common)
 - Monitor(special)
 - Recovery Action

Monitor Resource Definition

Type: multi-target monitor

Name: mtw1

Comment:

Get Licence Info

Description

Select the type of monitor resource and enter its name.

< Back Next > Cancel

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

Monitor Resource Definition

Steps

- Cluster
- Server
- Group
- Monitor
 - 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

Nics Value: 0

Choose servers that execute monitoring: Server

< Back Next > Cancel

5. The **Monitor (special)** page 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**.

Monitor Resources		Available Monitor Resources	
Monitor Resource	Type	Monitor Resource	Type
genw1	genw		
ipw1	ipw		
ipw2	ipw		

6. Click **Next**.
The **Recovery Action** page 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**.

Recovery Action: Execute only the final action

Recovery Target: LocalServer

Recovery Script Execution Count: 0 time

☐ Execute Script before Reactivation

Maximum Reactivation Count: 0 time

☐ Execute Script before Failover

☐ Execute migration before Failover

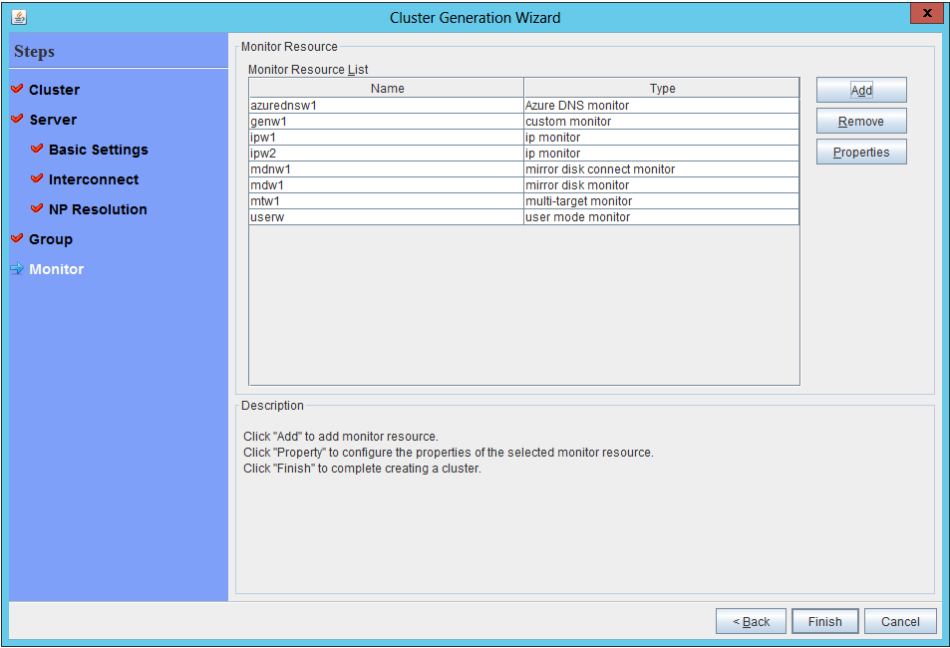
Maximum Failover Count: 0 time

☐ Execute Script before Final Action

Final Action: Stop the cluster service and shutdown OS

7. Click **Finish**.

8. Click **Finish** to finish setting.



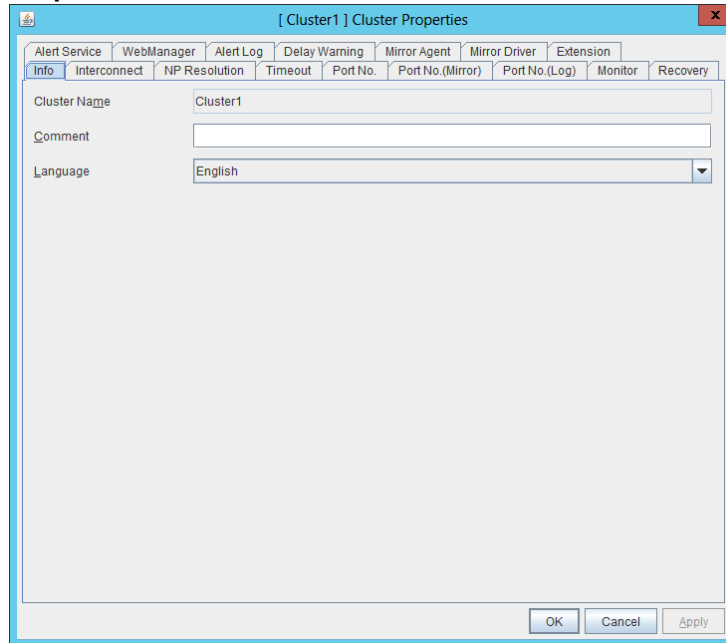
4) Setting the cluster properties

For details about the cluster properties, see “Cluster properties” in Chapter 2, “Functions of the Builder” in the *Reference Guide*.

◆ Cluster properties

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

1. Enter **Config Mode** from WebManager, right-click a cluster name, and select **Properties**.



2. Select the **Timeout** tab. For **Timeout of Heartbeat**, specify a value calculated by "A+B+30 ("Time that it took for the multi-target monitor resource to detect an error"+30 seconds)."

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)

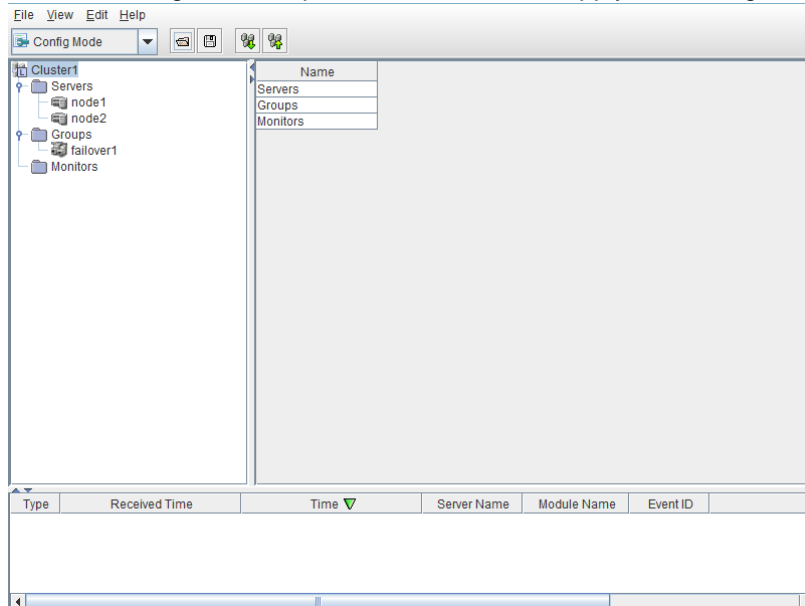
Note: If **Timeout of Heartbeat** is shorter than the time that it took for the multi-target monitor resource to detect an error, a heartbeat timeout will be detected before starting the NP resolution processing. In this case, the same service may start doubly in the cluster because the service also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

The screenshot shows the "[Cluster1] Cluster Properties" dialog box with the "Timeout" tab selected. The "Heartbeat" section is expanded, showing "Interval" set to 3 sec and "Timeout" set to 120 sec. Other settings include "Server Sync Wait Time" at 5 min and "Server Internal Timeout" at 180 sec. At the bottom are "Initialize", "OK", "Cancel", and "Apply" buttons.

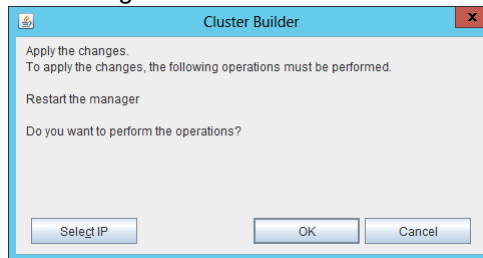
3. Click **OK**.

5) Applying the settings and starting the cluster

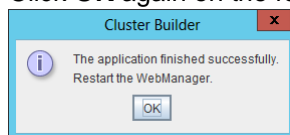
1. After all settings are complete, click the icon to apply the settings under the menu.



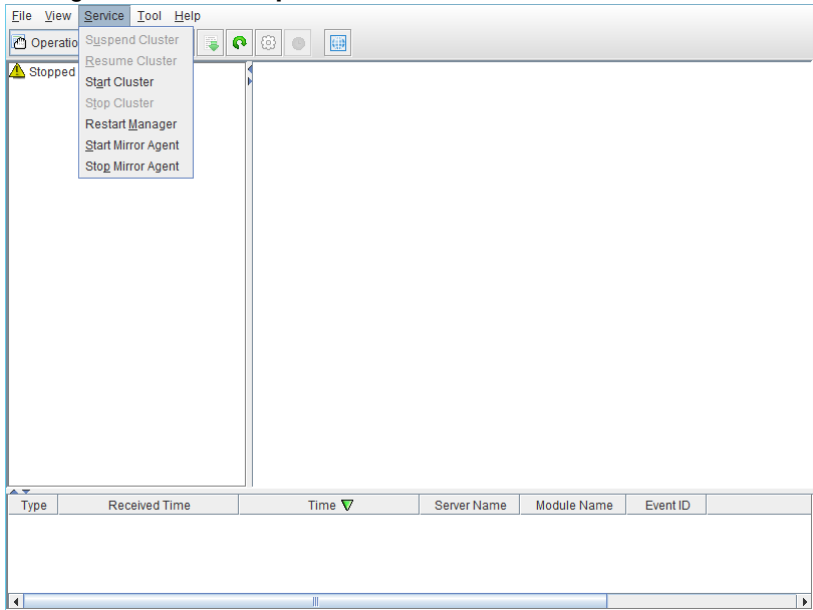
2. The dialog box to confirm to restart the manager is displayed.



3. Click **OK**.
4. Click **OK** again on the following dialog box.



5. Change the mode to **Operation Mode** and click **Start Cluster** from the **Service** menu.



3.4 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** blade, and then select **Summary**. Check the DNS servers displayed on the upper right of the window (name server 1, name server 2, name server 3, and name server 4 in the window example).
3. Confirm that the relevant record set exists in the DNS servers checked in the above step by executing the nslookup command as follows:
`$ nslookup test-record1.cluster1.zone <DNS_servers_checked_in_the_above_step>`
4. On the Microsoft Azure portal, delete an A record from the DNS zone. This causes azurednsw1 to detect a monitoring error. On the **DNS zone** blade, select cluster1.zone and then **Summary**.
5. Select the record you want to delete and click **Delete**. When the deletion confirmation dialog box is displayed, select **Yes**.
6. When the time specified for **Interval** of azurednsw1 elapses, the failover group (failover1) enters an error status and fails over to 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.

Chapter 4 Cluster Creation Procedure (for an HA Cluster Using an Internet Facing Load Balancer)

4.1 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	
Name	Vnet1
Resource group location	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 name	TestGroup1
Location	Japan East
Load balancer setting	
Name	TestLoadBalancer
Type	Public
Public IP address: Name	TestLoadBalancerPublicIP
Public IP address: Assignment	Static
Resource group	Vnet1
Location	Japan East
Backend pool: Name	TestBackendPool
Associated to	Availability set
Target virtual machine	node1 node2
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	
Name	TestHTTP
Protocol	TCP
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		
VM disk type	HDD	
User name	testlogin	
Password	PassWord_123	
Resource group name	TestGroup1	
Location	Japan East	
Storage account setting		
Name	clstorageacc1	
Performance	Standard	
Replication	Locally-redundant storage (LRS)	
Network security group setting		
Name	NetSecGroup1	
Availability set setting		
Name	AvailabilitySet1	
Update domains	5	
Fault domains	3	
Diagnostics storage account setting		
Name	clstorageaccdiag1	
Performance	Standard	
Replication	Locally-redundant storage (LRS)	
IP configuration setting		
IP address	10.5.0.110	10.5.0.111
Blob storage setting		
Name	Node1Blob	Node2Blob
Source type	New (empty disk)	
Account type	Standard (HDD)	
Size	20	

- EXPRESSCLUSTER settings (cluster properties)

Setting item	Setting value	
	node1	node2
Cluster Name	Cluster1	
Server Name	node1	node2
Timeout Tab: Heartbeat timeout	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
Azure probe port resource	Name	azurepp1
	Probe port	26001 (Value specified for Port of Health probe)

- EXPRESSCLUSTER settings (monitor resource)

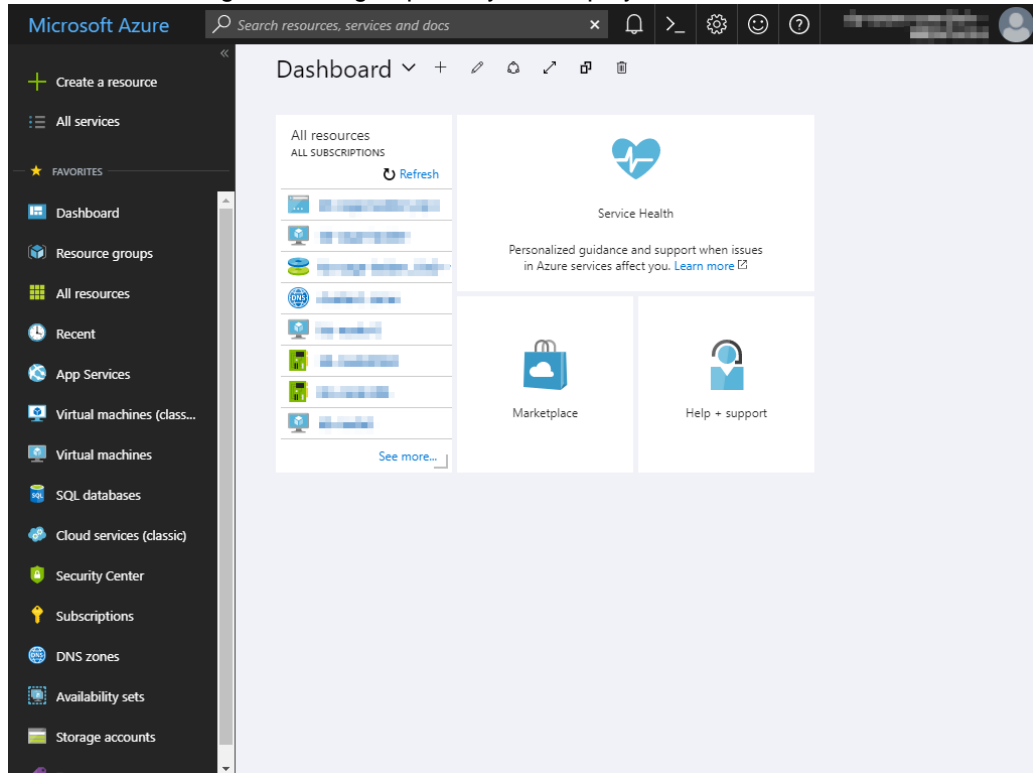
Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	-	-
Azure probe port monitor resource	Name	azureppw1
	Recovery Target	azurepp1
Azure load balance monitor resource	Monitor resource name	aurelbw1
	Recovery Target	azurepp1
Custom monitor resource	Name	genw1
	Script created with this product	On
	Monitor Type	Synchronous
	Normal Return Value	0
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
IP monitor resource	Name	ipw1
	Server to monitor	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
	Execute Script before Final Action	On
	Timeout	30

4.2 Configuring Microsoft Azure

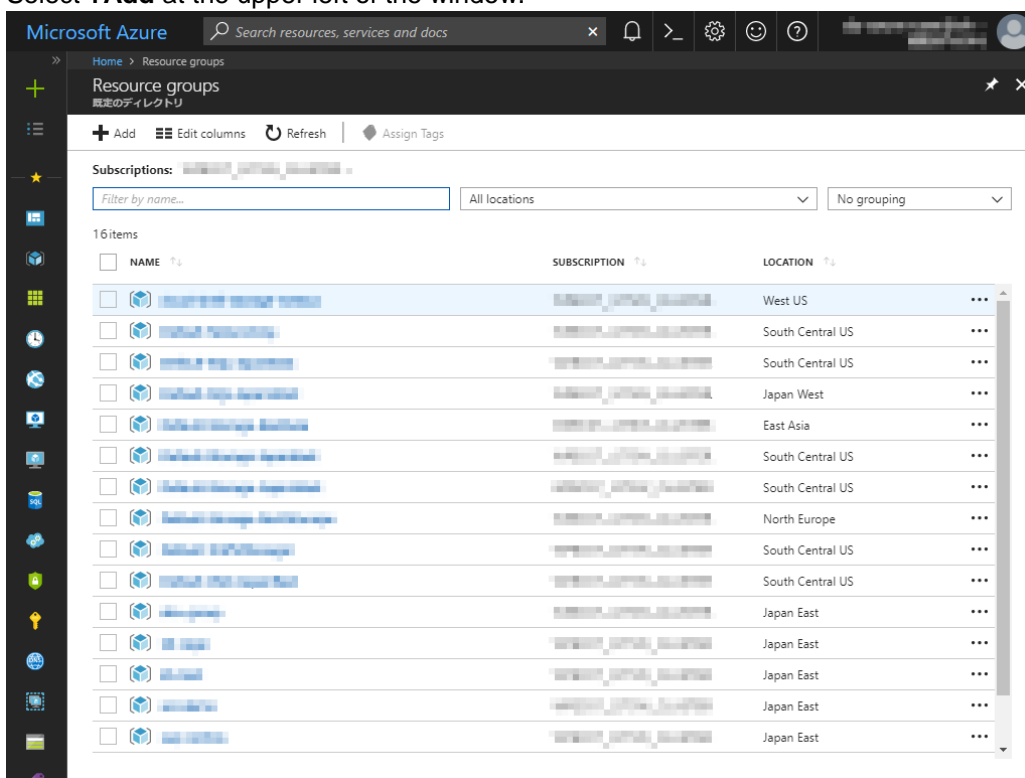
1) Creating a resource group

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

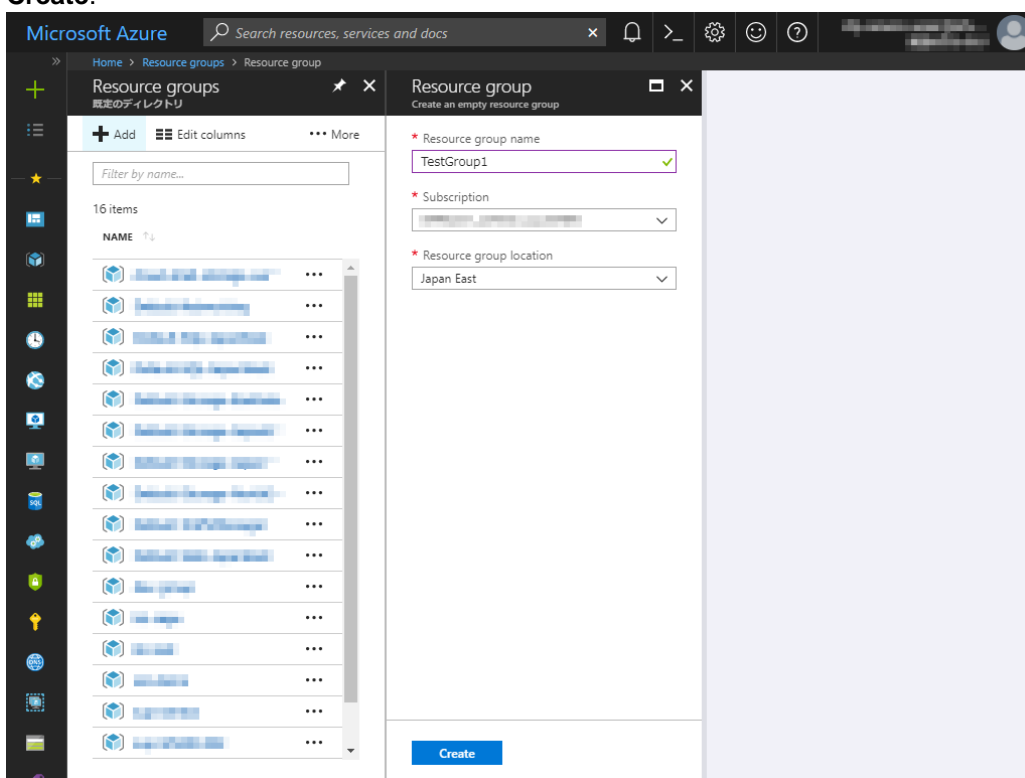
1. Select **Resource groups** or the resource group icon in the menu on the left side of the window. If there are existing resource groups, they are displayed in a list.



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



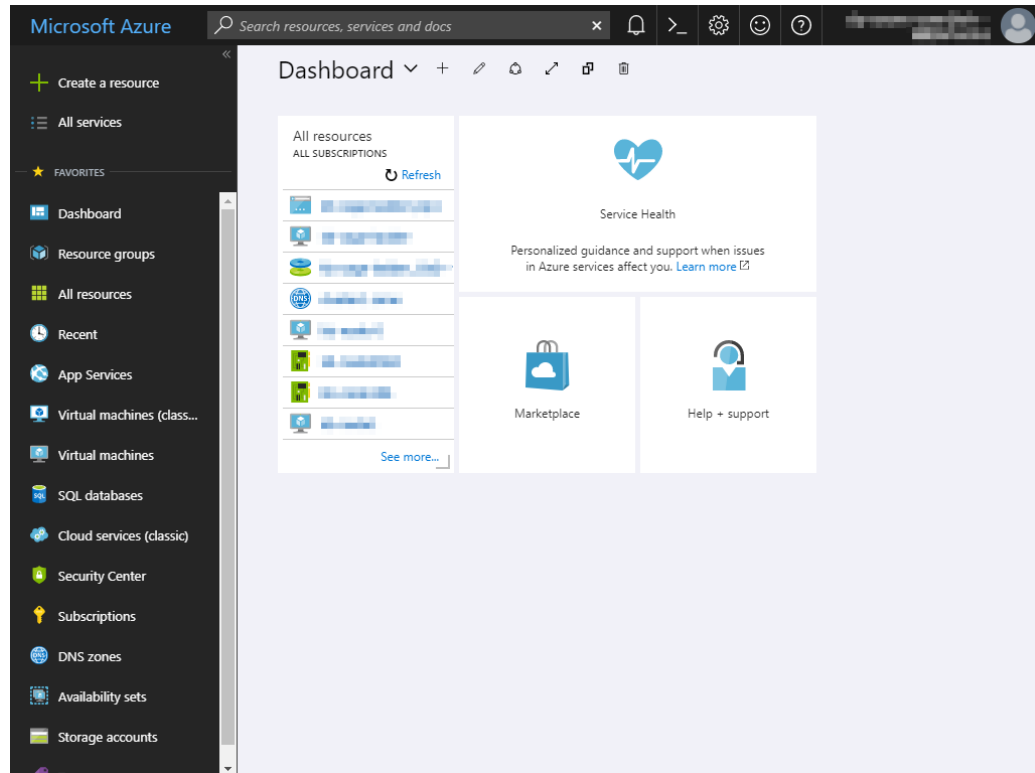
3. Specify **Resource group name**, **Subscription**, and **Resource group location**, and click **Create**.



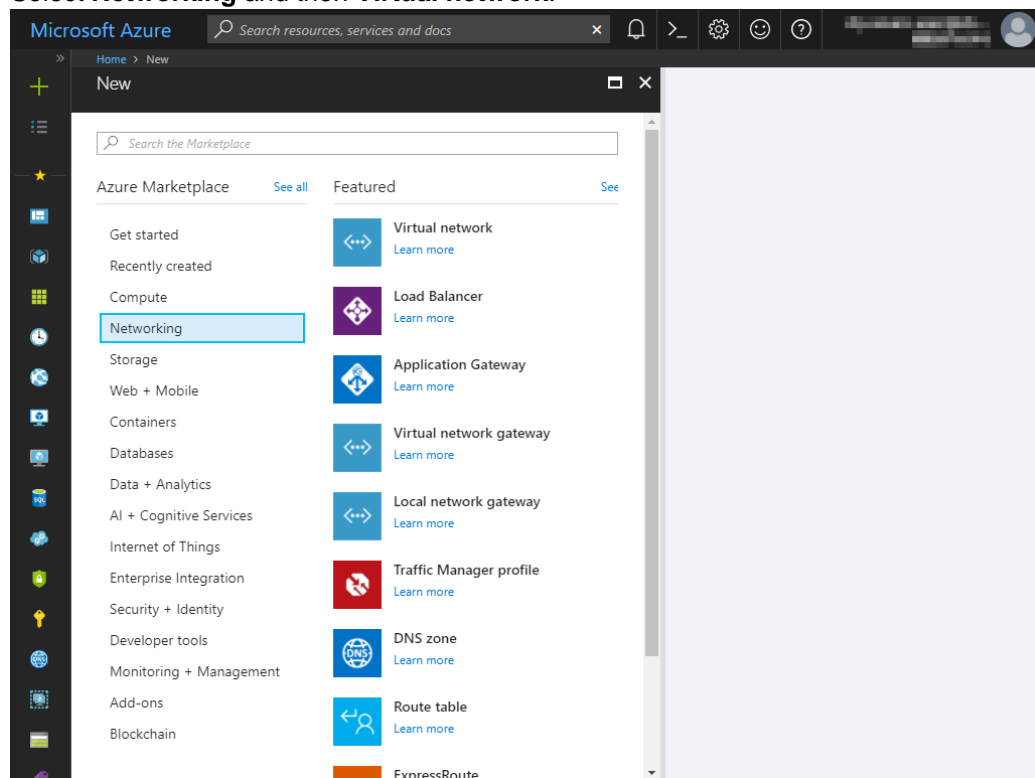
2) Creating a virtual network

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

1. Select **+Create a resource** or the **+** icon in the menu on the left side of the window.



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



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

The screenshot shows the 'Create virtual network' form in the Microsoft Azure portal. The form is titled 'Create virtual network' and is located under the 'Home > New > Create virtual network' breadcrumb. The form contains the following fields and options:

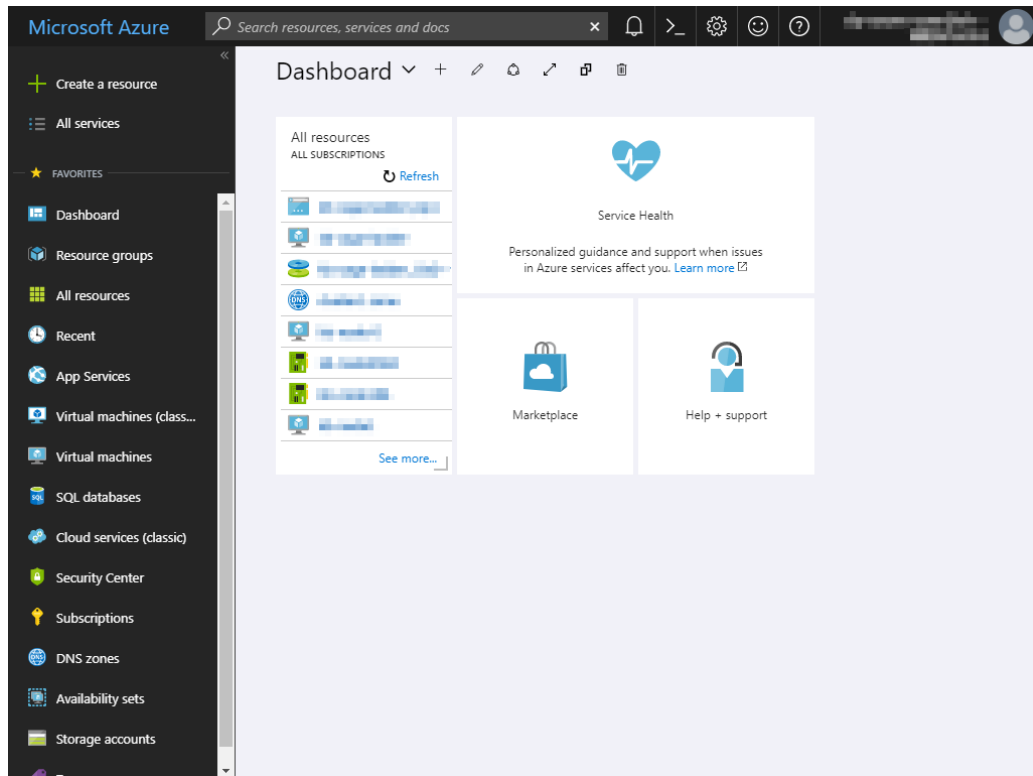
- Name:** Vnet1 (with a green checkmark)
- Address space:** 10.5.0.0/24 (with a green checkmark). Below the input, it says '10.5.0.0 - 10.5.0.255 (256 addresses)'.
- Subscription:** A dropdown menu showing a blurred subscription ID.
- Resource group:** ☐ Create new ☒ Use existing. Below, a dropdown menu shows 'TestGroup1'.
- Location:** A dropdown menu showing 'Japan East'.
- Subnet:**
 - Name:** Vnet1-1 (with a green checkmark)
 - Address range:** 10.5.0.0/24 (with a green checkmark). Below the input, it says '10.5.0.0 - 10.5.0.255 (256 addresses)'.
- Service endpoints:** ☒ Disabled ☐ Enabled
- Pin to dashboard:** ☐
- Create:** A blue button.
- Automation options:** A link.

3) Creating a virtual machine

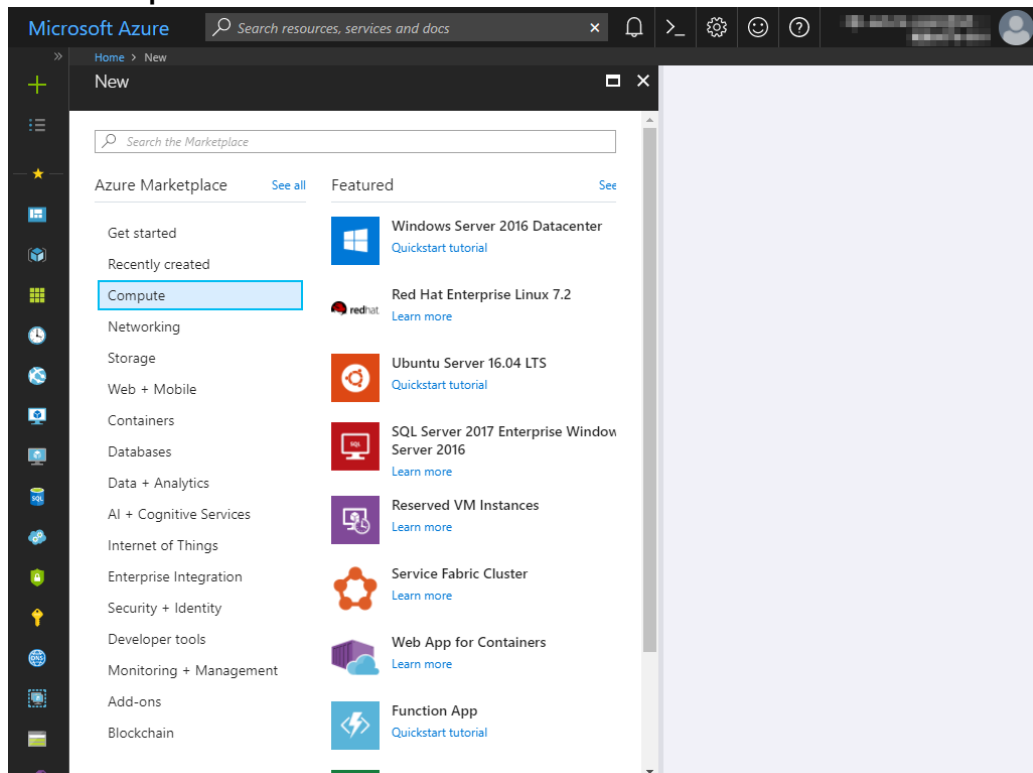
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create virtual machines and disks following the steps below.

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

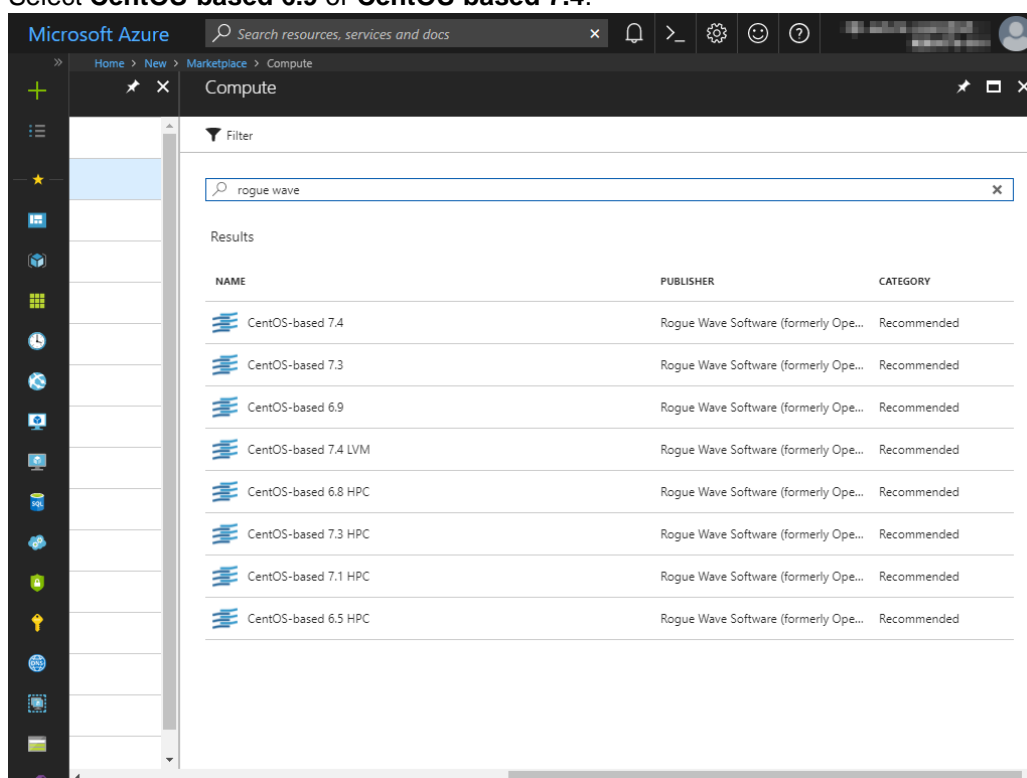
1. Select **+Create a resource** or the **+** icon in the menu on the left side of the window.



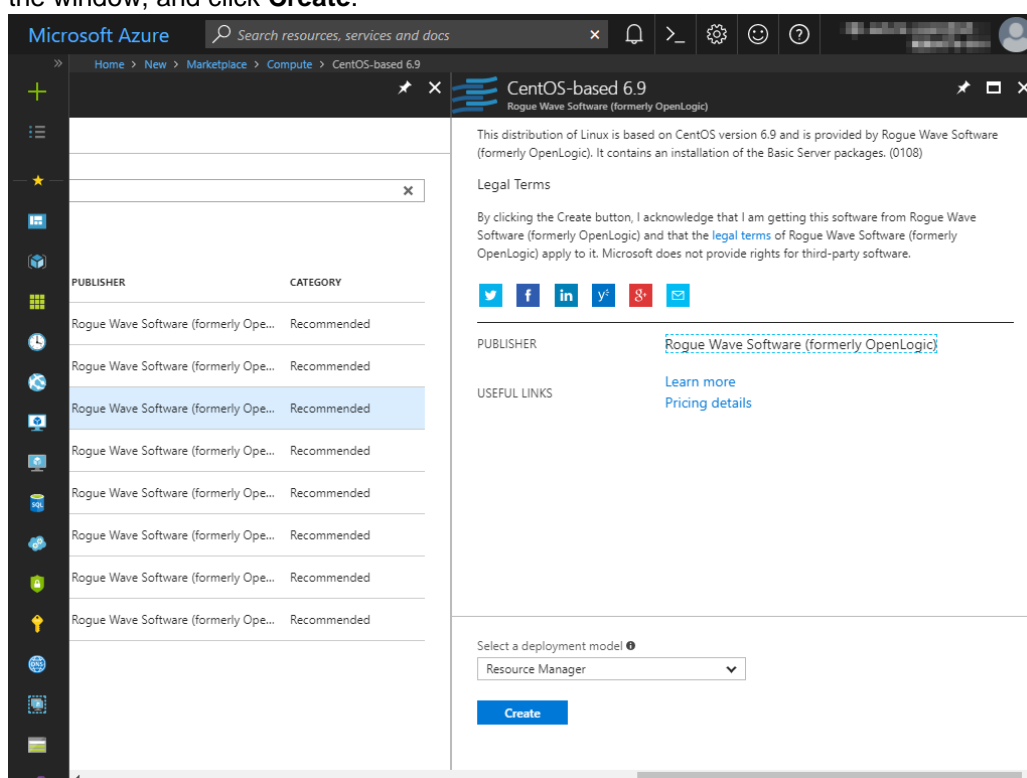
2. Select **Compute** and then **See all**.



3. Select **CentOS-based 6.9** or **CentOS-based 7.4**.



4. Confirm that **Resource Manager** is selected for **Select a deployment model** at the bottom of the window, and click **Create**.



5. The **Basics** blade is displayed. Specify **Name**, **VM disk type**, **User name**, **Password**, **Confirm password**, **Subscription**, **Resource group name**, and **Location**, and click **OK**. For **Name**, specify node1 for node1 and node2 for node2.

Microsoft Azure Search resources, services and docs

Home > New > Marketplace > Compute > CentOS-based 6.9 > Create virtual machine > Basics

Create virtual machine Basics

1 Basics Configure basic settings

2 Size Choose virtual machine size

3 Settings Configure optional features

4 Summary CentOS-based 6.9

* Name node1 ✓

VM disk type HDD

* User name testlogin

* Authentication type SSH public key Password

* Password

* Confirm password

Subscription

* Resource group Create new Use existing TestGroup1

* Location Japan East

OK

6. The **Choose a size** blade is displayed. Select the size appropriate for the usage purpose of the virtual machines from the list and click **Select**. In this guide, **A1 Standard** is selected.

Microsoft Azure Search resources, services and docs

Home > New > Marketplace > Compute > CentOS-based 6.9 > Create virtual machine > Choose a size

Create virtual machine Choose a size

Browse the available sizes and their features

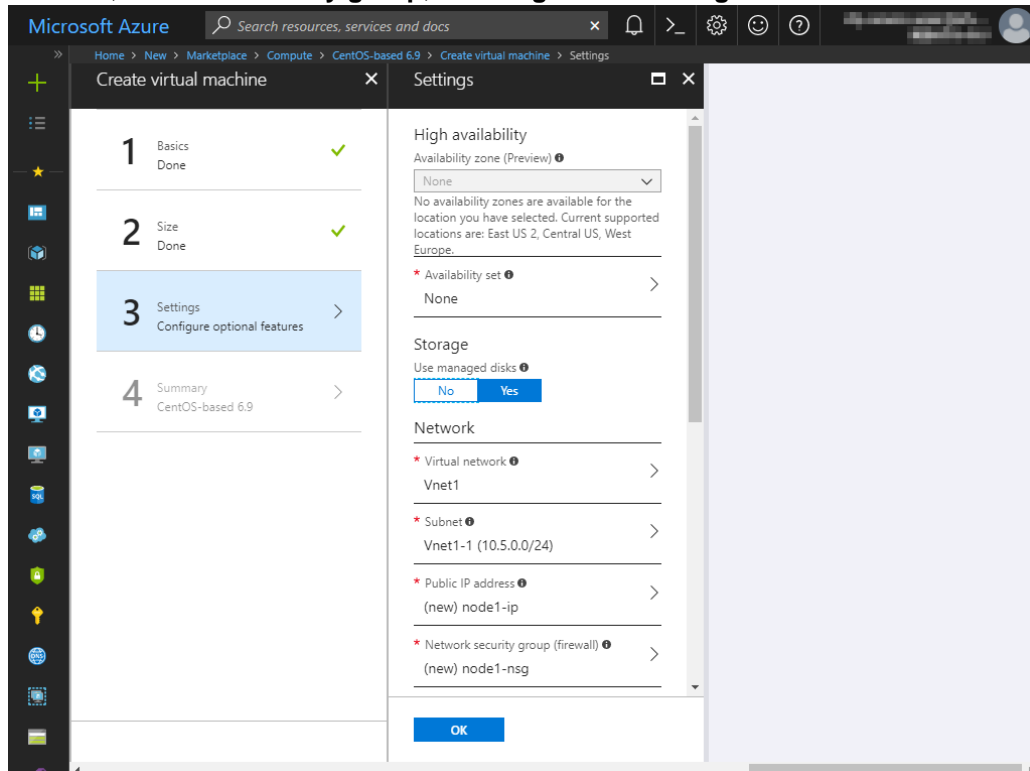
Supported disk type HDD Minimum vCPUs 1 Minimum memory (GiB) 0

★ Recommended | View all

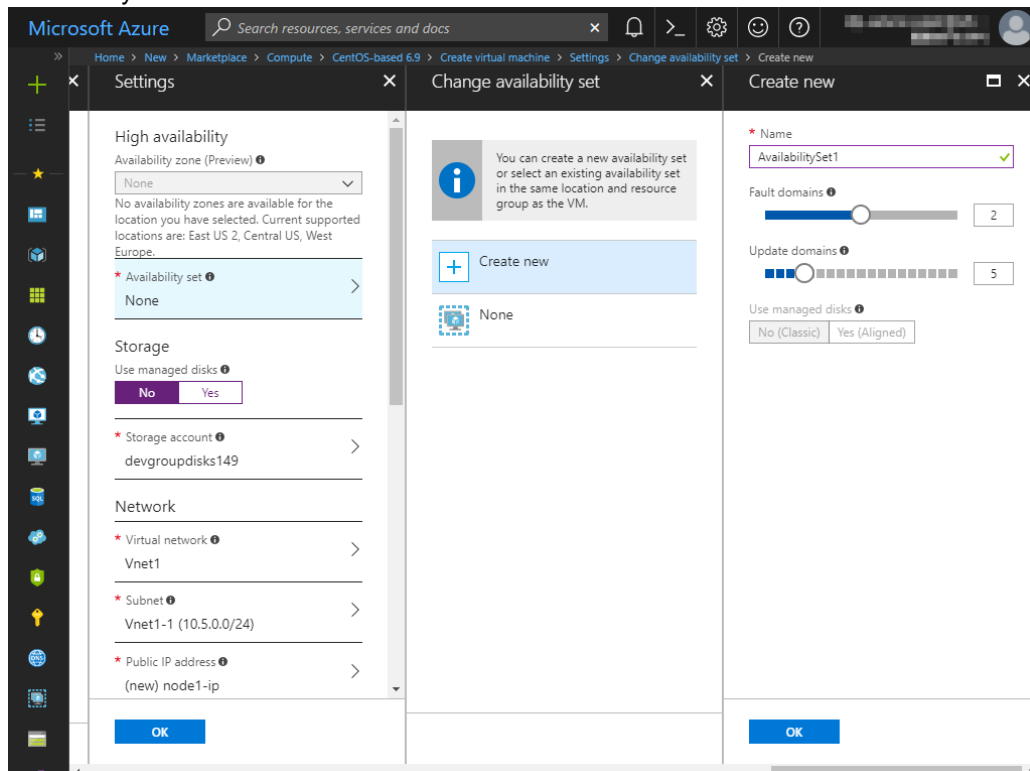
D1_V2 Standard ★	D1 Standard ★	A1 Standard ★
1 vCPU	1 vCPU	1 vCPU
3.5 GB	3.5 GB	1.75 GB
4 Data disks	4 Data disks	2 Data disks
2x500 Max IOPS	2x500 Max IOPS	2x500 Max IOPS
50 GB Local SSD	50 GB Local SSD	
Load balancing	Load balancing	Load balancing
7,015.92 JPY/MONTH (ESTIMATED)	7,343.28 JPY/MONTH (ESTIMATED)	3,935.76 JPY/MONTH (ESTIMATED)

Select

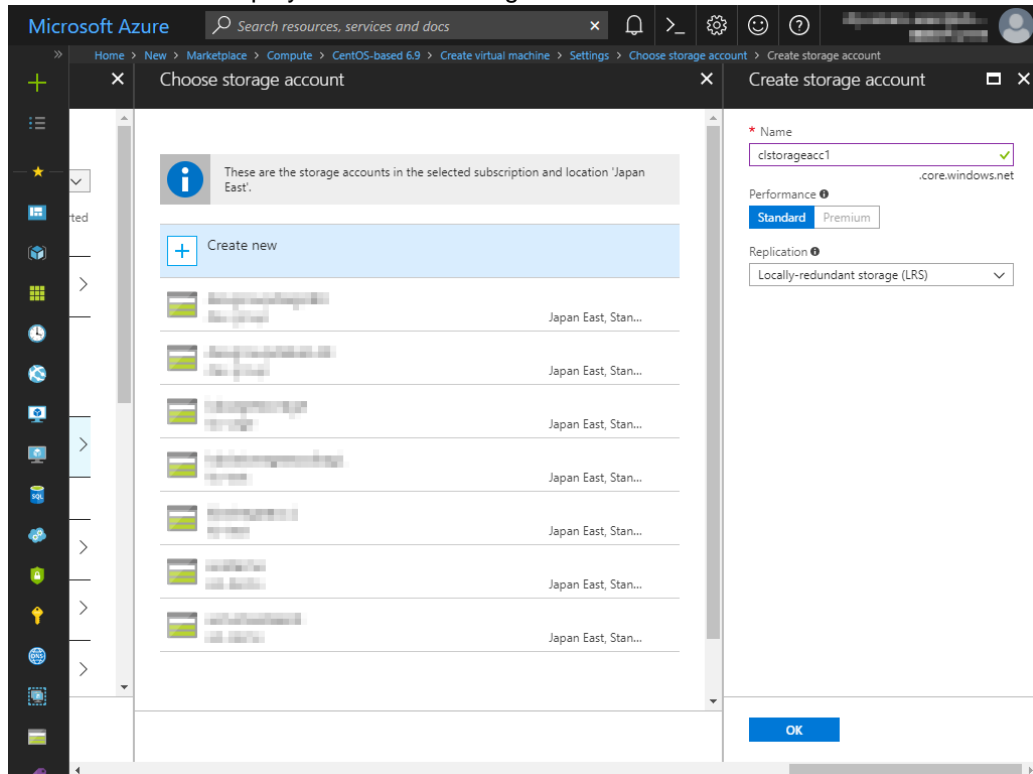
7. The **Settings** blade is displayed. Specify **Availability set**, **Storage account**, **Public IP address**, **Network security group**, and **Diagnostics storage account**.



8. Select **No** for **Use managed disks** for **Storage**.
9. Return to the **Settings** blade and select **Availability set**. For node1, the **Change availability set** blade is displayed. Select **Create new**. Specify **Name**, **Fault domains**, and **Update domains**, and click **OK**. For node2, the **Change availability set** blade is displayed. Select AvailabilitySet1 created for node1.

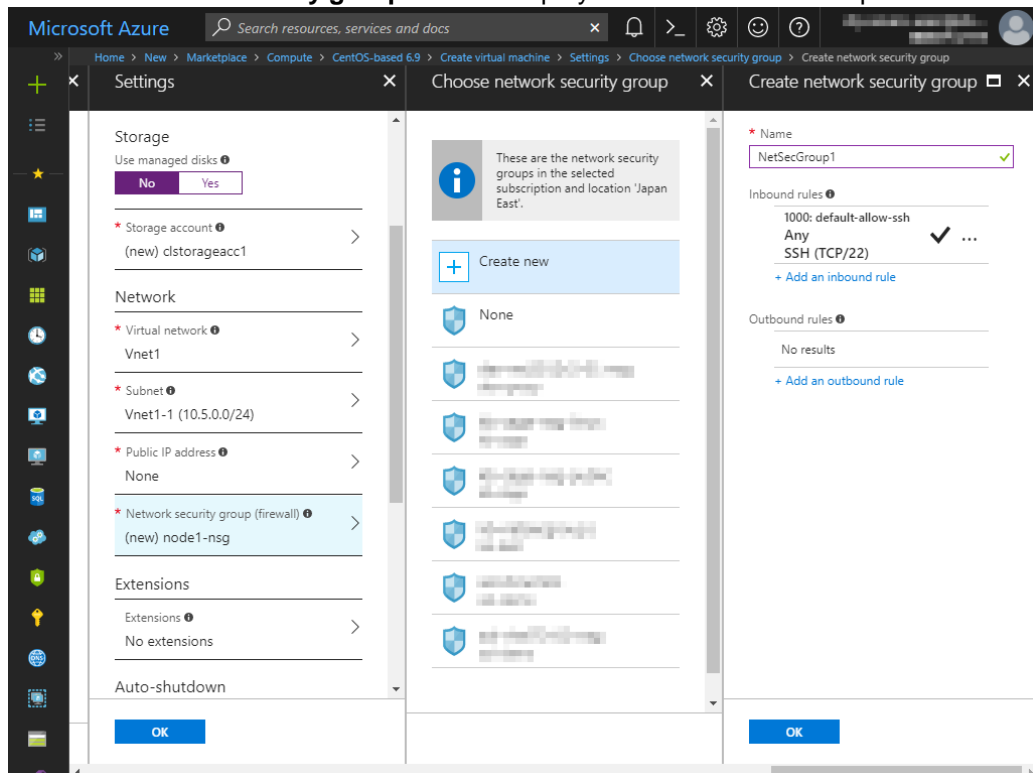


10. Select **Storage account**. For node1, the **Create storage account** blade is displayed. Specify **Name**, **Performance**, and **Replication**, and click **OK**. For node2, the **Choose storage account** blade is displayed. Select clstorageacc1 created for node1.

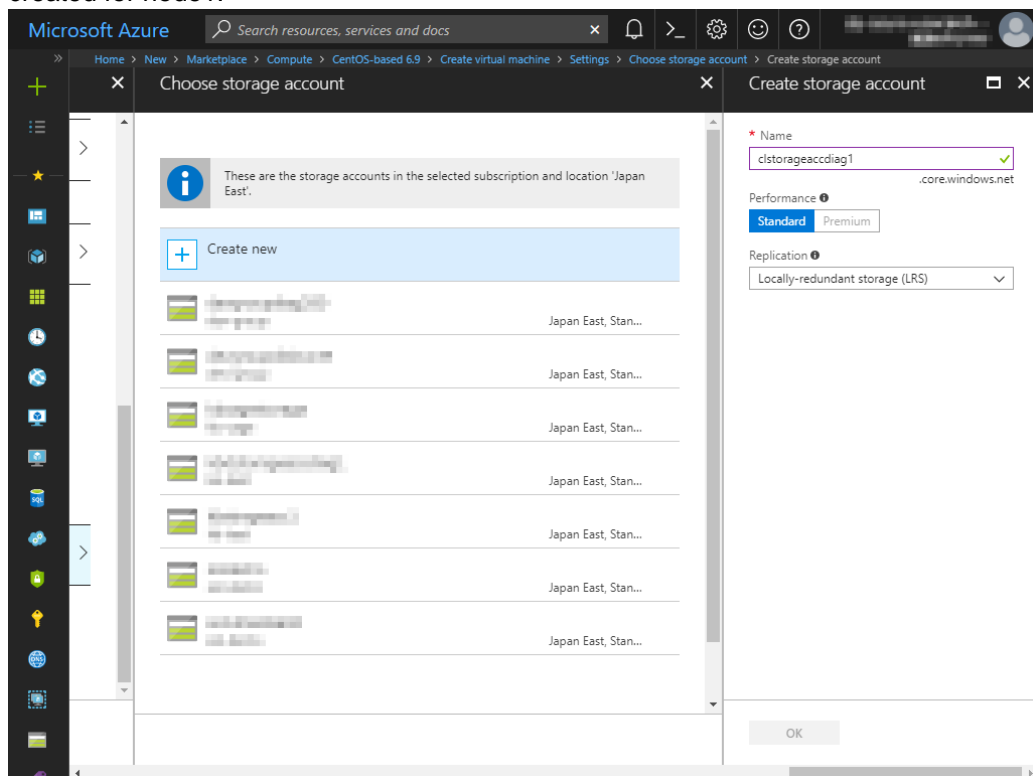


11. Return to the **Settings** blade and select **Public IP address**.
12. The **Choose public IP address** blade is displayed. Select **None**. Ignore the **Create public IP address** blade.

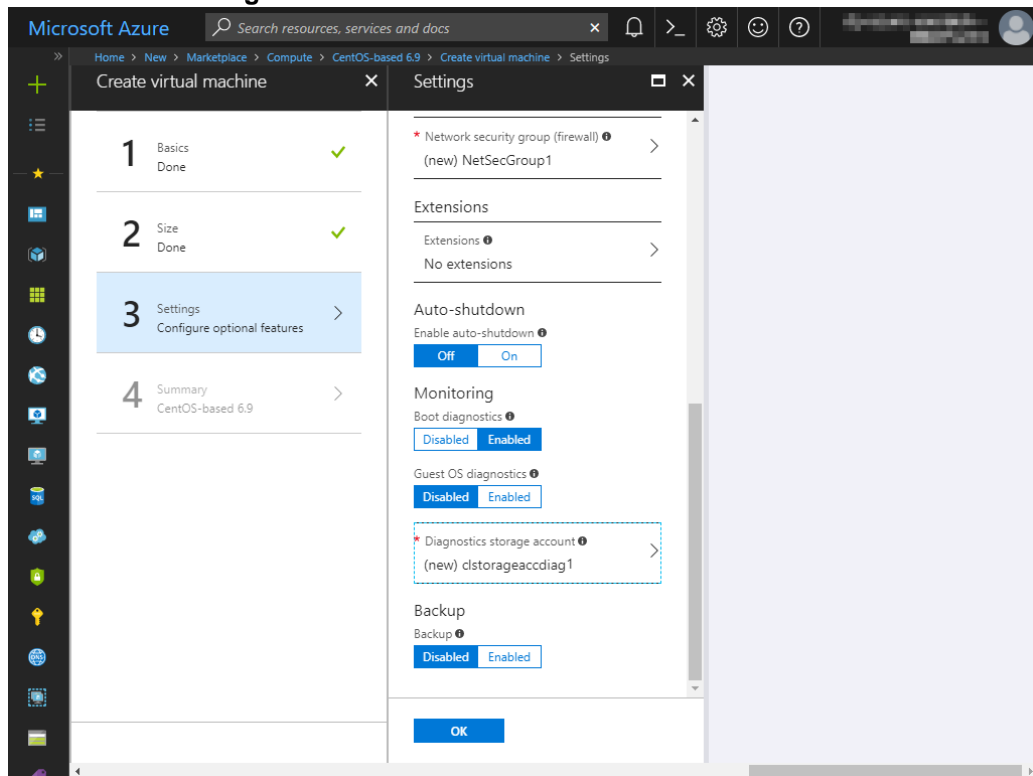
13. Return to the **Settings** blade and select **Network security group**. For node1, the **Create network security group** blade is displayed. Specify **Name** and click **OK**. For node2, the **Choose network security group** blade is displayed. Select NetSecGroup1 created for node1.



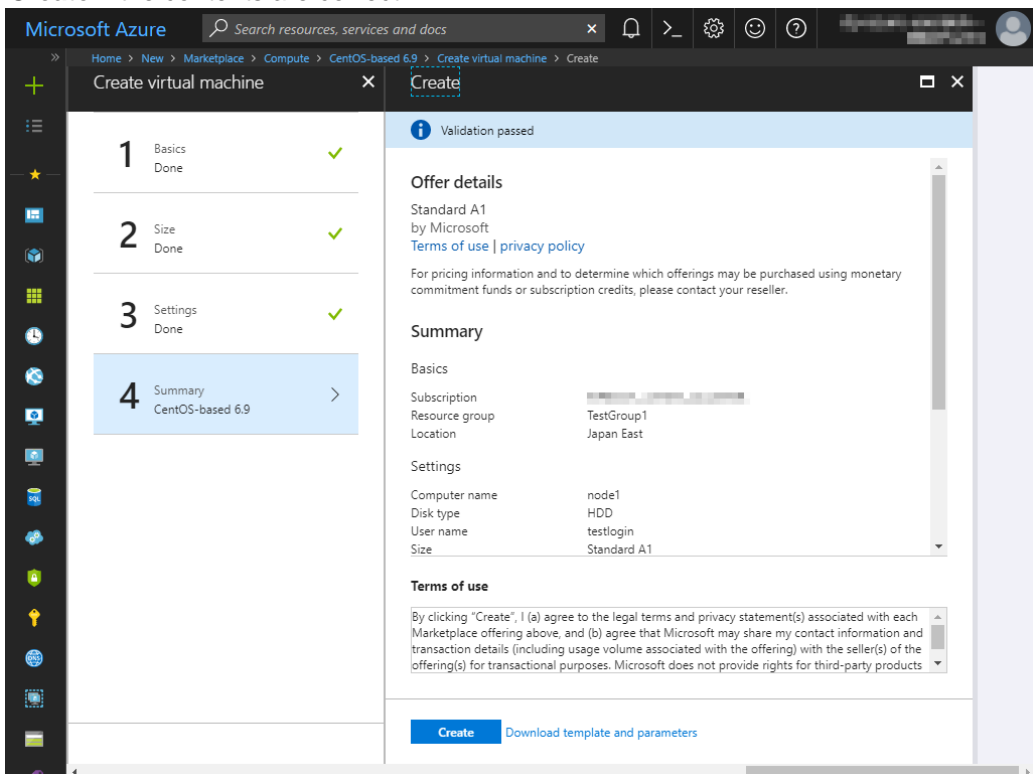
14. Return to the **Settings** blade and select **Diagnostics storage account**. For node1, the **Create storage account** blade is displayed. Specify **Name**, **Performance**, and **Replication**, and click **OK**. For node2, the **Choose storage account** blade is displayed. Select clstorageacctdiag1 created for node1.



15. Return to the **Settings** blade and click **OK**.



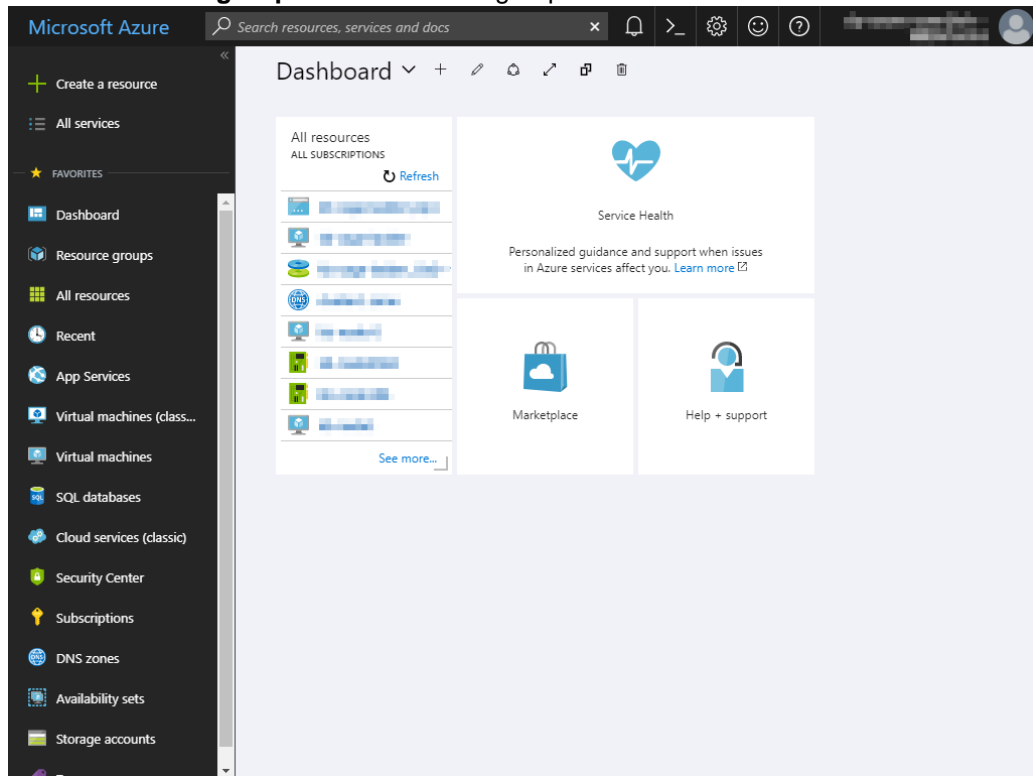
16. The **Create** blade is displayed. Check the contents displayed on the **Create** blade and click **Create** if the contents are correct.



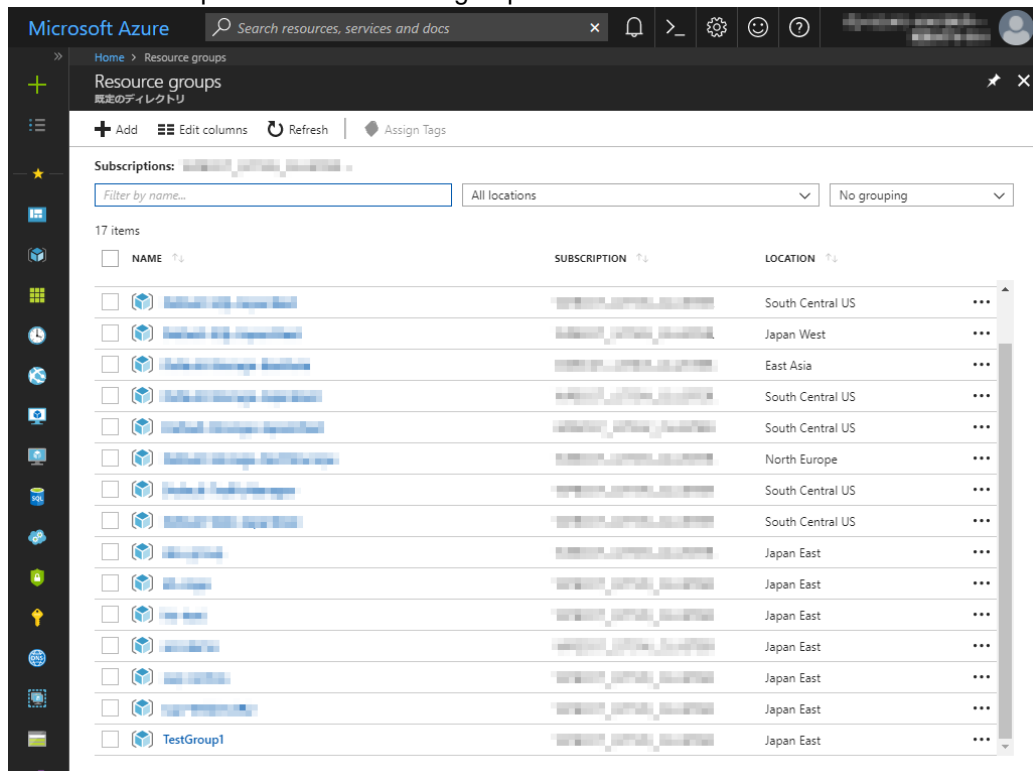
4) Setting a private IP address

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 **Resource groups** or the resource group icon in the menu on the left side 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.

Microsoft Azure

Home > Resource groups > TestGroup1

TestGroup1
Resource group

Subscription (change) [Subscription ID] Deployments: 3 Succeeded

Filter by name... All types All locations No

9 items ☐ Show all resources

NAME	TYPE	LOCATION
AvailabilitySet1	Availability set	Japan East
clstorageacct1	Storage account	Japan East
clstorageacctdiag1	Storage account	Japan East
NetSecGroup1	Network security group	Japan East
node1	Virtual machine	Japan East
node1435	Network interface	Japan East
node2	Virtual machine	Japan East
node2680	Network interface	Japan East
Vnet1	Virtual network	Japan East

4. Select **Networking**.

Microsoft Azure

Home > Resource groups > TestGroup1 > node1 - Networking

node1 - Networking
Virtual machine

Attach network interface Detach network interface

Network Interface: node1435 Effective security rules Topology

Virtual network/subnet: Vnet1/Vnet1-1 Public IP: None Private IP: 10.5.0.4

INBOUND PORT RULES

Network security group NetSecGroup1 (attached to network interface: node1435)
Impacts 0 subnets, 2 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATI...	ACTION
1000	default-allow-ssh	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNet...	VirtualNet...	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

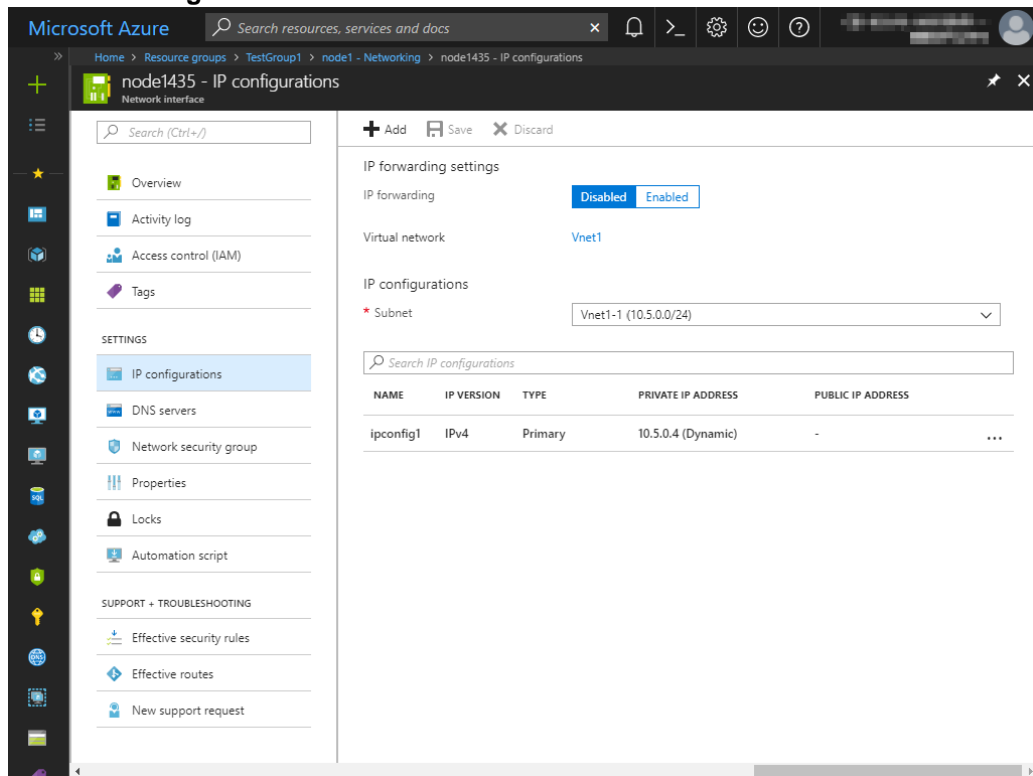
OUTBOUND PORT RULES

Network security group NetSecGroup1 (attached to network interface: node1435)
Impacts 0 subnets, 2 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATI...	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNet...	VirtualNet...	Allow
65001	AllowInternetOutBou...	Any	Any	Any	Internet	Allow

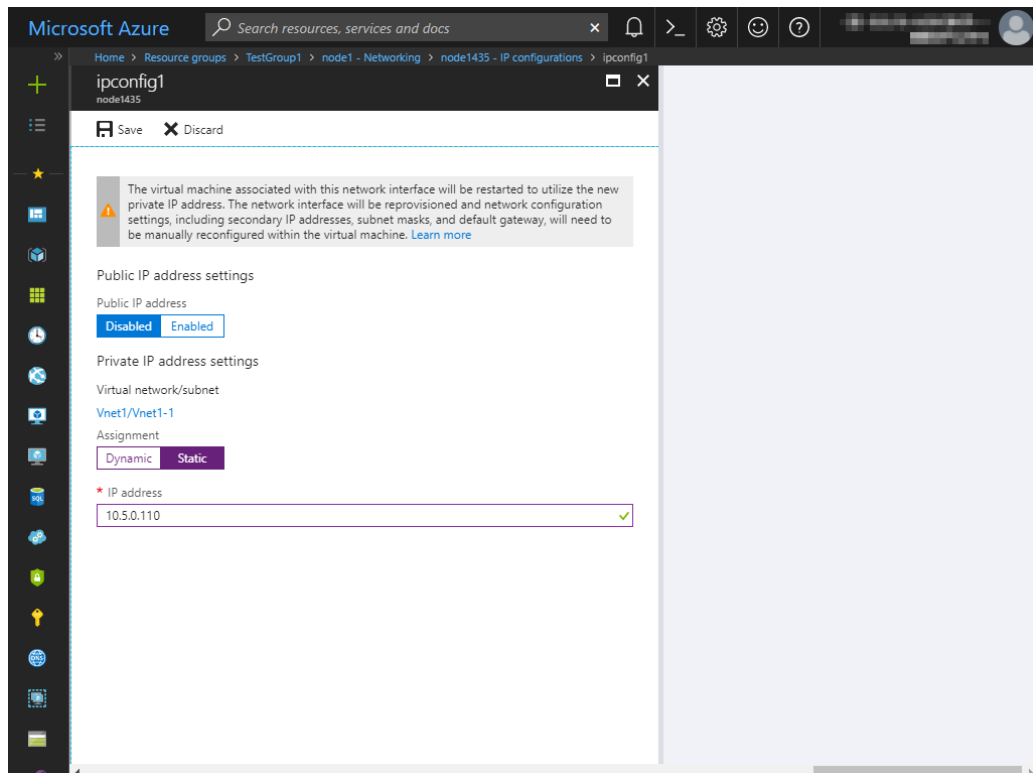
5. Select a network interface displayed in the list. The network interface name is generated automatically.

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.

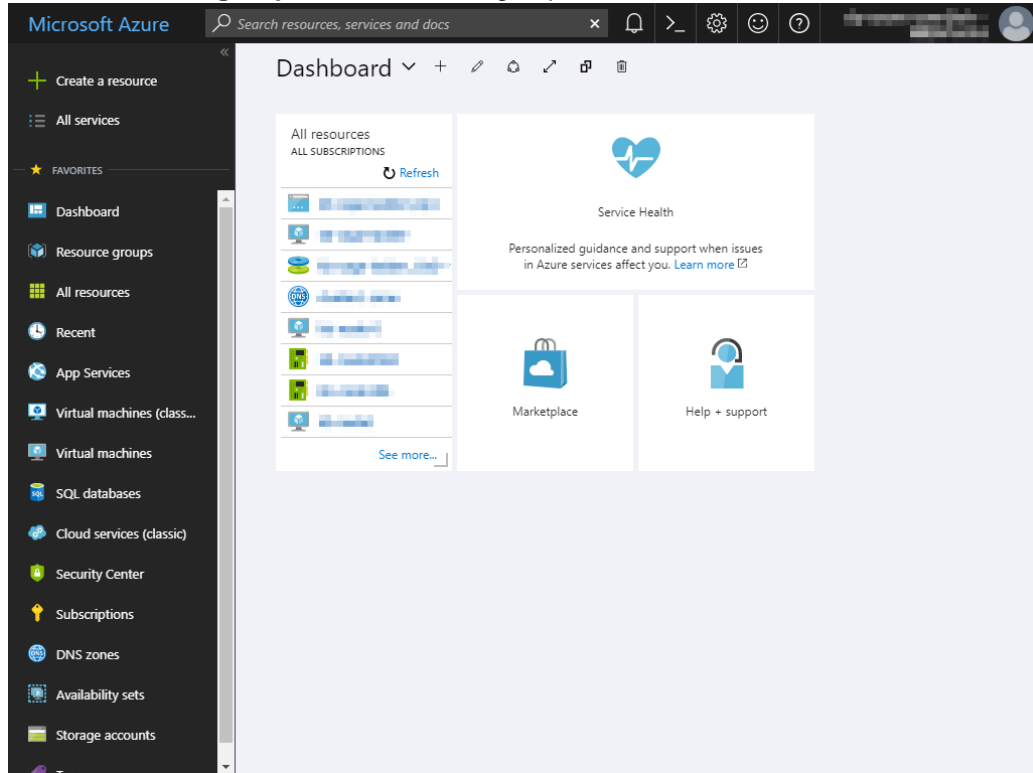


9. The virtual machines restart automatically so that new private IP addresses can be used.

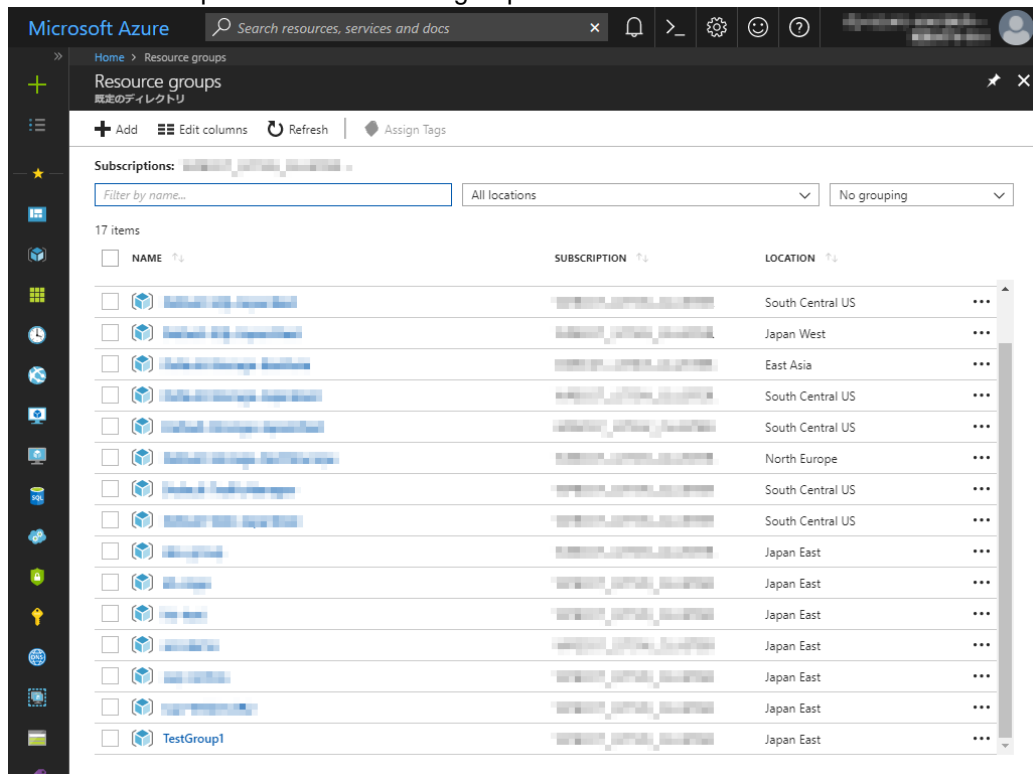
5) Adding Blob storage

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and add Blob storage to be used for a mirror disk (cluster partition or data partition). Change the settings of node1 and then node2.

1. Select **Resource groups** or the resource group icon in the menu on the left side of the window.



2. Select TestGroup1 from the resource group list.



Cluster Creation Procedure (for an HA Cluster Using an Internet Facing Load Balancer)

3. The summary of TestGroup1 is displayed. Select virtual machine node1 or node2 to which to add Blob storage from the item list and select **Disk**.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1

TestGroup1 Resource group

Subscription (change) Deployments 3 Succeeded

Subscription ID

Filter by name... All types All locations No

9 items Show all resources

NAME	TYPE	LOCATION
AvailabilitySet1	Availability set	Japan East
clstorageacct1	Storage account	Japan East
clstorageacctdiag1	Storage account	Japan East
NetSecGroup1	Network security group	Japan East
node1	Virtual machine	Japan East
node1435	Network interface	Japan East
node2	Virtual machine	Japan East
node2680	Network interface	Japan East
Vnet1	Virtual network	Japan East

4. Select **+Add data disk**.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1 > node1 - Disks

node1 - Disks Virtual machine

Edit

OS disk

NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOS
node1	30 GiB	Standard_LRS	Not enabled	Rea

Data disks

None

+ Add data disk

5. The **Attach unmanaged disk** blade is displayed. Click **Browse** right to the **Storage container** text box. For **Name** and **Storage blob name**, the automatically generated default values are entered.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1 > node1 - Disks > Attach unmanaged disk

Attach unmanaged disk

* Name
node1-20180215-104728 ✓

* Source type
New (empty disk) ▾

* Account type
Standard (HDD) ▾

* Size (GiB)
1023

ESTIMATED PERFORMANCE
IOPS limit 500
Throughput limit (MB/s) 60

* Storage container
 [Browse](#)

* Storage blob name
node1-20180215-104728.vhd ✓

OK

6. Select clstorageacc1 from the storage account list.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1 > node1 - Disks > Attach unmanaged disk > Storage accounts

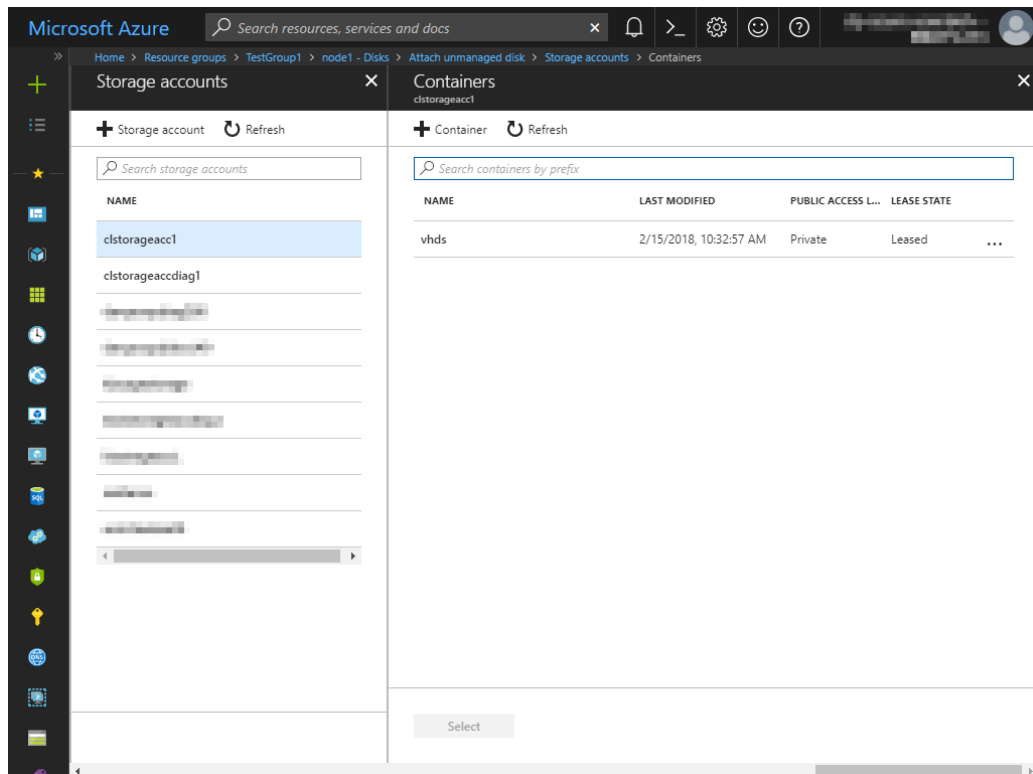
Storage accounts

+ Storage account Refresh

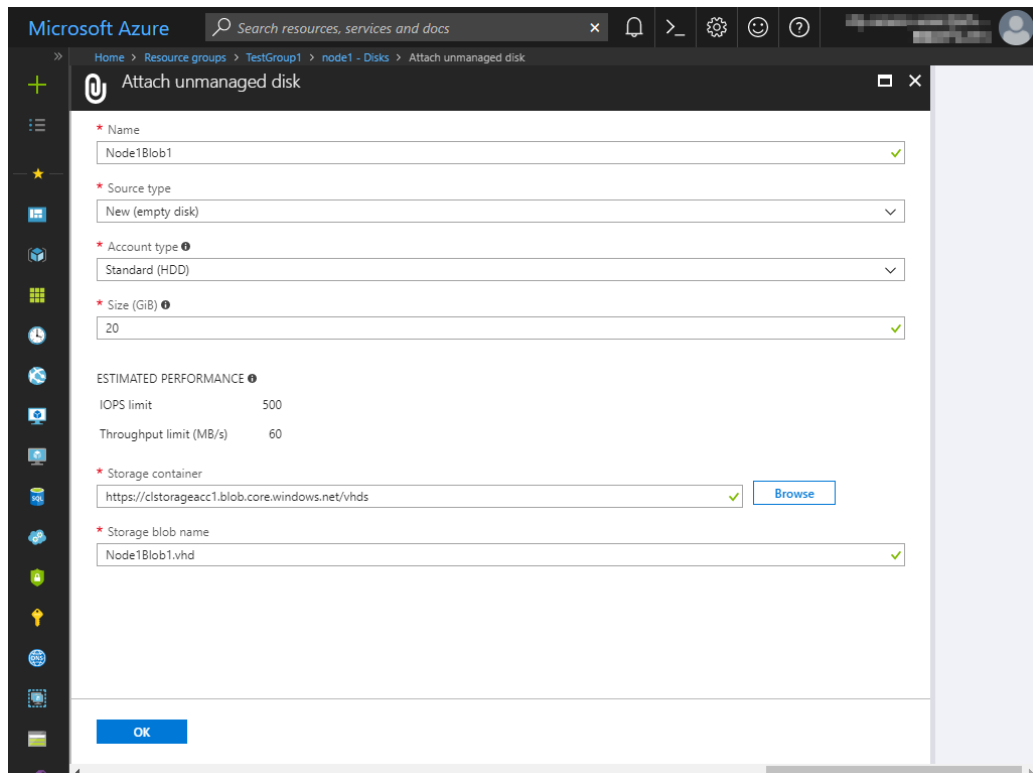
Search storage accounts

NAME	TYPE	RESOURCE GROUP
clstorageacc1	Standard-LRS	TestGroup1
clstorageaccdiag1	Standard-LRS	TestGroup1
clstorageaccdiag2	Standard-LRS	TestGroup1
clstorageaccdiag3	Standard-LRS	TestGroup1
clstorageaccdiag4	Standard-LRS	TestGroup1
clstorageaccdiag5	Standard-LRS	TestGroup1
clstorageaccdiag6	Standard-LRS	TestGroup1
clstorageaccdiag7	Standard-LRS	TestGroup1
clstorageaccdiag8	Standard-LRS	TestGroup1
clstorageaccdiag9	Standard-LRS	TestGroup1

7. Select vhds from the container list and click **Select**.



8. The **Attach unmanaged disk** blade is displayed again. Specify **Name**, **Source type**, **Account type**, **Size**, and **Storage blob name**, and click **OK**. For **Name**, specify Node1Blob for node1 and Node2Blob for node2. For **Storage blob name**, specify Node1Blob.vhd for node1 and Node2Blob.vhd for node2.



9. Click **Save**.

Microsoft Azure Search resources, services and docs

Home > node1 - Disks

node1 - Disks Virtual machine

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

SETTINGS
Networking
Disks
Size
Extensions
Availability set
Configuration
Properties
Locks
Automation script

OPERATIONS

Save Discard

OS disk

NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOS
node1	30 GiB	Standard_LRS	Not enabled	Re

Data disks

LUN	NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOS
0	Node1Blob1	20 GiB	Standard_LRS	Not enabled	Ni

+ Add data disk

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 Blob storage.
 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 Chapter 1, "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

    8     16      73400320      sdb
    8     17      73398272      sdb1
    8      0      31459328       sda
    8      1      31456256      sda1
    8     32      20971520       sdc
```

5. 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. The following is an example of creating one partition including all areas of /dev/sdc.

```
$ sudo fdisk /dev/sdc
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0xe3c83b13.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
```

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

The device presents a logical sector size that is smaller than the physical sector size. Aligning to a physical sector (or optimal I/O) size boundary is recommended, or performance may be impacted.

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to switch off the mode (command 'c') and change display units to sectors (command 'u').

```
Command (m for help): n
Command action
    e extended
    p primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-2610, default 1):
Using default value 1
```

```
Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610): +1G
```

```
Command (m for help): p
```

```
Disk /dev/sdc: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0xe29ed566
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sdc1		1	132	1060256+	83	Linux

Partition 1 does not end on cylinder boundary.
Partition 1 does not start on physical sector boundary.

Command (m for help): n
Command action
e extended
p primary partition (1-4)
p
Partition number (1-4): 2
First cylinder (132-2610, default 132):
Using default value 132
Last cylinder, +cylinders or +size{K,M,G} (132-2610, default 2610):
Using default value 2610
Command (m for help): p

Disk /dev/sdc: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0xe29ed566

Device	Boot	Start	End	Blocks	Id	System
/dev/sdc1		1	132	1060256+	83	Linux
Partition 1 does not end on cylinder boundary.						
Partition 1 does not start on physical sector boundary.						
/dev/sdc2		132	2610	19904537	83	Linux

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.

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

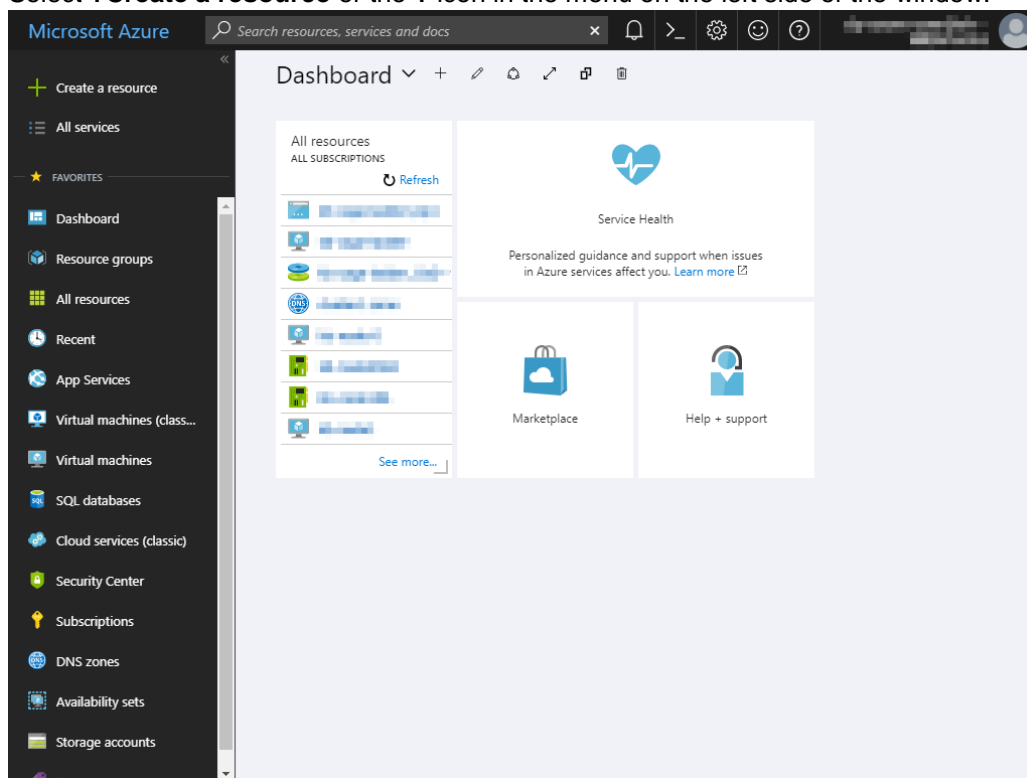
7) Configuring a load balancer

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

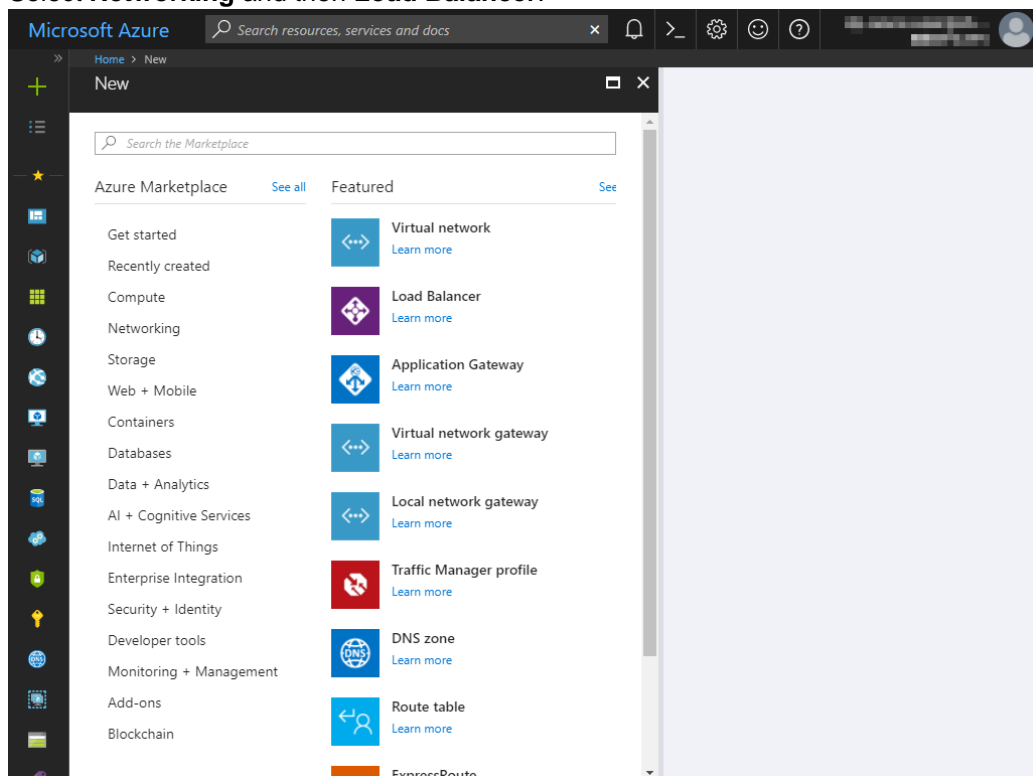
For details, see the following websites:

- Azure Load Balancer overview:
<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>
- Creating an Internet-facing load balancer using the Azure portal:
<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-get-started-internet-portal>

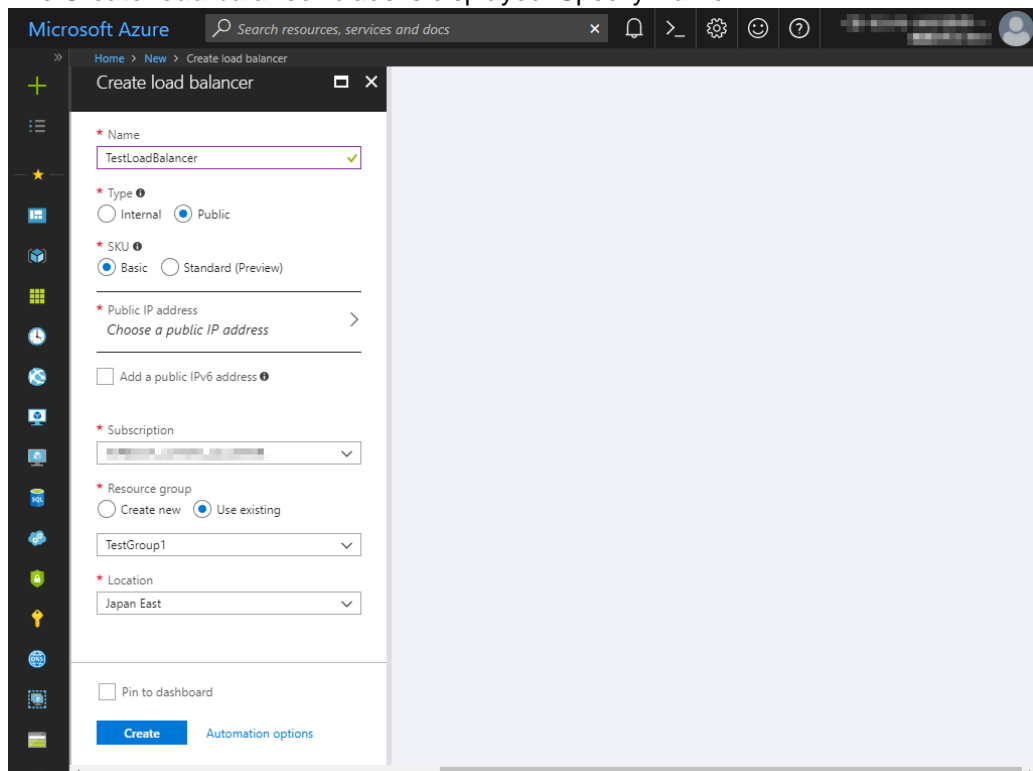
1. Select **+Create a resource** or the **+** icon in the menu on the left side of the window.



2. Select **Networking** and then **Load Balancer**.

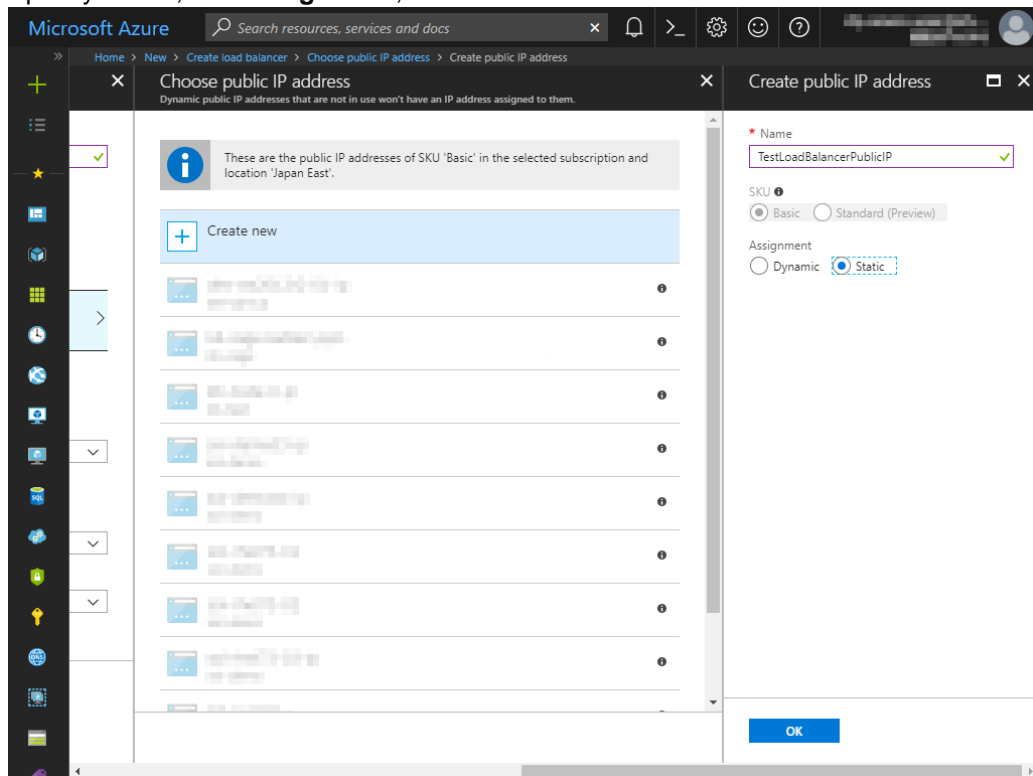


3. The **Create load balancer** blade is displayed. Specify **Name**.

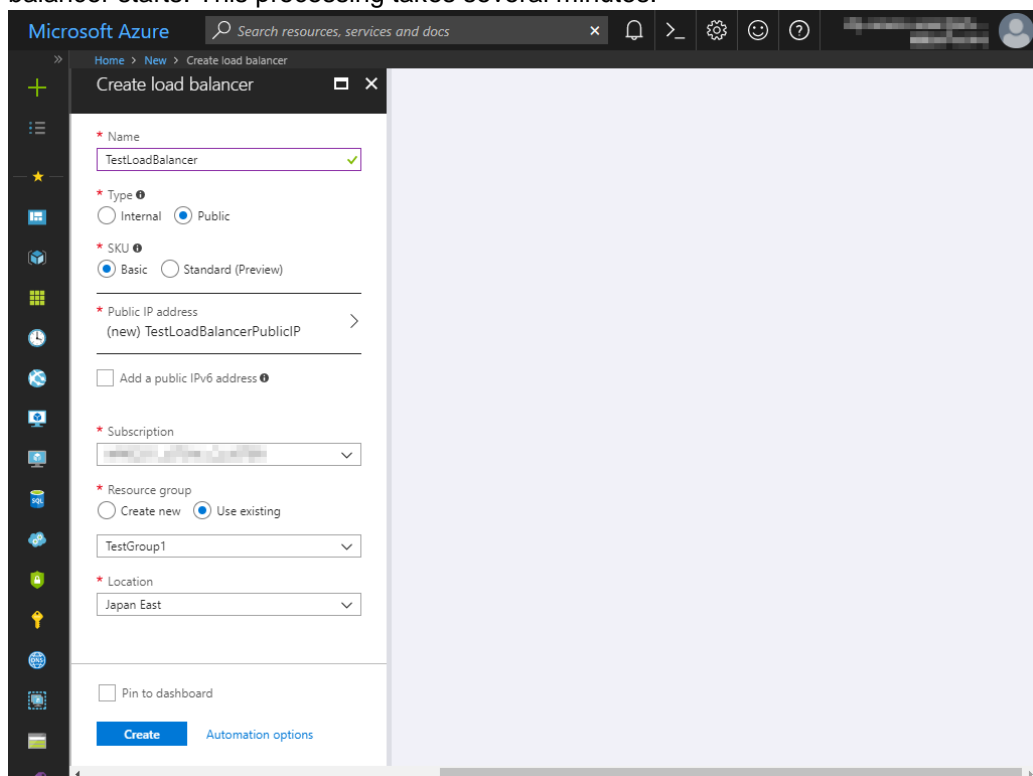


4. Select **Public** for **Type** and select **Create new** for **Public IP address**.

5. Specify **Name**, and **Assignment**, and click **OK**.

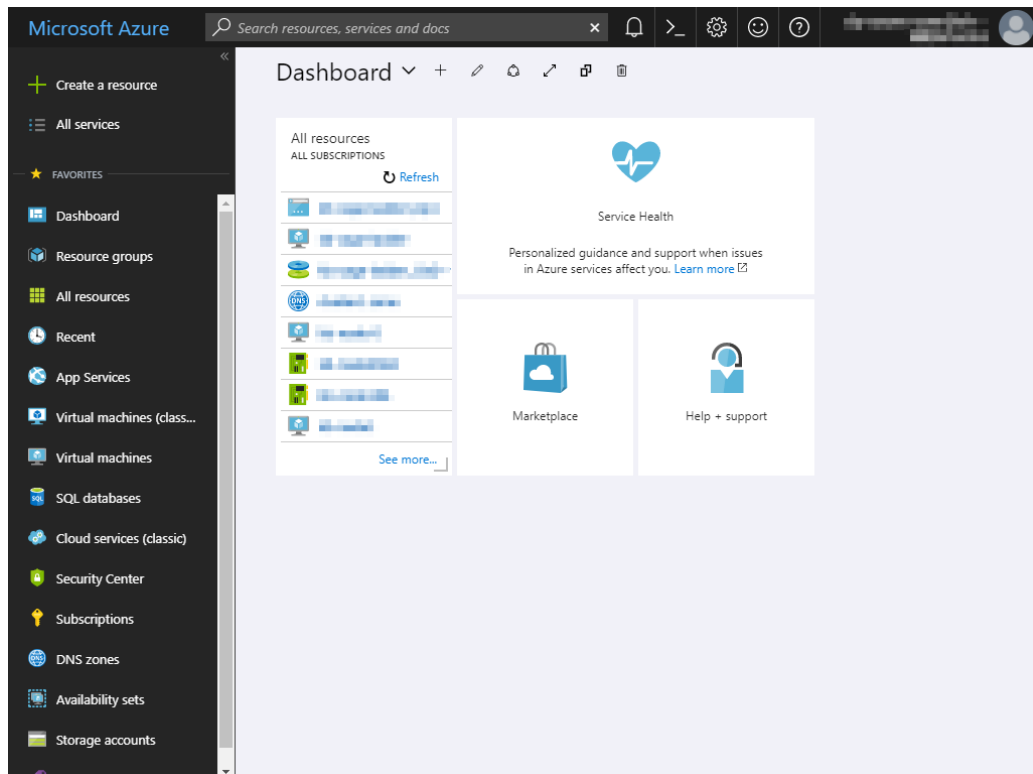


6. Specify **Subscription**, **Resource group**, and **Location**, and click **Create**. Deploying the load balancer starts. This processing takes several minutes.

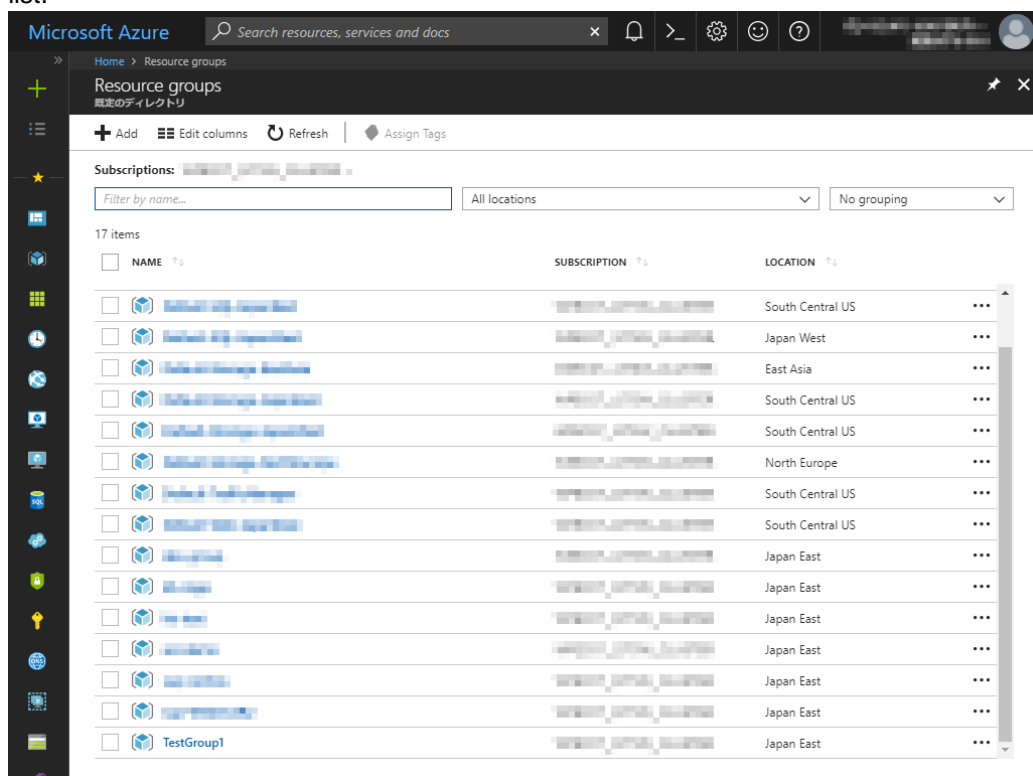


8) Configuring a load balancer (configuring a backend pool)

1. Associate a virtual machine registered to the availability set to the load balancer. After the load balancer has been deployed, select **Resource groups** or the resource group icon in the menu on the left side of the window.



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



Cluster Creation Procedure (for an HA Cluster Using an Internet Facing Load Balancer)

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

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1

TestGroup1 Resource group

Subscription (change) Deployments 5 Succeeded

Subscription ID

Filter by name... All types All locations No

11 items Show all resources

NAME	TYPE	LOCATION
AvailabilitySet1	Availability set	Japan East
clstorageacct1	Storage account	Japan East
clstorageacctdiag1	Storage account	Japan East
NetSecGroup1	Network security group	Japan East
node1	Virtual machine	Japan East
node1435	Network interface	Japan East
node2	Virtual machine	Japan East
node2680	Network interface	Japan East
TestLoadBalancer	Load balancer	Japan East
TestLoadBalancerPublicIP	Public IP address	Japan East
Vnet1	Virtual network	Japan East

4. Select **Backend pools**.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1 > TestLoadBalancer - Backend pools

TestLoadBalancer - Backend pools Load balancer

Search backend address pools

VIRTUAL MACHINE	VIRTUAL MACHI...	NETWORK INTERFACE	PRIVATE IP ADDRESS
No results.			

5. Click **Add**.
6. The **Add backend pool** blade is displayed. Specify **Name**.
7. For **Associated to**, select **Availability set**.
8. Specify **Availability set**.
9. Click **Add a target network IP configuration**.
10. Specify the target virtual machine for **Target virtual machine** and **Network IP configuration**.

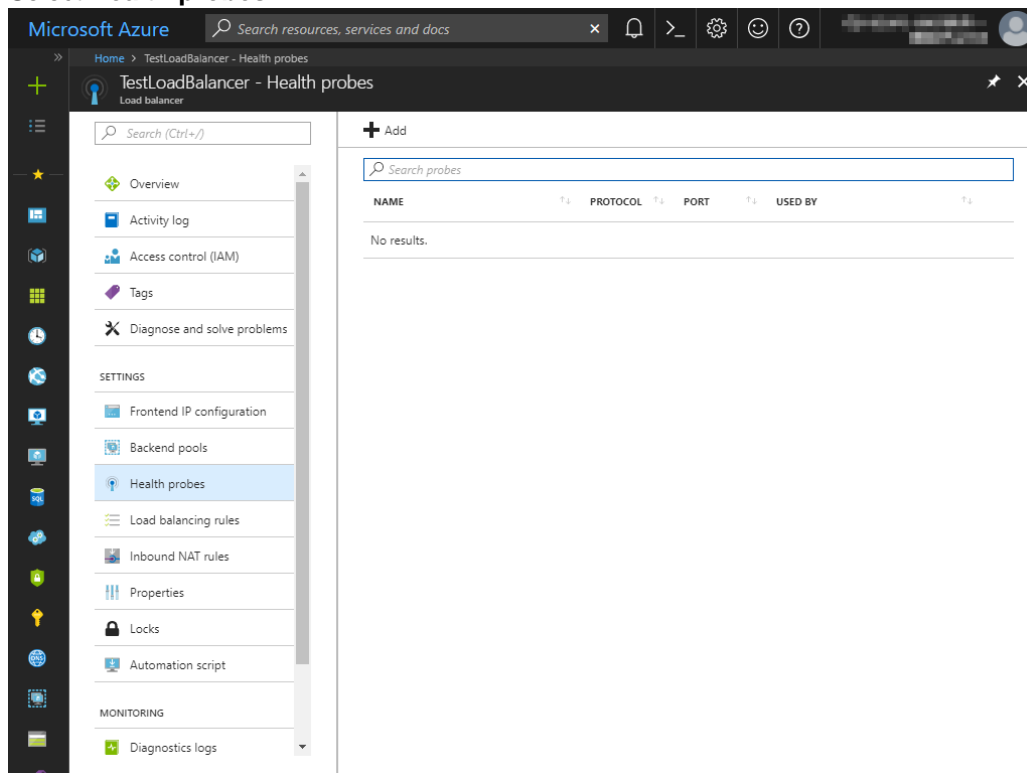
11. Repeat steps 9 and 10 as many times as the number of target virtual machines.
12. Click **OK**.

The screenshot shows the 'Add backend pool' dialog in the Microsoft Azure portal. The breadcrumb navigation at the top reads: Home > Resource groups > TestGroup1 > TestLoadBalancer - Backend pools > Add backend pool. The dialog title is 'Add backend pool' for 'TestLoadBalancer'. The form contains the following fields and options:

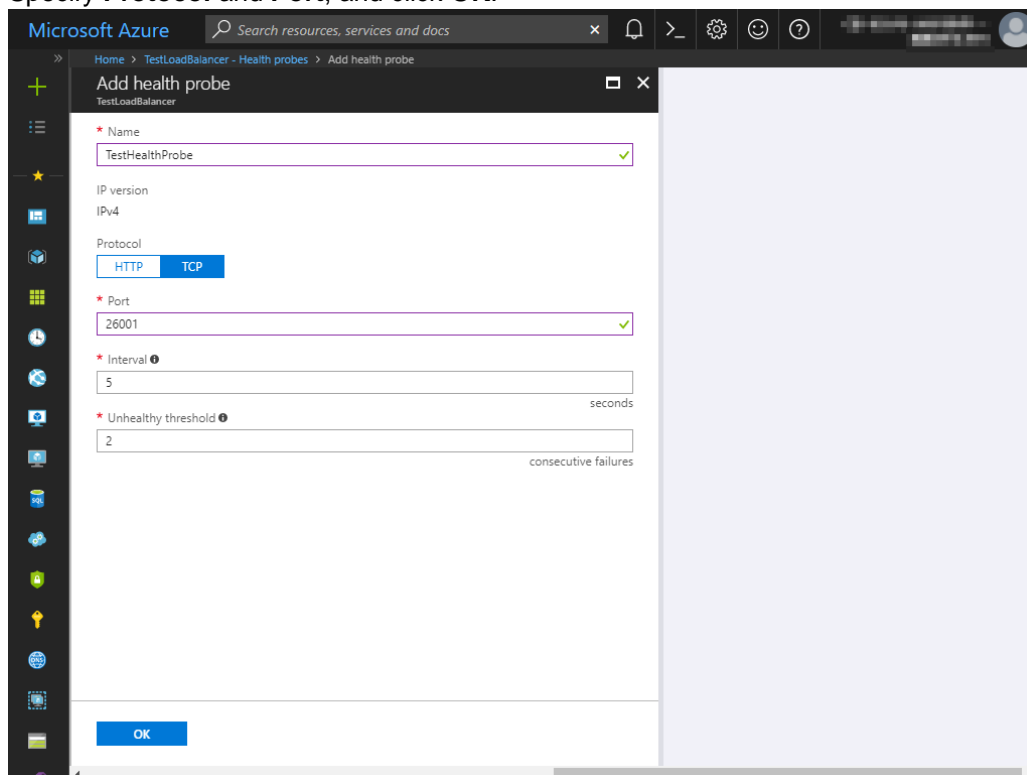
- Name:** TestBackendPool (with a green checkmark icon).
- IP version:** IPv4 (selected) and IPv6 (available).
- Associated to:** Availability set (dropdown menu).
- Availability set:** AvailabilitySet1 (dropdown menu) with a note 'number of virtual machines: 2'.
- Target network IP configurations:** A section with a warning icon and text: 'Only VMs within the current availability set can be chosen. Once a VM is chosen, you can select a network IP configuration related to it.' It lists 'Virtual machine: node1' and 'Network IP configuration: node1435/ipconfig1 (10.5.0.110)' with a trash icon.
- Target virtual machine:** node2 (dropdown menu) with a note 'size: Standard_A1, network interfaces: 1' and a trash icon.
- Network IP configuration:** ipconfig1 (10.5.0.111) (dropdown menu).
- Buttons:** '+ Add a target network IP configuration' (blue link) and 'OK' (blue button).

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

1. Select **Health probes**.

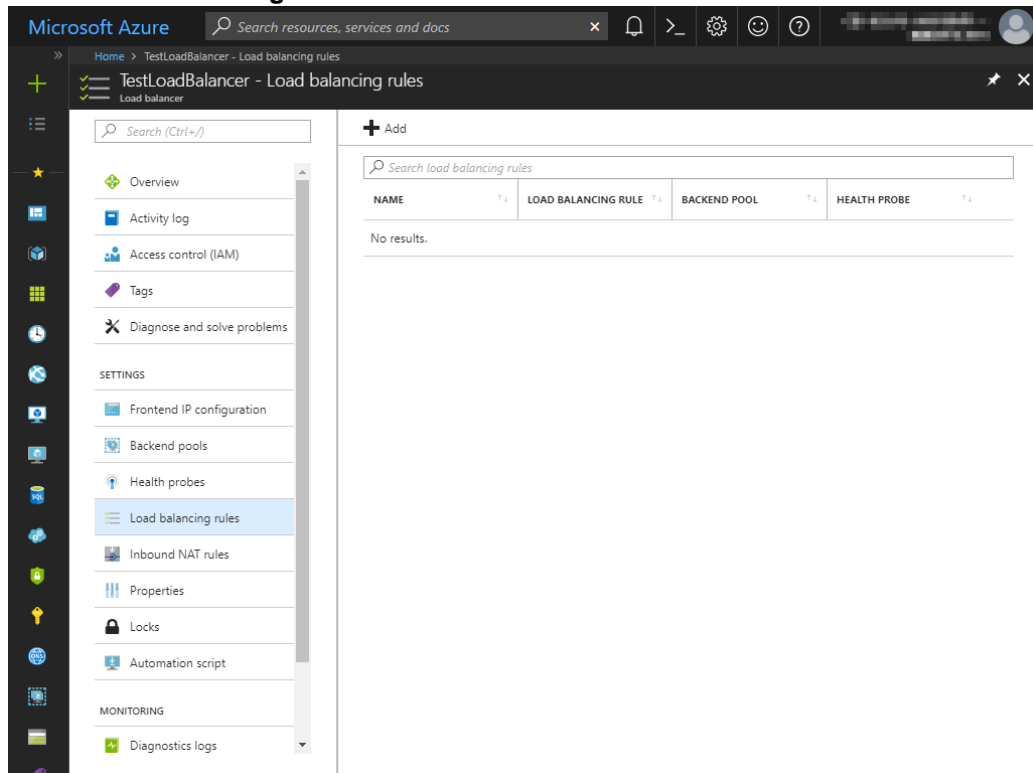


2. Click **Add**.
3. The **Add health probe** blade is displayed. Specify **Name**.
4. Specify **Protocol** and **Port**, and click **OK**.

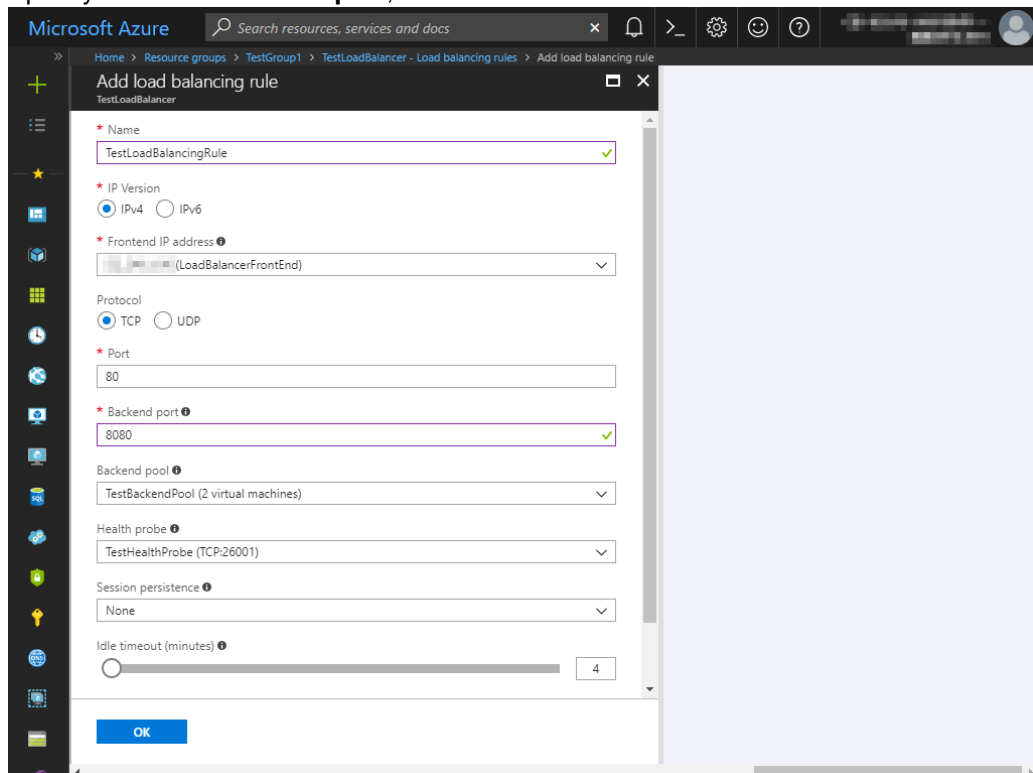


10) Configuring a load balancer (setting the load balancing rules)

1. Select **Load balancing rules**.



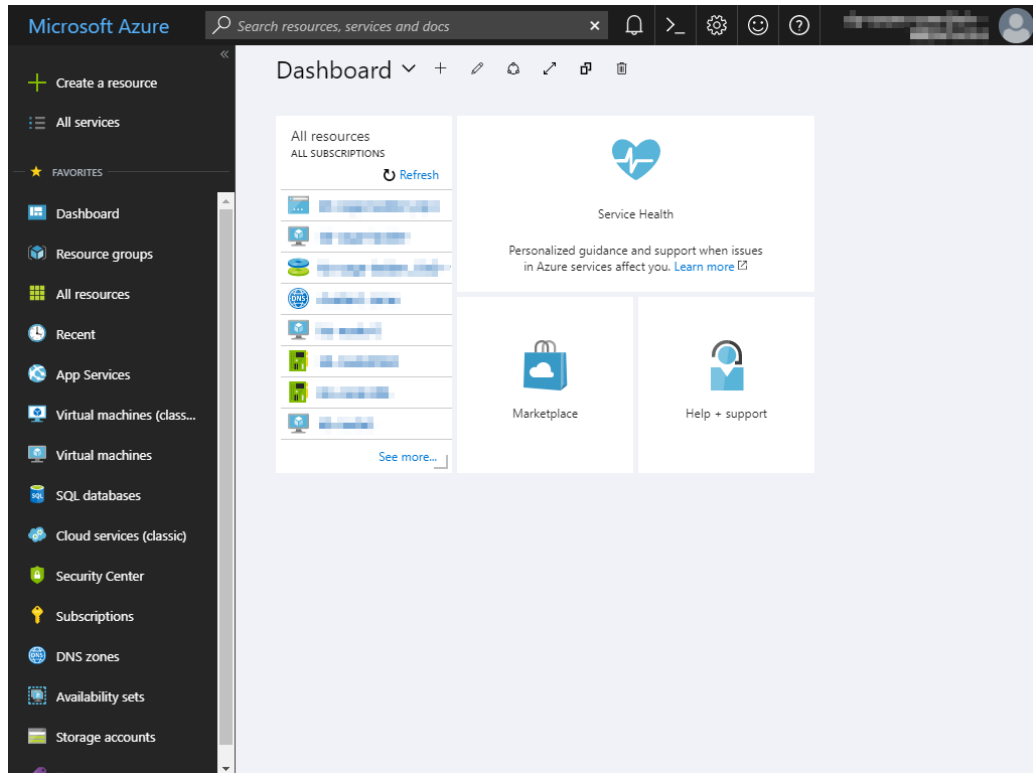
2. Click **Add**.
3. The **Add load balancing rule** blade is displayed. Specify **Name**.
4. Specify **Port** and **Backend port**, and click **OK**.



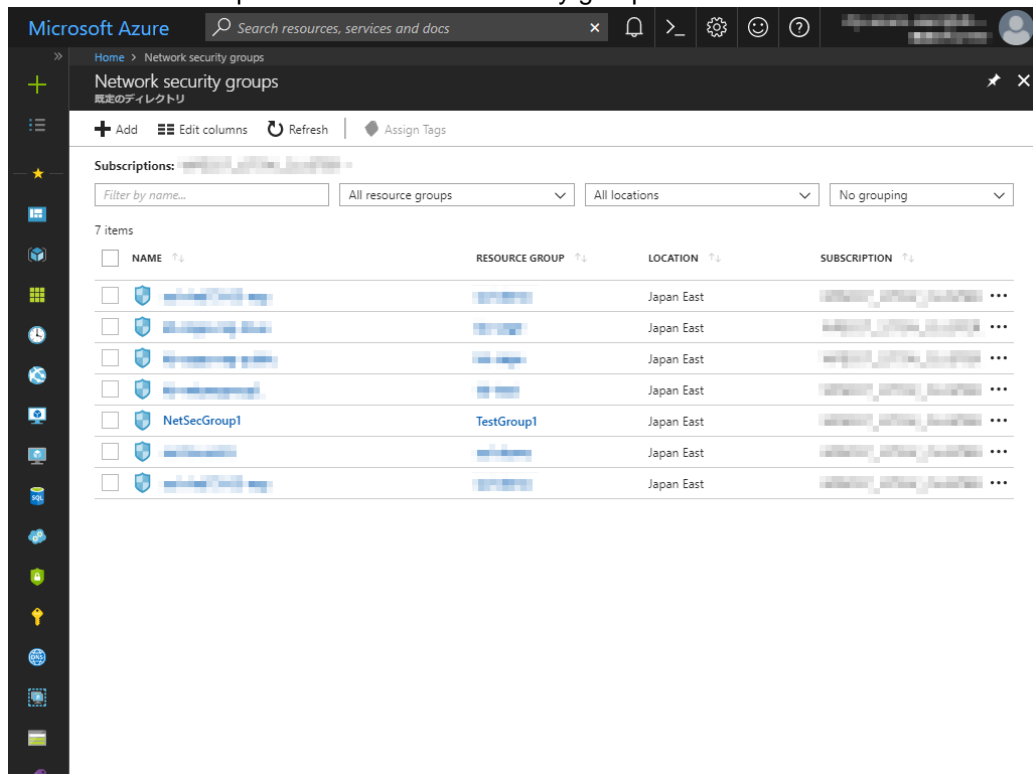
11) Setting the inbound security rules

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

1. Select **Network security groups** or the network security group icon in the menu on the left side of the window.

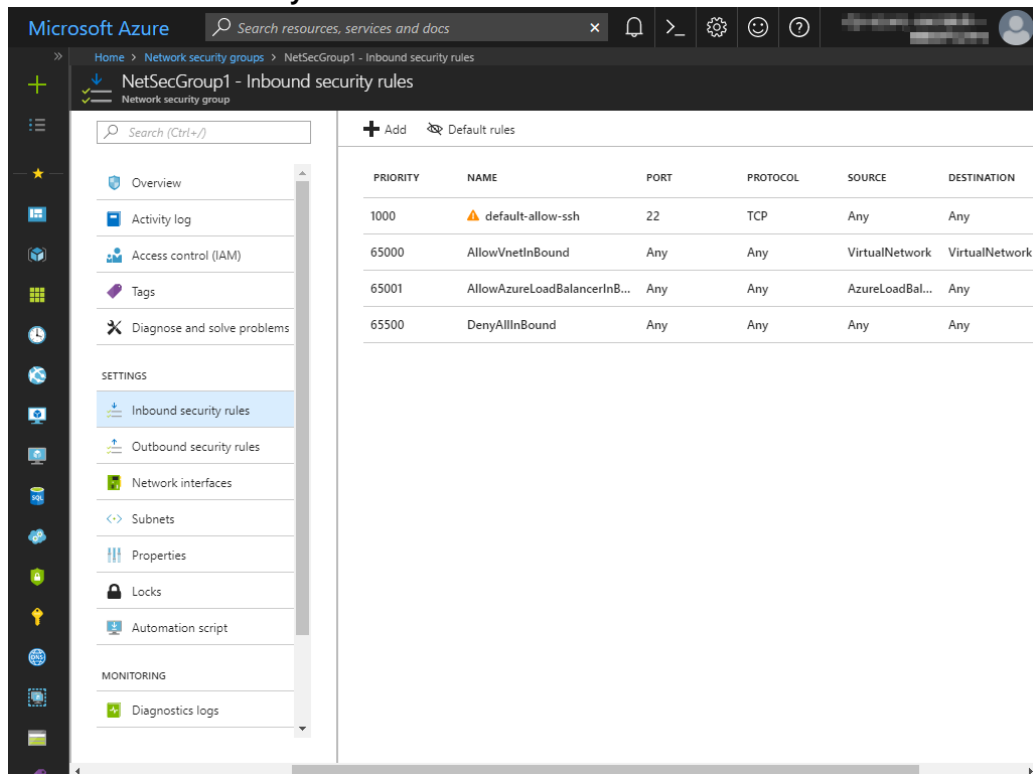


2. Select NetSecGroup1 from the network security group list.



3. The summary of NetSecGroup1 is displayed.

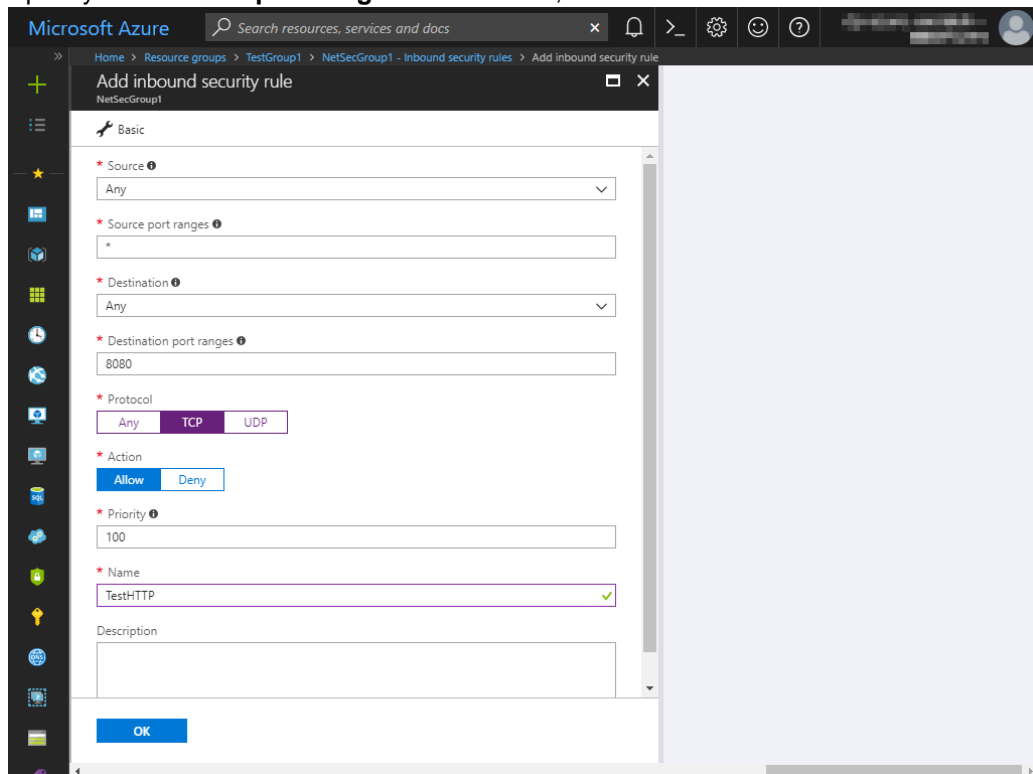
4. Select **Inbound security rules**.



5. Click **Add**.

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

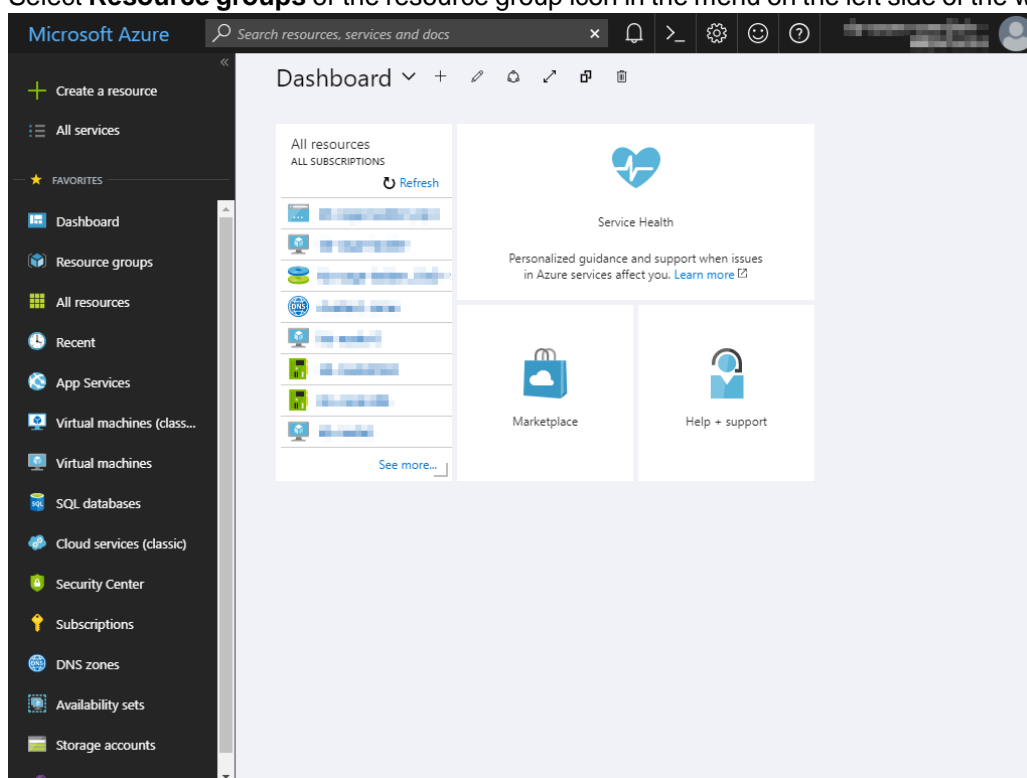
7. Specify **Destination port range** and **Protocol**, and click **OK**.



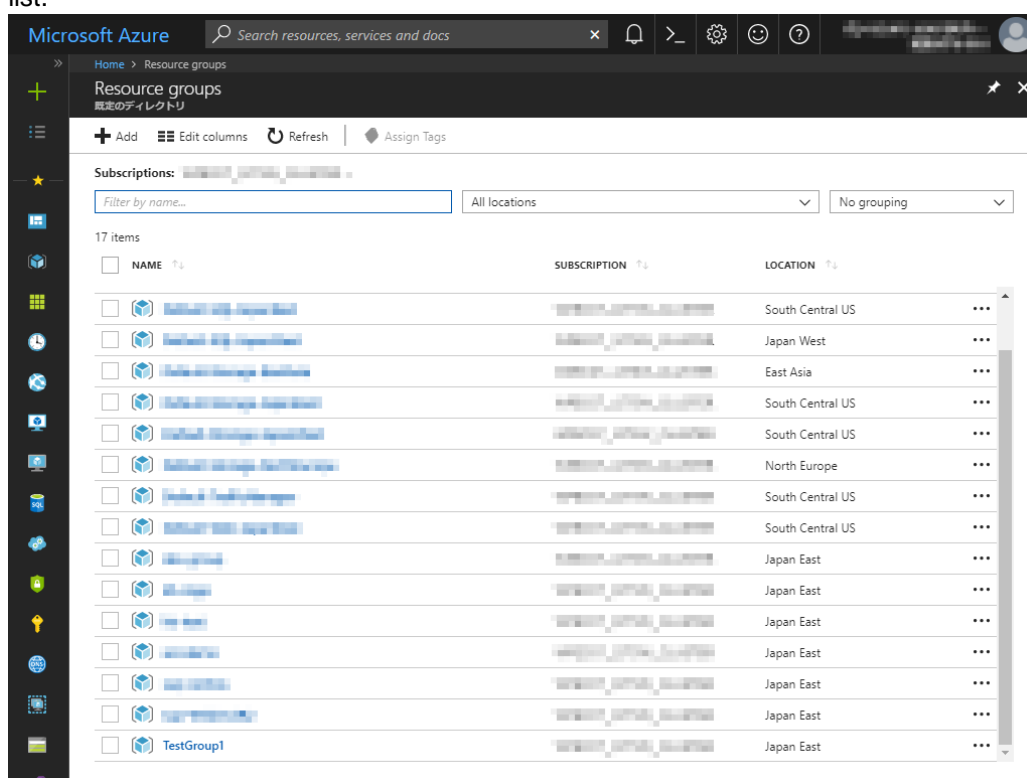
Then, check `<Load_balancer_frontend_IP(public_IP_address)>` specified in the script before recovery action of the multi-target monitor resource that is set in "3) Adding a monitor resource." Write down the confirmatory result.

Cluster Creation Procedure (for an HA Cluster Using an Internet Facing Load Balancer)

1. Select **Resource groups** or the resource group icon in the menu on the left side 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.

Microsoft Azure

Home > Resource groups > TestGroup1

TestGroup1
Resource group

Search (Ctrl+/)

+ Add Edit columns Delete resource group Refresh Move Assign Tags

Subscription (change) Deployments
5 Succeeded

Subscription ID

Filter by name... All types All locations No

11 items Show all resources

NAME	TYPE	LOCATION
AvailabilitySet1	Availability set	Japan East
clstorageacc1	Storage account	Japan East
clstorageaccdiag1	Storage account	Japan East
NetSecGroup1	Network security group	Japan East
node1	Virtual machine	Japan East
node1435	Network interface	Japan East
node2	Virtual machine	Japan East
node2680	Network interface	Japan East
TestLoadBalancer	Load balancer	Japan East
TestLoadBalancerPublicIP	Public IP address	Japan East
Vnet1	Virtual network	Japan East

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

Microsoft Azure

Home > Load balancers > TestLoadBalancer

TestLoadBalancer
Load balancer

Search (Ctrl+/)

Move Delete Refresh

Essentials

Resource group (change)
TestGroup1

Location
Japan East

Subscription name (change)

Subscription ID

SKU
Basic

Backend pool
TestBackendPool (2 virtual machines)

Health probe
TestHealthProbe (TCP:26001)

Load balancing rule
TestLoadBalancingRule (TCP/80 to TCP/8080)

NAT rules

Public IP address
(TestLoadBalancerPublicIP)

12) 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 Chapter 1, “Determining a system configuration” in the *Installation and Configuration Guide*.

13) Installing EXPRESSCLUSTER

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

After installation is complete, restart the OS.

14) Registering the EXPRESSCLUSTER license

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

4.3 Configuring the EXPRESSCLUSTER settings

Configure the following on the WebManager cluster generation wizard.

For the WebManager setup and connection procedures, see Chapter 5, "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)

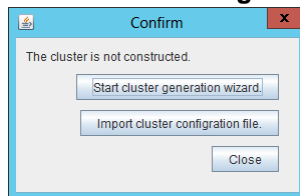
For the settings of other resources and monitor resources, see the *Installation and Configuration Guide* and the *Reference Guide*.

1) Creating a cluster

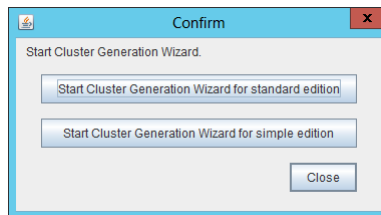
Start the cluster generation wizard to create a cluster.

◆ Creating a cluster

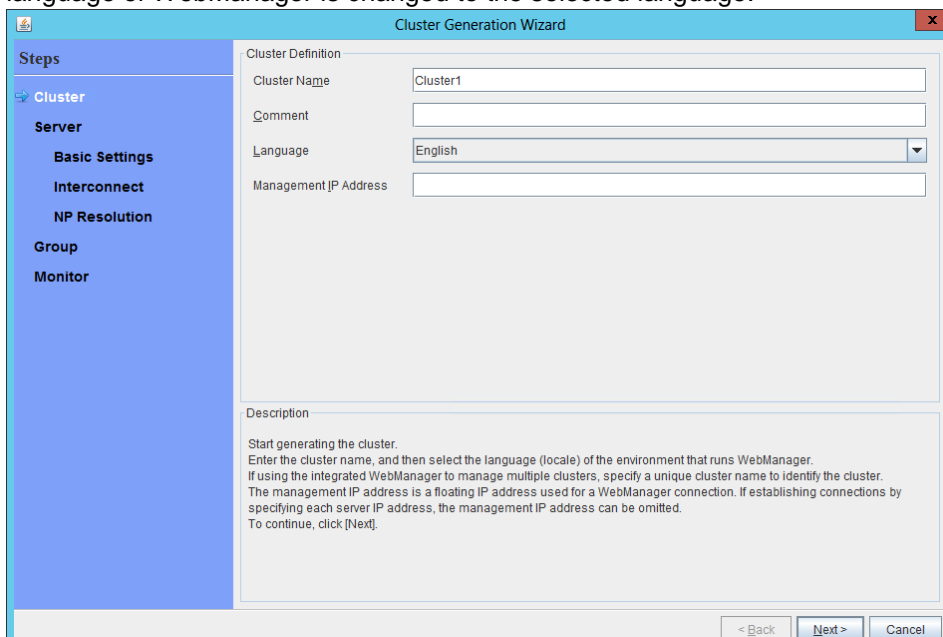
1. Access WebManager. Then, the following dialog box is displayed.
Click **Start cluster generation wizard**.



2. The following dialog box is displayed.
Click **Start Cluster Generation Wizard for standard edition**.

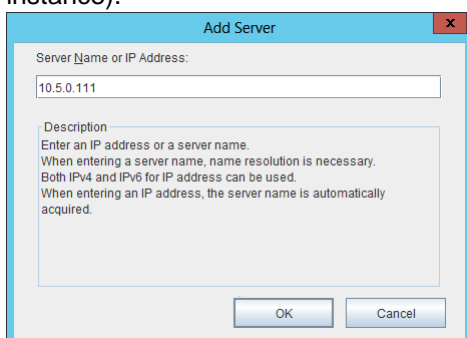


3. The **Cluster Definition** page is displayed.
Enter a desired name in **Cluster Name**.
Select an appropriate language in **Language**. After the setting is applied, the display language of WebManager is changed to the selected language.



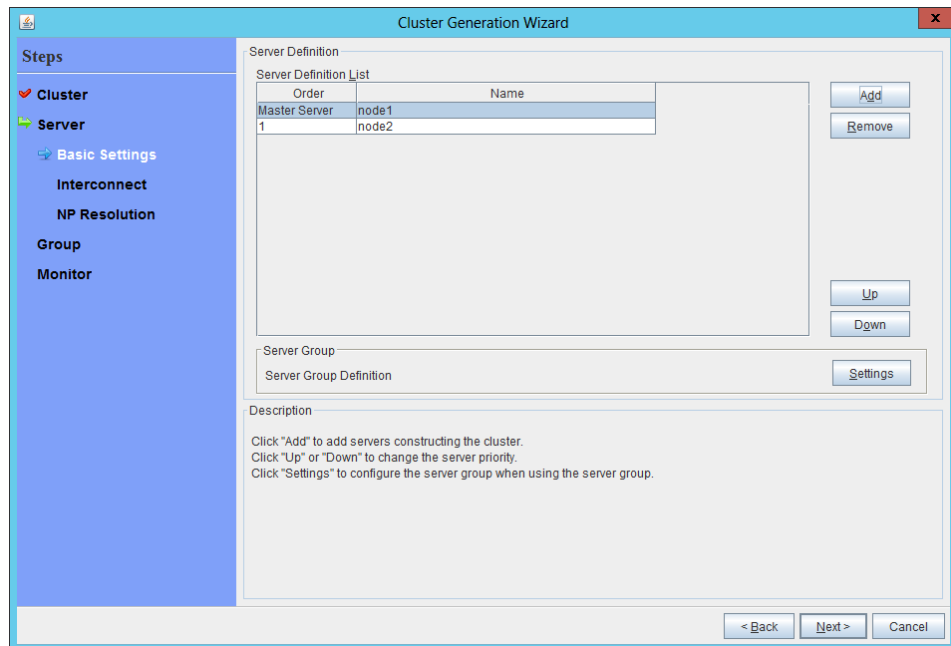
The screenshot shows the 'Cluster Generation Wizard' window. On the left, a 'Steps' sidebar lists 'Cluster', 'Server', 'Basic Settings', 'Interconnect', 'NP Resolution', 'Group', and 'Monitor'. The 'Cluster' step is selected. The main area is titled 'Cluster Definition' and contains four input fields: 'Cluster Name' (with 'Cluster1' entered), 'Comment' (empty), 'Language' (a dropdown menu showing 'English'), and 'Management IP Address' (empty). Below these fields is a 'Description' section with the following text: 'Start generating the cluster. Enter the cluster name, and then select the language (locale) of the environment that runs WebManager. If using the integrated WebManager to manage multiple clusters, specify a unique cluster name to identify the cluster. The management IP address is a floating IP address used for a WebManager connection. If establishing connections by specifying each server IP address, the management IP address can be omitted. To continue, click [Next].'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

4. The **Server Definition** page is displayed.
The instance connected to WebManager is displayed as a registered master server.
Click **Add** to add the remaining instances (by specifying the private IP address of each instance).



The screenshot shows the 'Add Server' dialog box. It has a title bar with 'Add Server' and a close button. Inside, there is a label 'Server Name or IP Address:' followed by a text input field containing '10.5.0.111'. Below this is a 'Description' section with the text: 'Enter an IP address or a server name. When entering a server name, name resolution is necessary. Both IPv4 and IPv6 for IP address can be used. When entering an IP address, the server name is automatically acquired.' At the bottom, there are two buttons: 'OK' and 'Cancel'.

5. Click **Next**.



The screenshot shows the 'Cluster Generation Wizard' window, specifically the 'Server Definition' step. The left sidebar shows the 'Steps' list with 'Cluster' selected. The main area contains a 'Server Definition List' table with columns 'Order' and 'Name'. The table has one row with 'Order' 1 and 'Name' 'node1'. Below the table are 'Add', 'Remove', 'Up', and 'Down' buttons. There is also a 'Server Group' section with a 'Server Group Definition' button. A 'Description' box at the bottom provides instructions on how to use the buttons.

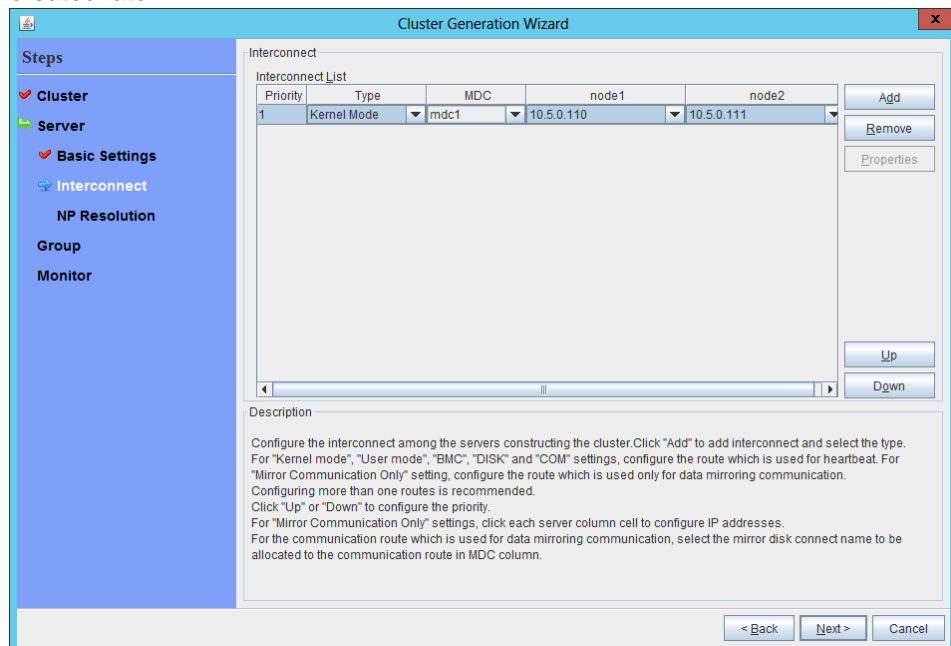
Order	Name
1	node1

Buttons: Add, Remove, Up, Down, Settings

Description:
Click "Add" to add servers constructing the cluster.
Click "Up" or "Down" to change the server priority.
Click "Settings" to configure the server group when using the server group.

6. The **Interconnect** page 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.



The screenshot shows the 'Cluster Generation Wizard' window, specifically the 'Interconnect' step. The left sidebar shows the 'Steps' list with 'Cluster' selected. The main area contains an 'Interconnect List' table with columns 'Priority', 'Type', 'MDC', 'node1', and 'node2'. The table has one row with 'Priority' 1, 'Type' 'Kernel Mode', 'MDC' 'mdc1', 'node1' '10.5.0.110', and 'node2' '10.5.0.111'. Below the table are 'Add', 'Remove', 'Properties', 'Up', and 'Down' buttons. A 'Description' box at the bottom provides instructions on how to use the buttons.

Priority	Type	MDC	node1	node2
1	Kernel Mode	mdc1	10.5.0.110	10.5.0.111

Buttons: Add, Remove, Properties, Up, Down

Description:
Configure the interconnect among the servers constructing the cluster. Click "Add" to add interconnect and select the type. For "Kernel mode", "User mode", "BMC", "DISK" and "COM" settings, configure the route which is used for heartbeat. For "Mirror Communication Only" setting, configure the route which is used only for data mirroring communication. Configuring more than one routes is recommended. Click "Up" or "Down" to configure the priority. For "Mirror Communication Only" settings, click each server column cell to configure IP addresses. For the communication route which is used for data mirroring communication, select the mirror disk connect name to be allocated to the communication route in MDC column.

7. Click **Next**.

8. The **NP Resolution** page is displayed.
 Note that NP resolution is not configured on this page. 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."
 Click **Next**.

Cluster Generation Wizard

Steps

- Cluster
- Server
- Basic Settings
- Interconnect
- NP Resolution**
- Group
- Monitor

NP Resolution

NP Resolution List

Type	Ping Target	node1	node2

Add
Remove
Properties

Tuning

Description

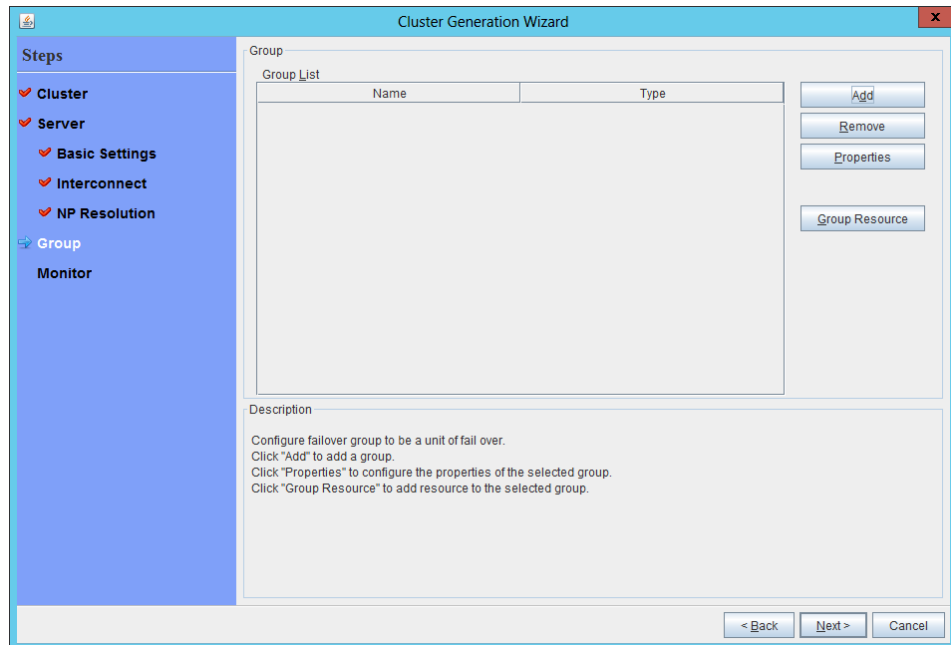
Configure network partition (NP) resolution function.
 In case Ping method NP resolution, click "Add" to add Ping NP resolution resource and click Ping target column cell to configure IP address of Ping destination.
 Click each server column cell to configure "Use" or "Do not use".
 The detailed settings can be verified and changed by clicking "Properties".
 Click "Tuning" to configure the actions at NP occurrence.

< Back Next > Cancel

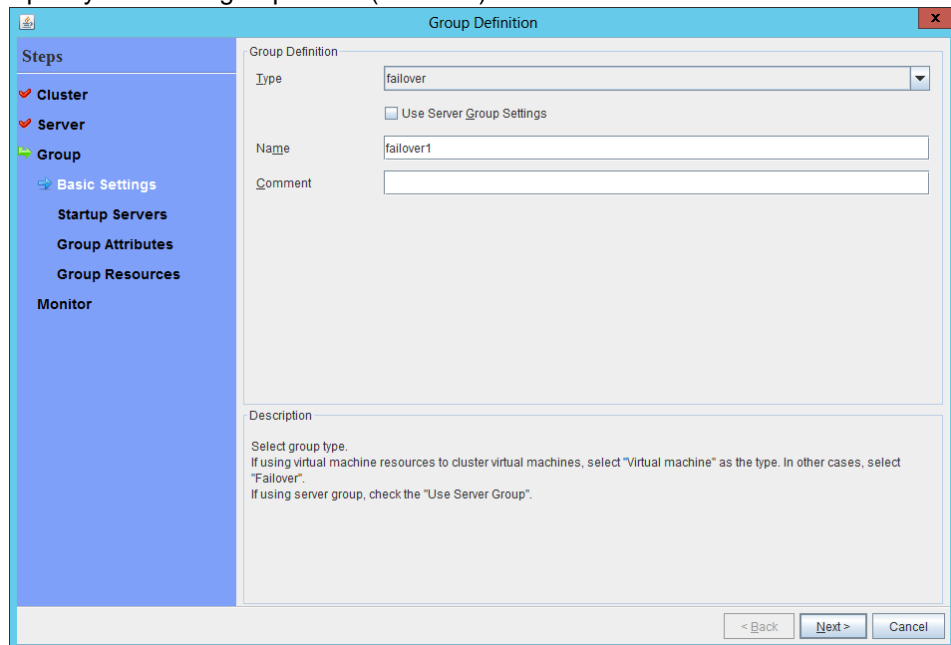
2) Adding a group resource

- ◆ Defining a group
Create a failover group.

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



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



3. Click **Next**.

4. The **Servers that can run the Group** page is displayed.
Click **Next** without specifying anything.

The screenshot shows the 'Group Definition(failover1)' window. On the left is a 'Steps' sidebar with options: Cluster, Server, Group (selected), Basic Settings, Startup Servers, Group Attributes, Group Resources, and Monitor. The main area is titled 'Servers that can run the Group'. It contains a checkbox 'Failover is possible on all servers' which is checked. Below this are two lists: 'Servers that can run the Group' (empty) and 'Available Servers' (containing 'node1' and 'node2'). Between the lists are buttons: '< Add', 'Remove >', 'Up', and 'Down'. At the bottom right are buttons: '< Back', 'Next >', and 'Cancel'. A 'Description' section at the bottom provides instructions on selecting servers and configuring failover.

5. The **Group Attribute Settings** page is displayed.
Click **Next** without specifying anything.

The screenshot shows the 'Group Definition(failover1)' window, now on the 'Group Attribute Settings' page. The 'Steps' sidebar remains the same. The main area contains settings for 'Startup Attribute' (radio buttons for 'Auto Startup' and 'Manual Startup'), 'Failover Attribute' (radio buttons for 'Auto Failover' and 'Manual Failover'), and 'Failback Attribute' (radio buttons for 'Auto Failback' and 'Manual Failback'). Under 'Auto Failover', there are checkboxes for 'Use the startup server settings', 'Failover dynamically', 'Perform a Forced Failover', 'Prioritize failover policy in the server group', and 'Perform a Smart Failover'. There is also a checkbox for 'Prioritize failover policy in the server group' and a checkbox for 'Enable only manual failover among the server groups'. An 'Edit exclusion monitor' button is present. At the bottom right are buttons: '< Back', 'Next >', and 'Cancel'. A 'Description' section at the bottom provides instructions on configuring starting failover group or actions of fail over.

6. The **Group Resource** page is displayed.
On this page, add a group resource following the procedure below.

The screenshot shows a window titled "Group Definition(failover1)" with a close button in the top right corner. On the left is a blue sidebar with a "Steps" section containing a tree view with the following items: "Cluster" (with a red heart icon), "Server" (with a red heart icon), "Group" (with a green arrow icon and highlighted), "Basic Settings" (with a red heart icon), "Startup Servers" (with a red heart icon), "Group Attributes" (with a red heart icon), "Group Resources" (with a blue gear icon), and "Monitor". The main area of the window is titled "Group Resource" and contains a "Group Resource List" table with two columns: "Name" and "Type". The table is currently empty. To the right of the table are three buttons: "Add", "Remove", and "Properties". Below the table is a "Description" section with the text: "Click 'Add' to add resources." and "Click 'Properties' to configure the properties of the selected resource." At the bottom right of the window are three buttons: "< Back", "Finish", and "Cancel".

Name	Type
------	------

Buttons: Add, Remove, Properties

Description:

Click "Add" to add resources.
Click "Properties" to configure the properties of the selected resource.

Navigation: < Back, Finish, Cancel

◆ Mirror disk resource

Create a mirror disk resource.

For details, see “Understanding mirror disk resources” in Chapter 4, “Group resource details” in the *Reference Guide*.

1. Click **Add** on the **Group Resource List** page.
2. The **Resource Definition of Group** 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.

3. Click **Next**.
4. The **Dependent Resources** page is displayed.
Click **Next** without specifying anything.

5. The **Recovery Operation at Activation Failure Detection** and **Recovery Operation at Deactivation Failure Detection** page is displayed.
Click **Next**.

The screenshot shows the 'Resource Definition of Group(failover1)' window with the 'Recovery Operation' tab selected. The left sidebar lists steps: Cluster, Server, Group, Basic Settings, Startup Servers, Group Attributes, Group Resources, Info, Dependency, Recovery Operation (selected), Details, and Monitor. The main area is divided into two sections: 'Recovery Operation at Activation Failure Detection' and 'Recovery Operation at Deactivation Failure Detection'. The first section has a 'Retry Count' of 0, a 'Failover Threshold' of 1, and a 'Final Action' of 'No operation (not activate next resource)'. The second section has a 'Retry Count at Deactivation Failure' of 0 and a 'Final Action' of 'Stop the cluster service and shutdown OS'. Both sections have an 'Execute Script before Final Action' checkbox and a 'Settings' button. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

6. The **Details** page 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.

The screenshot shows the 'Resource Definition of Group(failover1)' window with the 'Details' tab selected. The left sidebar is the same as in the previous screenshot, with 'Details' now selected. The main area has tabs for 'Common', 'node1', and 'node2'. The 'Common' tab is active, showing fields for 'Mirror Partition Device Name' (set to /dev/nmp1), 'Mount Point' (set to /dev/md), 'Data Partition Device Name' (set to /dev/sdc2), 'Cluster Partition Device Name' (set to /dev/sdc1), and 'File System' (set to ext4). There is a 'Mirror Disk Connect' button with a 'Select' button next to it. At the bottom right is a 'Tuning' button. At the bottom are '< Back', 'Finish', and 'Cancel' buttons.

- ◆ 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 Chapter 4, "Group resource details" in the *Reference Guide*.

1. Click **Add** on the **Group Resource List** page.
2. The **Resource Definition of Group** 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.

3. Click **Next**.
4. The **Dependent Resources** page is displayed. Click **Next** without specifying anything.

5. The **Recovery Operation at Activation Failure Detection** and **Recovery Operation at Deactivation Failure Detection** page is displayed. Click **Next**.

Resource Definition of Group(failover1)

Steps

- Cluster
- Server
- Group
- Basic Settings
- Startup Servers
- Group Attributes
- Group Resources
- Info
- Dependency
- Recovery Operation
- Details
- Monitor

Execute Script before or after Activation or Deactivation [Settings]

Recovery Operation at Activation Failure Detection

Retry Count: 5 time

Failover Threshold: 1 time

Final Action: No operation (not activate next resource)

☐ Execute Script before Final Action [Settings]

Recovery Operation at Deactivation Failure Detection

Retry Count at Deactivation Failure: 0 time

Final Action: Stop the cluster service and shutdown OS

☐ Execute Script before Final Action [Settings]

< Back Next > Cancel

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

Resource Definition of Group(failover1)

Steps

- Cluster
- Server
- Group
- Basic Settings
- Startup Servers
- Group Attributes
- Group Resources
- Info
- Dependency
- Recovery Operation
- Details
- Monitor

Probeport: 26001

Tuning

< Back Finish Cancel

7. 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 Chapter 5, “Monitor resource details” 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 Chapter 5, “Monitor resource details” in the *Reference Guide*.

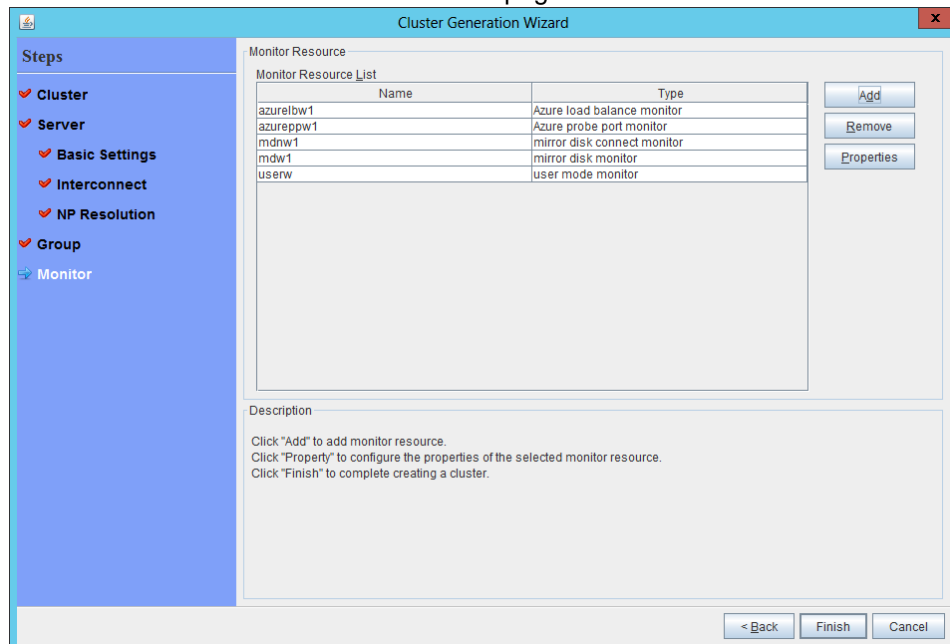
Adding one Azure probe port resource creates one Azure load balance monitor resource automatically.

◆ Custom monitor resource

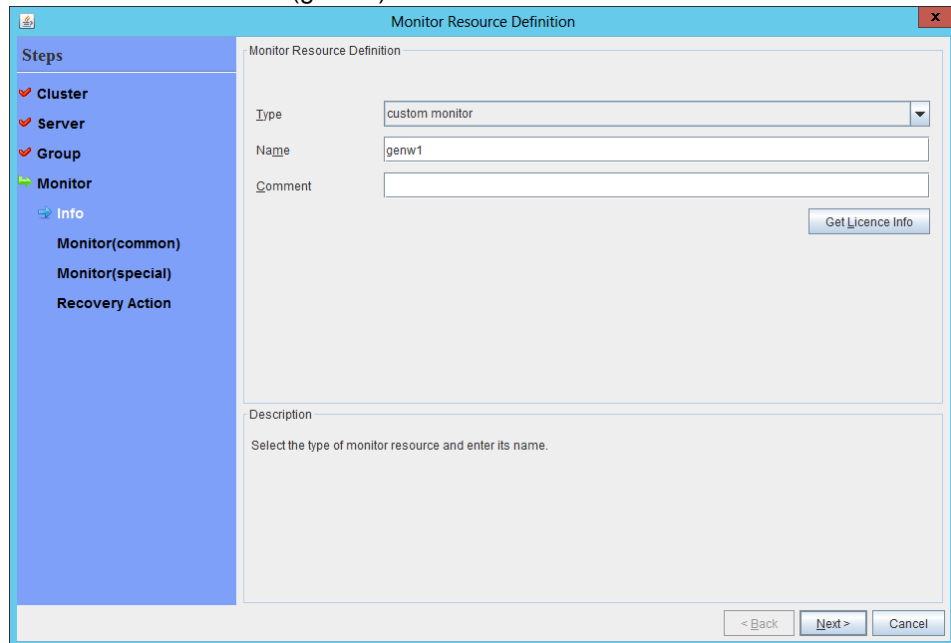
Sets a script to monitor whether communication with Microsoft Azure Service Management API is possible, and also monitors health of communication with an external network.

For details about the custom monitor resource, see “Understanding custom monitor resources” in Chapter 5, “Monitor resource details” in the *Reference Guide*.

1. Click **Add** on the **Monitor Resource List** page.

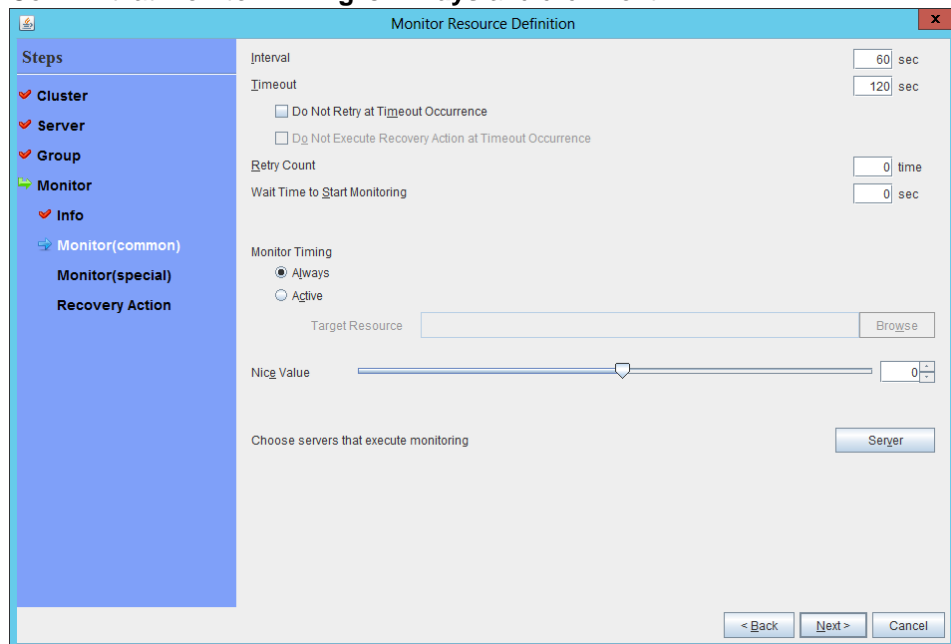


2. Select the monitor resource type (custom monitor) from the **Type** box and enter the monitor resource name (genw1) in the **Name** box.



The dialog box is titled "Monitor Resource Definition". On the left, a "Steps" sidebar shows a tree view with "Cluster", "Server", "Group", "Monitor", "Info", "Monitor(common)", "Monitor(special)", and "Recovery Action". The "Monitor" step is highlighted. The main area is divided into two sections. The top section, "Monitor Resource Definition", contains a "Type" dropdown menu set to "custom monitor", a "Name" text box containing "genw1", and an empty "Comment" text box. A "Get Licence Info" button is to the right. The bottom section, "Description", contains the text "Select the type of monitor resource and enter its name." At the bottom right are "< Back", "Next >", and "Cancel" buttons.

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



The dialog box is titled "Monitor Resource Definition". The "Steps" sidebar on the left now highlights "Monitor(common)". The main area contains configuration options for the monitor. "Interval" is set to 60 sec and "Timeout" to 120 sec. There are checkboxes for "Do Not Retry at Timeout Occurrence" and "Do Not Execute Recovery Action at Timeout Occurrence". "Retry Count" is set to 0 time and "Wait Time to Start Monitoring" is set to 0 sec. Under "Monitor Timing", the "Always" radio button is selected, and the "Active" radio button is unselected. There is a "Target Resource" text box with a "Browse" button. A "Nice Value" slider is set to 0. At the bottom is a "Choose servers that execute monitoring" section with a "Server" button. At the bottom right are "< Back", "Next >", and "Cancel" buttons.

5. The **Monitor (special)** page 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 443exit $?
-----
```

Select **Synchronous** for **Monitor Type**.

6. Click **Next**.
7. The **Recovery Action** page is displayed.
Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final Action**.

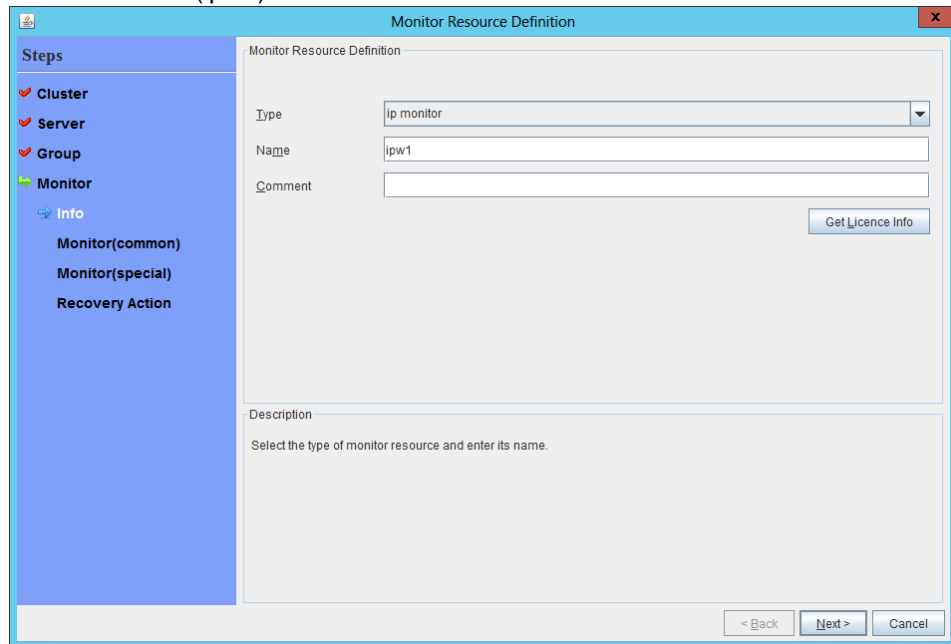
8. Click **Finish** to finish setting.

◆ 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 Chapter 5, “Monitor resource details” 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.



The screenshot shows the 'Monitor Resource Definition' dialog box. On the left, a 'Steps' sidebar lists 'Cluster', 'Server', 'Group', 'Monitor', and 'Info'. The 'Monitor' step is selected and expanded, showing sub-steps: 'Monitor(common)', 'Monitor(special)', and 'Recovery Action'. The main area is titled 'Monitor Resource Definition' and contains three input fields: 'Type' (a dropdown menu with 'ip monitor' selected), 'Name' (a text box containing 'ipw1'), and 'Comment' (an empty text box). A 'Get Licence Info' button is located to the right of the 'Comment' field. Below these fields is a 'Description' section with the text 'Select the type of monitor resource and enter its name.' At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

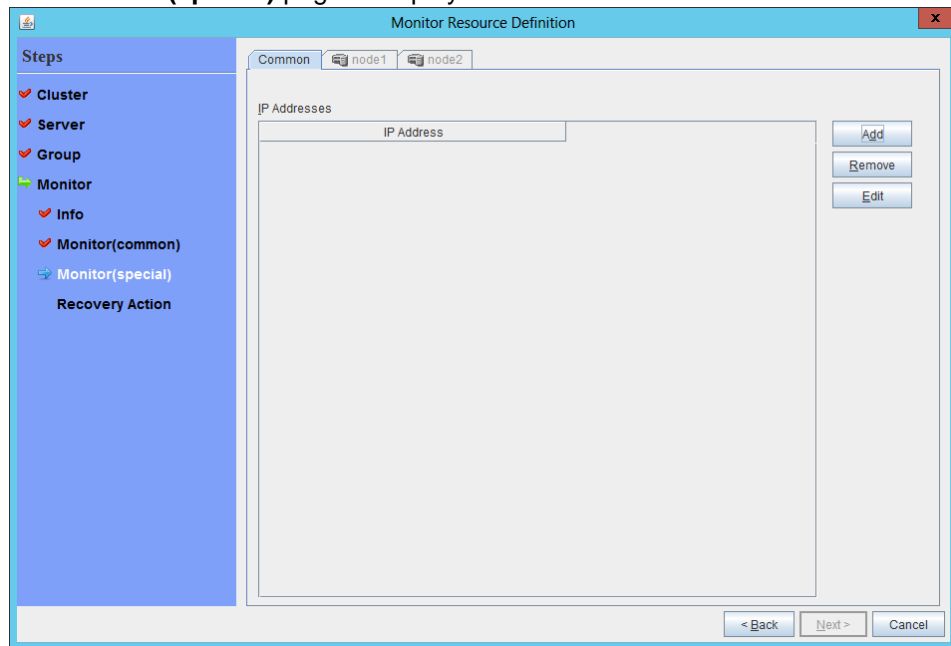
3. Click **Next**.

4. The **Monitor (common)** page is displayed.
Confirm that **Monitor Timing** is **Always**.

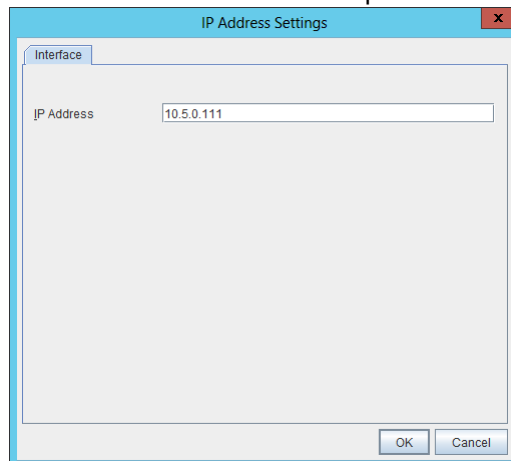
Select one available server for **Choose servers that execute monitoring**.

Click **Next**.

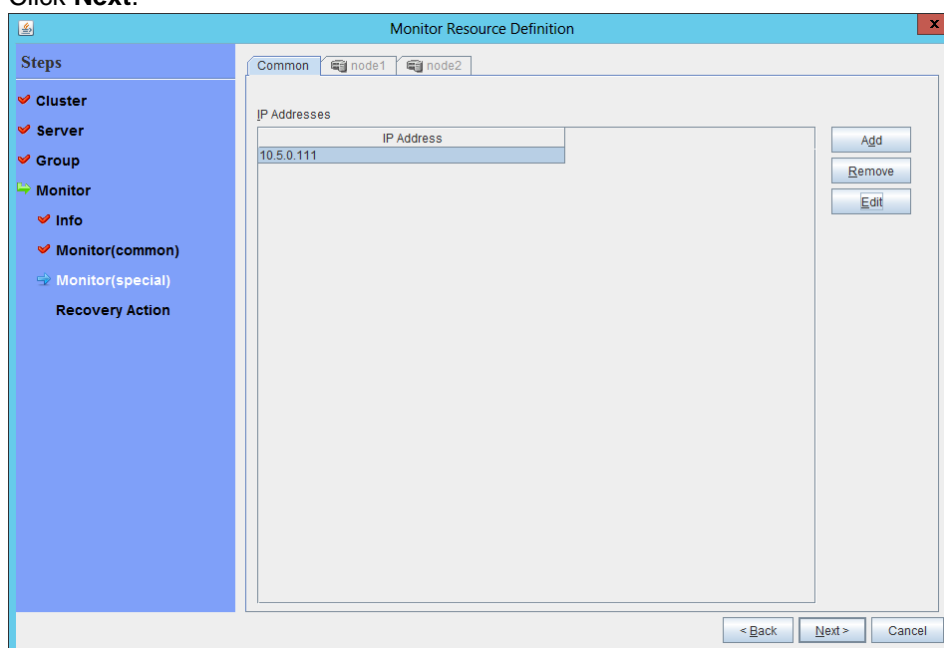
5. The **Monitor (special)** page is displayed.



On the **Common** tab, select **Add** of **IP Address** and set an IP address of a server other than the server selected in step 4.



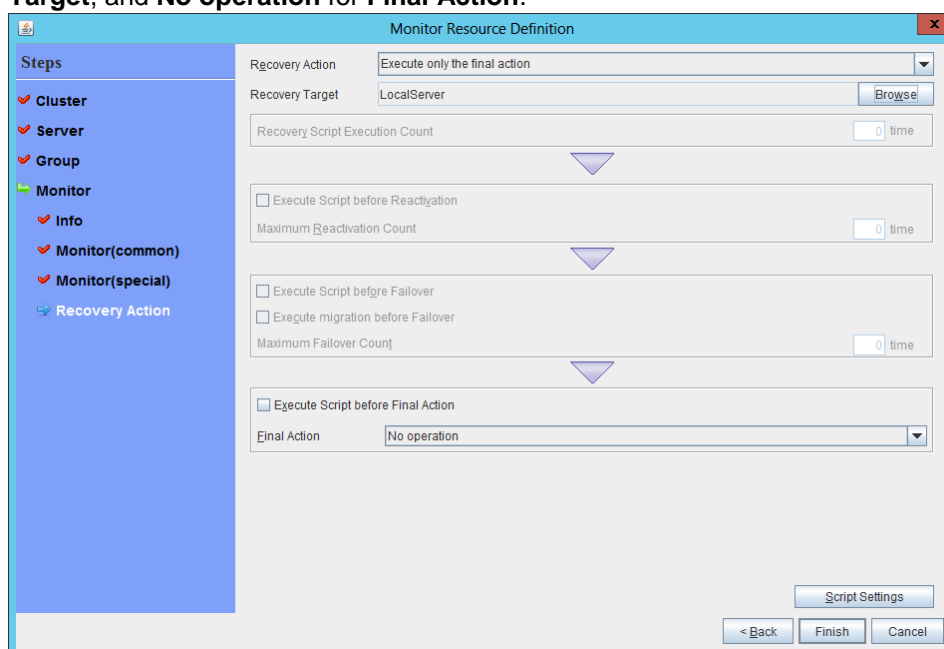
6. Click **Next**.



The screenshot shows the 'Monitor Resource Definition' dialog box with the 'Common' tab selected. The 'IP Addresses' section contains a table with one entry: '10.5.0.111'. To the right of the table are buttons for 'Add', 'Remove', and 'Edit'. At the bottom of the dialog are buttons for '< Back', 'Next >', and 'Cancel'.

IP Address
10.5.0.111

7. The **Recovery Action** page 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' dialog box with the 'Recovery Action' tab selected. The 'Recovery Action' dropdown is set to 'Execute only the final action'. The 'Recovery Target' is 'LocalServer'. The 'Recovery Script Execution Count' is '0' time. There are checkboxes for 'Execute Script before Reactivation', 'Execute Script before Failover', and 'Execute migration before Failover', all of which are unchecked. The 'Maximum Reactivation Count' is '0' time. The 'Maximum Failover Count' is '0' time. The 'Final Action' dropdown is set to 'No operation'. At the bottom right are buttons for 'Script Settings', '< Back', 'Finish', and 'Cancel'.

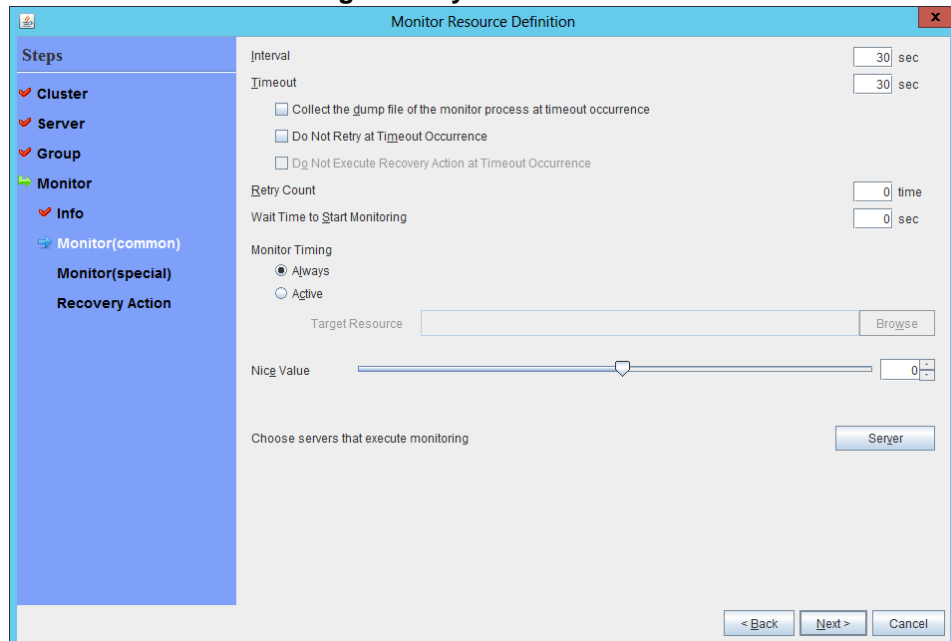
8. Click **Finish** to finish setting.
9. Then, create a monitor resource on the other server. Click **Add** on the **Monitor Resource List** page.

10. Select the monitor resource type (ip monitor) from the **Type** box and enter the monitor resource name (ipw2) in the **Name** box.

The screenshot shows a window titled "Monitor Resource Definition" with a sidebar on the left and a main content area on the right. The sidebar, under the "Steps" section, lists "Cluster", "Server", "Group", "Monitor" (which is highlighted with a green arrow), and "Info". Below "Info", there are three sub-items: "Monitor(common)", "Monitor(special)", and "Recovery Action". The main content area is divided into two sections. The top section, titled "Monitor Resource Definition", contains three input fields: "Type" (a dropdown menu showing "ip monitor"), "Name" (a text box containing "ipw2"), and "Comment" (an empty text box). To the right of the "Comment" field is a button labeled "Get Licence Info". The bottom section, titled "Description", contains a text box with the instruction "Select the type of monitor resource and enter its name." At the bottom right of the window are three buttons: "< Back", "Next >", and "Cancel".

11. Click **Next**.

12. The **Monitor (common)** page is displayed.
Confirm that **Monitor Timing** is **Always**.

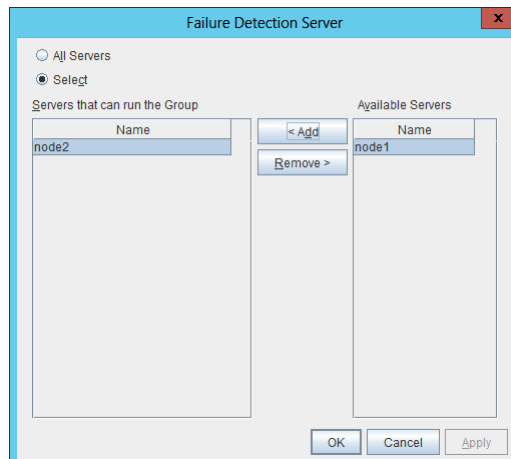


The **Monitor Resource Definition** dialog box is shown. On the left, the **Steps** pane lists: Cluster, Server, Group, Monitor, Info, **Monitor(common)** (selected), Monitor(special), and Recovery Action. The main area contains the following settings:

- 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 with a **Browse** button)
- Nice Value:** A slider set to 0
- Choose servers that execute monitoring:** (empty field with a **Server** button)

At the bottom right are buttons for **< Back**, **Next >**, and **Cancel**.

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



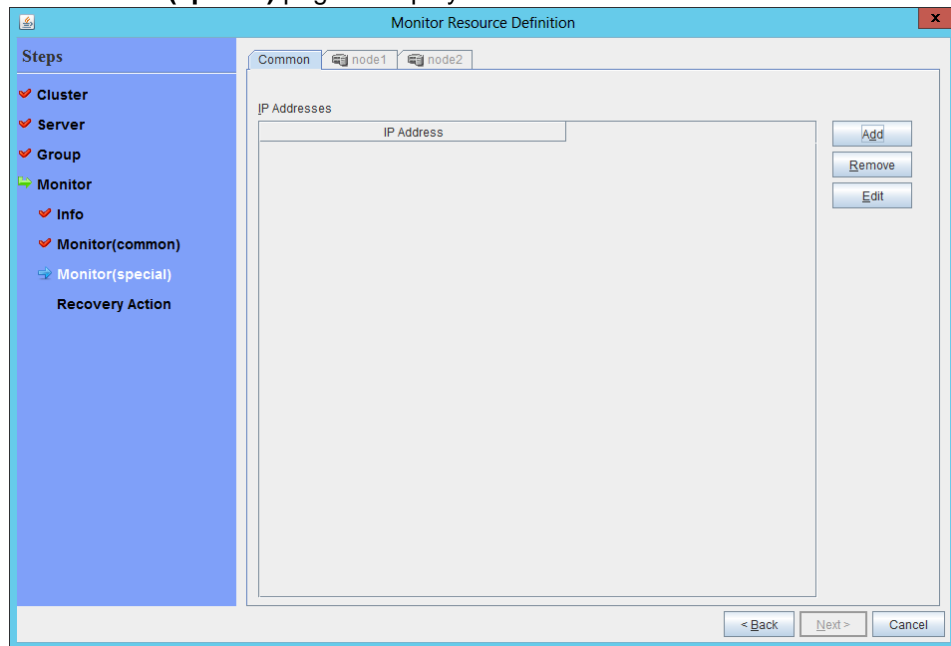
The **Failure Detection Server** dialog box is shown. It has two radio buttons: **All Servers** and **Select** (which is selected). Below the radio buttons are two list boxes:

- Servers that can run the Group:** Contains **node2**.
- Available Servers:** Contains **node1**.

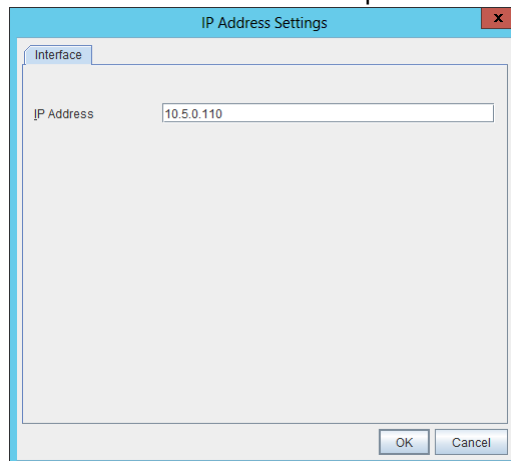
Between the list boxes are buttons for **< Add** and **Remove >**. At the bottom are buttons for **OK**, **Cancel**, and **Apply**.

Click **Next**.

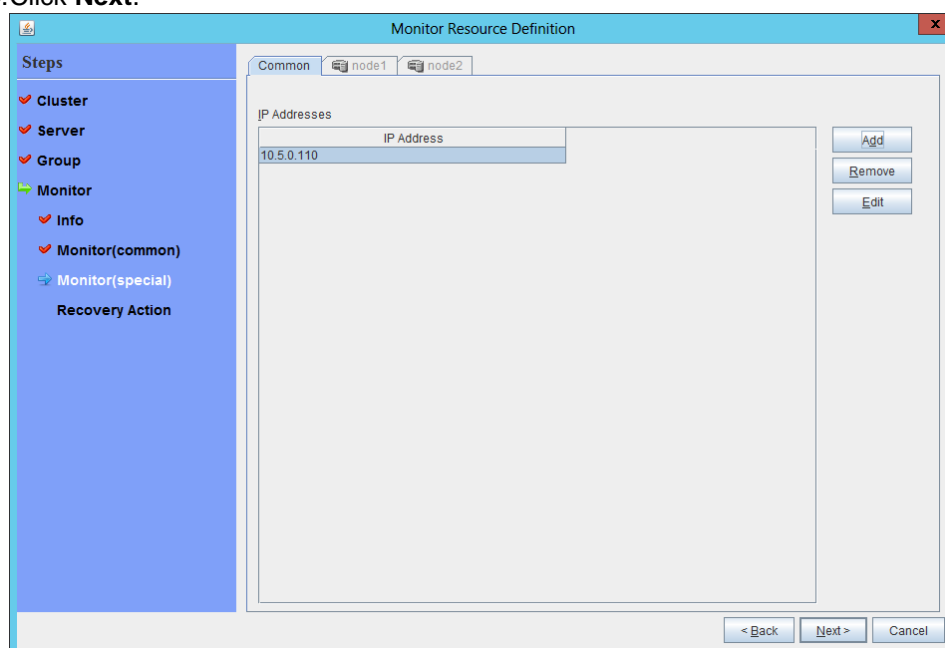
13. The **Monitor (special)** page is displayed.



On the **Common** tab, select **Add** of **IP Address** and set an IP address of a server other than the server selected in step 12.

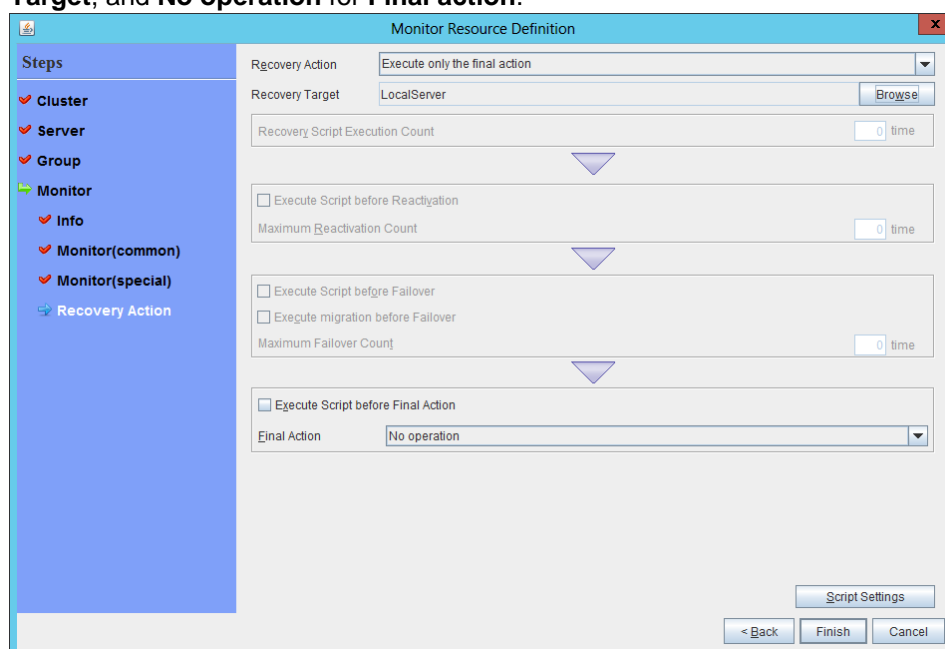


14. Click **Next**.



The 'Monitor Resource Definition' dialog box is shown with the 'Common' tab selected. The left sidebar lists steps: Cluster, Server, Group, Monitor (selected), Info, Monitor(common), Monitor(special), and Recovery Action. The main area has tabs for 'Common', 'node1', and 'node2'. Under 'IP Addresses', there is a table with one entry: '10.5.0.110'. To the right of the table are buttons for 'Add', 'Remove', and 'Edit'. At the bottom right are buttons for '< Back', 'Next >', and 'Cancel'.

15. The **Recovery Action** page is displayed.
Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final action**.



The 'Monitor Resource Definition' dialog box is shown with the 'Recovery Action' tab selected. The left sidebar is the same as in the previous step, but 'Recovery Action' is now selected. The main area contains the following settings:
 - Recovery Action: A dropdown menu set to 'Execute only the final action'.
 - Recovery Target: A text field containing 'LocalServer' with a 'Browse...' button to its right.
 - Recovery Script Execution Count: A text field with '0' and a 'time' unit.
 - A section with a downward arrow containing:
 ☐ Execute Script before Reactivation
 Maximum Reactivation Count: A text field with '0' and a 'time' unit.
 - Another section with a downward arrow containing:
 ☐ Execute Script before Failover
 ☐ Execute migration before Failover
 Maximum Failover Count: A text field with '0' and a 'time' unit.
 - A final section with a downward arrow containing:
 ☐ Execute Script before Final Action
 Final Action: A dropdown menu set to 'No operation'.
 At the bottom right are buttons for 'Script Settings', '< Back', 'Finish', and 'Cancel'.

16. 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 Chapter 5, “Monitor resource details” 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.

Monitor Resource Definition

Steps

- Cluster
- Server
- Group
- Monitor
- Info
 - Monitor(common)
 - Monitor(special)
 - Recovery Action

Monitor Resource Definition

Type: multi-target monitor

Name: mtw1

Comment:

Get Licence Info

Description

Select the type of monitor resource and enter its name.

< Back Next > Cancel

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

Monitor Resource Definition

Steps

- Cluster
- Server
- Group
- Monitor
- 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: Server

< Back Next > Cancel

5. The **Monitor (special)** page 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**.

The dialog box is titled "Monitor Resource Definition". On the left, a "Steps" sidebar shows a tree view with "Cluster", "Server", "Group", "Monitor", "Info", "Monitor(common)", "Monitor(special)" (selected), and "Recovery Action". The main area is divided into two panes. The left pane, "Monitor Resources", contains a table with the following data:

Monitor Resource	Type
genw1	genw
ipw1	ipw
ipw2	ipw

Below the table are buttons "< Add" and "Remove >". The right pane, "Available Monitor Resources", is empty. At the bottom right are buttons "Tuning", "< Back", "Next >", and "Cancel".

6. Click **Next**.
7. The **Recovery Action** page 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.

The dialog box is titled "Monitor Resource Definition". The "Steps" sidebar on the left is the same as in the previous image, but "Recovery Action" is now selected. The main area contains the following settings:

- Rcovery Action:** A dropdown menu set to "Execute only the final action".
- Recovery Target:** A text field containing "LocalServer" with a "Browse" button to its right.
- Recovery Script Execution Count:** A text field with "0" and a "time" unit.
- Execute Script before Reactivation:** An unchecked checkbox.
- Maximum Reactivation Count:** A text field with "0" and a "time" unit.
- Execute Script before Failover:** An unchecked checkbox.
- Execute migration before Failover:** An unchecked checkbox.
- Maximum Failover Count:** A text field with "0" and a "time" unit.
- Execute Script before Final Action:** An unchecked checkbox.
- Final Action:** A dropdown menu set to "No operation".

At the bottom right are buttons "Script Settings", "< Back", "Finish", and "Cancel".

8. 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 "3.1 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 "11) Setting the inbound security rules" to the following:
 - **Frontend IP** (public IP address) of the load balancer

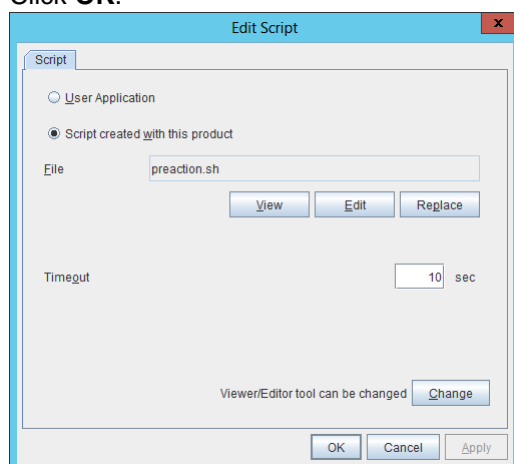
```

-----
#!/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**.



9. Click **Finish** to finish setting.

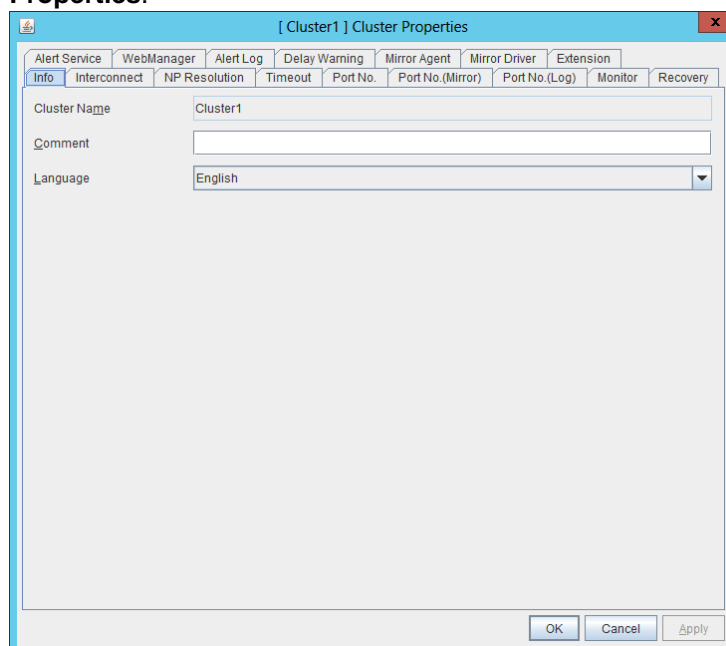
4) Setting the cluster properties

For details about the cluster properties, see “Cluster properties” in Chapter 2, “Functions of the Builder” in the *Reference Guide*.

◆ Cluster properties

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

1. Enter **Config Mode** from WebManager, right-click a cluster name, and select **Properties**.



2. Select the **Timeout** tab. For **Timeout of Heartbeat**, specify a value calculated by "A+B+30" ("Time that the multi-target monitor resource requires to detect an error"+30 seconds).

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)

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.

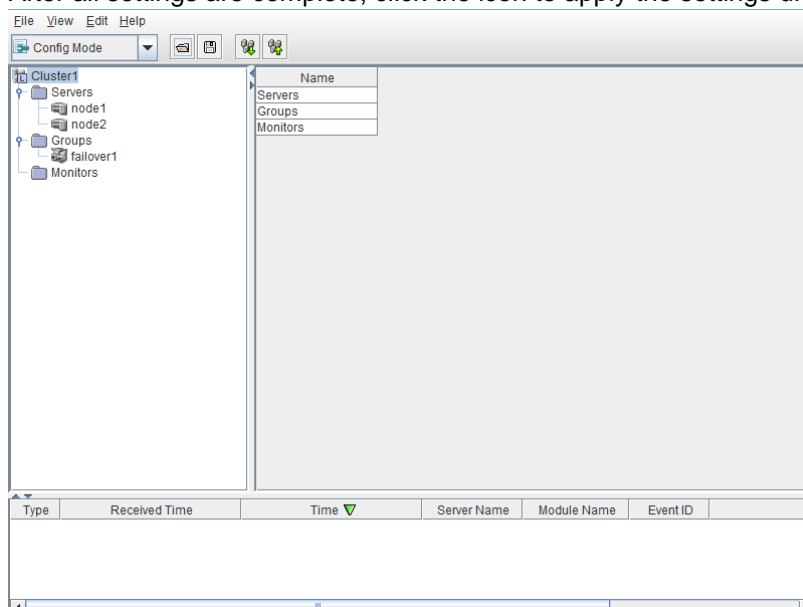
The screenshot shows the 'Cluster Properties' dialog box for 'Cluster1'. The 'Timeout' tab is selected. The 'Heartbeat' section is expanded, showing 'Interval' set to 3 seconds and 'Timeout' set to 120 seconds. The 'Server Sync Wait Time' is set to 5 minutes, and the 'Server Internal Timeout' is set to 180 seconds. At the bottom right, there is an 'Initialize' button. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

Property	Value	Unit
Server Sync Wait Time	5	min
Heartbeat Interval	3	sec
Heartbeat Timeout	120	sec
Server Internal Timeout	180	sec

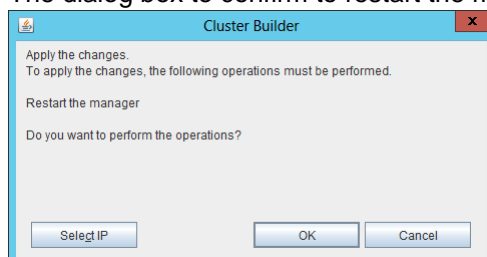
3. Click **OK**.

5) Applying the settings and starting the cluster

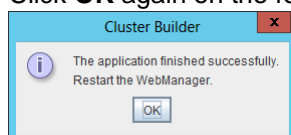
1. After all settings are complete, click the icon to apply the settings under the menu.



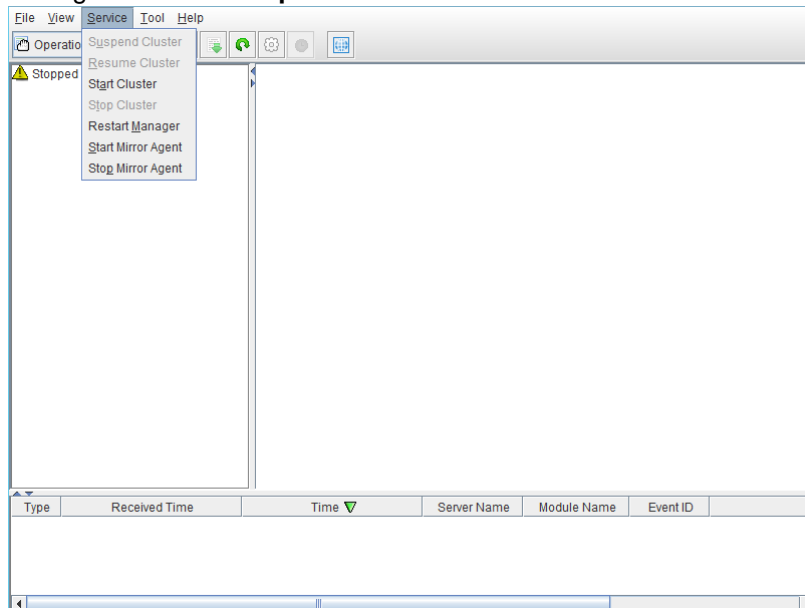
2. The dialog box to confirm to restart the manager is displayed.



3. Click **OK**.
4. Click **OK** again on the following dialog box.



5. Change the mode to **Operation Mode** and click **Start Cluster** from the **Service** menu.



4.4 Verifying the created environment

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

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

1. Start the failover group (failover1) on the active node (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.

Chapter 5 Cluster Creation Procedure (for an HA Cluster Using an Internal Load Balancer)

5.1 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	
Name	Vnet1
Resource group location	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 name	TestGroup1
Location	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	Vnet1
Location	Japan East
Backend pool: Name	TestBackendPool
Associated to	Availability set
Target virtual machine	node1 node2
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		
VM disk type	HDD	
User name	testlogin	
Password	PassWord_123	

Resource group name	TestGroup1	
Location	Japan East	
Storage account setting		
Name	clstorageacc1	
Performance	Standard	
Replication	Locally-redundant storage (LRS)	
Network security group setting		
Name	NetSecGroup1	
Availability set setting		
Name	AvailabilitySet1	
Update domains	5	
Fault domains	3	
Diagnostics storage account setting		
Name	clstorageaccdiag1	
Performance	Standard	
Replication	Locally-redundant storage (LRS)	
IP configuration setting		
IP address	10.5.0.110	10.5.0.111
Blob storage setting		
Name	Node1Blob	Node2Blob
Source type	New (empty disk)	
Account type	Standard (HDD)	
Size	20	

- EXPRESSCLUSTER settings (cluster properties)

Setting item	Setting value	
	node1	node2
Cluster Name	Cluster1	
Server Name	node1	node2
NP Resolution Tab: Type	Ping	
NP Resolution Tab: Ping Target	10.5.0.5	
NP Resolution Tab: <server> column	Use	Use

- EXPRESSCLUSTER settings (failover group)

Resource name	Setting item	Setting value
Mirror disk resource	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
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	-	-
Azure probe port monitor resource	Name	azureppw1
	Recovery Target	azurepp1

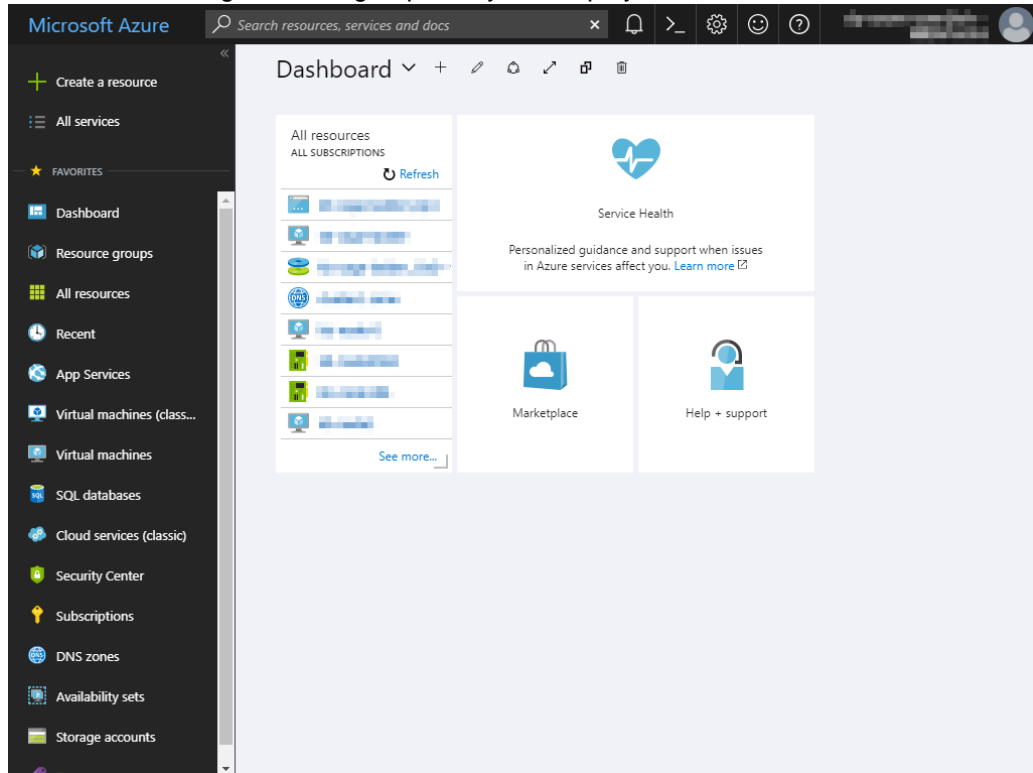
Azure load balance monitor resource	Name	aurelbw1
	Recovery Target	azurepp1

5.2 Configuring Microsoft Azure

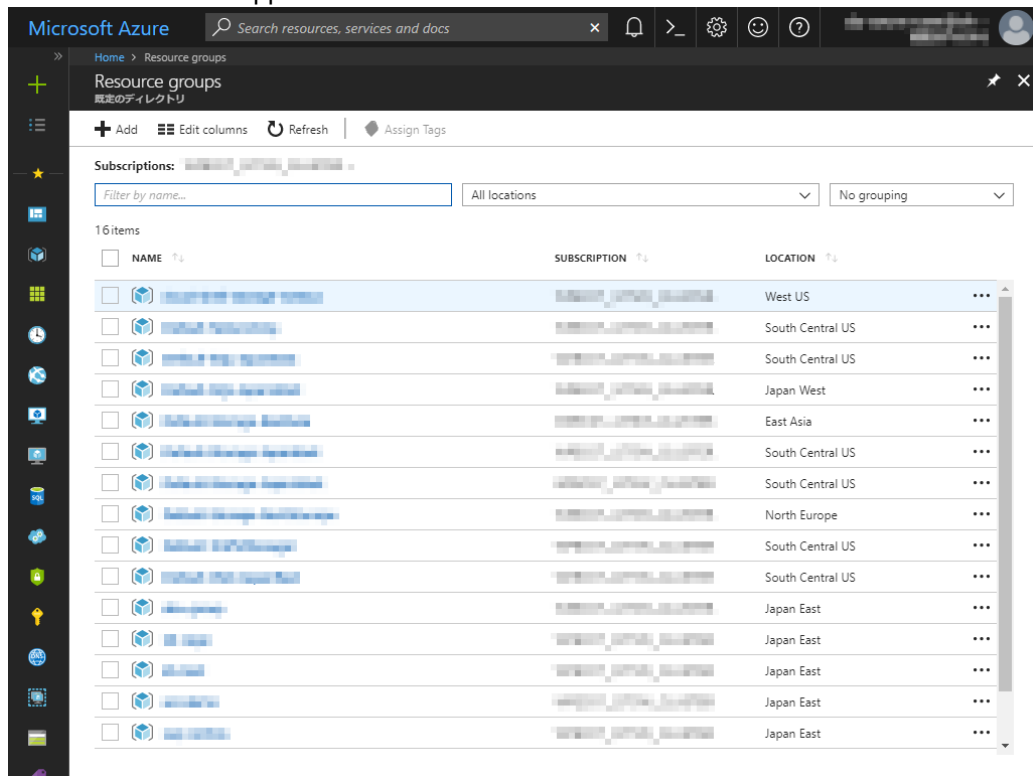
1) Creating a resource group

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

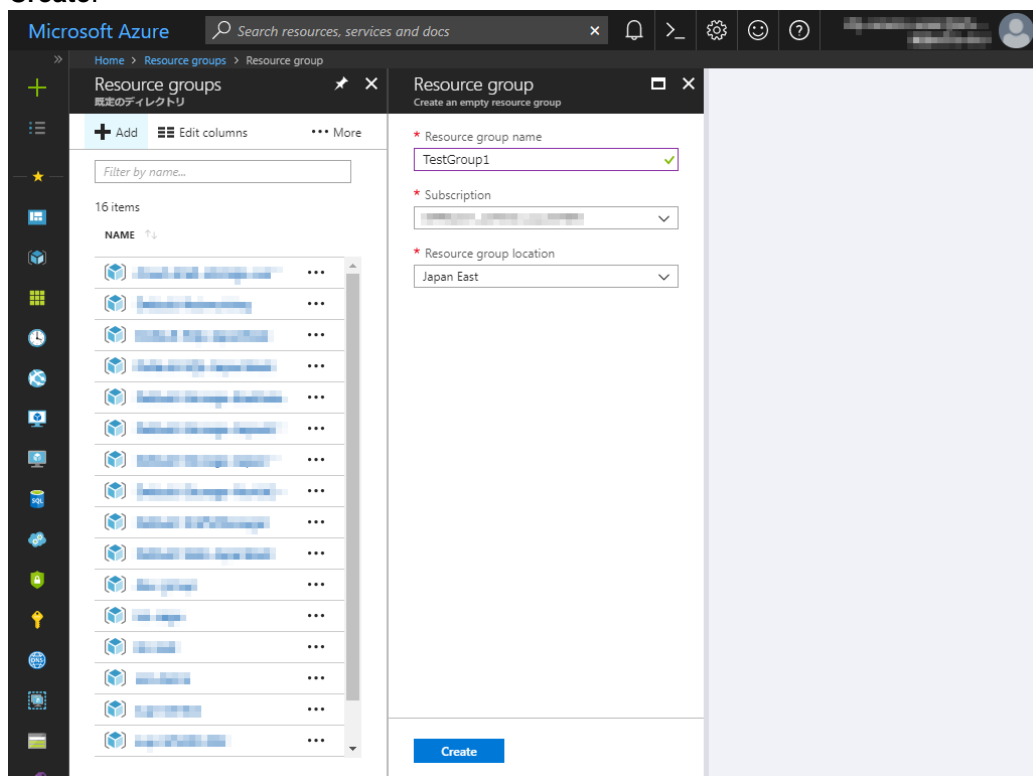
1. Select **Resource groups** or the resource group icon in the menu on the left side of the window. If there are existing resource groups, they are displayed in a list.



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



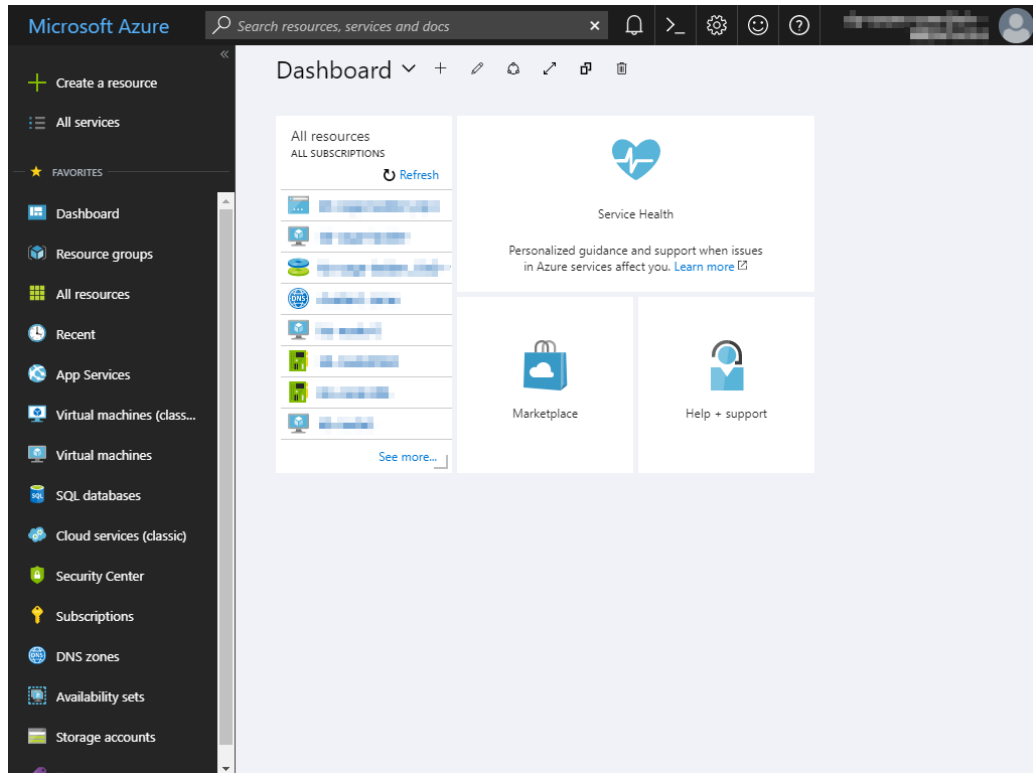
3. Specify **Resource group name**, **Subscription**, and **Resource group location**, and click **Create**.



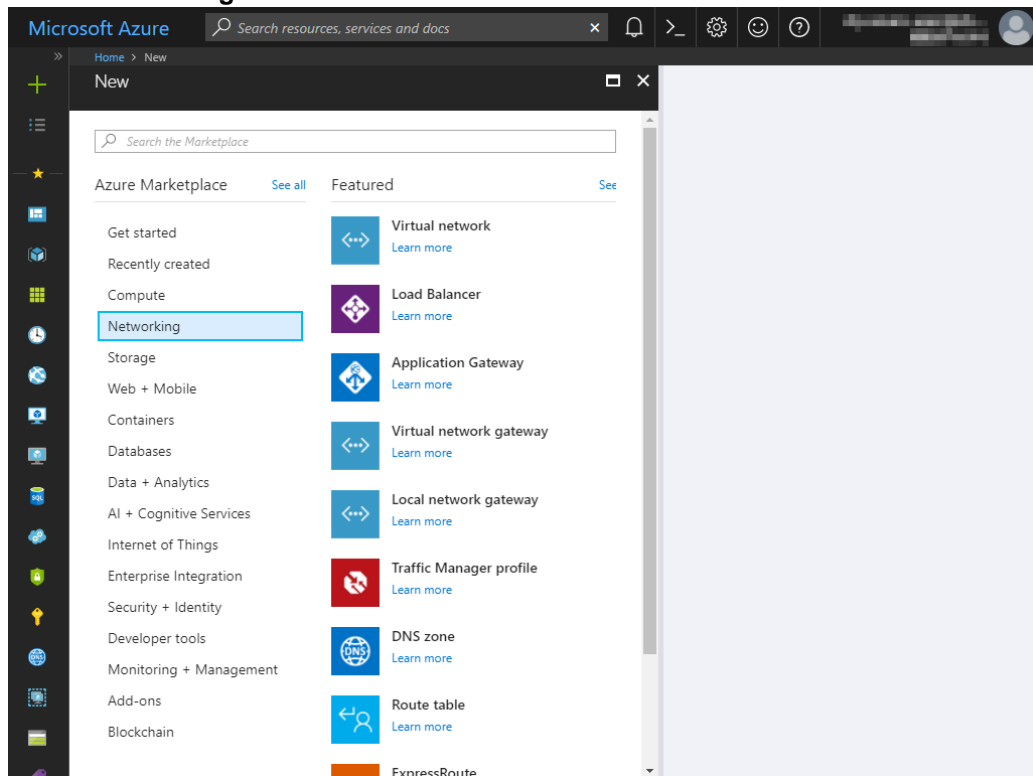
2) Creating a virtual network

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

1. Select **+Create a resource** or the **+** icon in the menu on the left side of the window.



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



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

The screenshot shows the 'Create virtual network' form in the Microsoft Azure portal. The form is titled 'Create virtual network' and is located under the 'Home > New > Create virtual network' breadcrumb. The form fields are as follows:

- Name:** Vnet1 (with a green checkmark)
- Address space:** 10.5.0.0/24 (with a green checkmark). Below the input, it says '10.5.0.0 - 10.5.0.255 (256 addresses)'.
- Subscription:** A dropdown menu showing a blurred subscription name.
- Resource group:** ☐ Create new ☒ Use existing. Below, a dropdown menu shows 'TestGroup1'.
- Location:** A dropdown menu showing 'Japan East'.
- Subnet:**
 - Name:** Vnet1-1 (with a green checkmark)
 - Address range:** 10.5.0.0/24 (with a green checkmark). Below the input, it says '10.5.0.0 - 10.5.0.255 (256 addresses)'.
- Service endpoints:** ☒ Disabled ☐ Enabled
- Pin to dashboard:** ☐
- Create:** A blue button.
- Automation options:** A link.

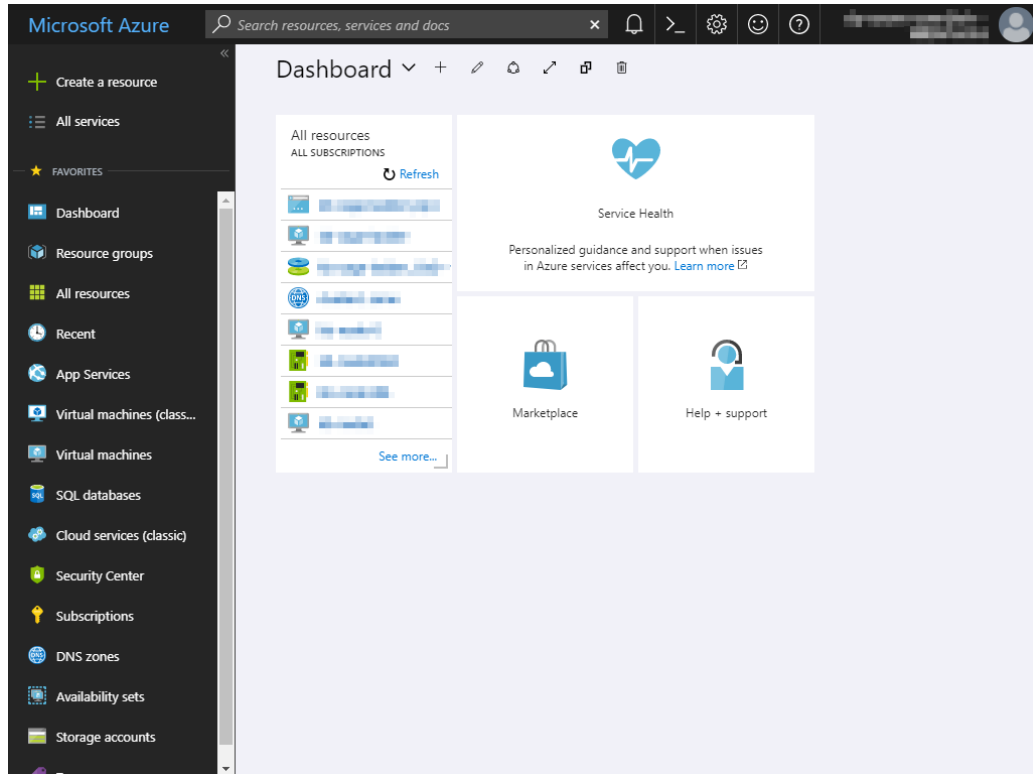
The form is part of a larger window with a dark header bar containing the 'Microsoft Azure' logo, a search bar, and navigation icons. A sidebar on the left contains various Azure service icons.

3) Creating a virtual machine

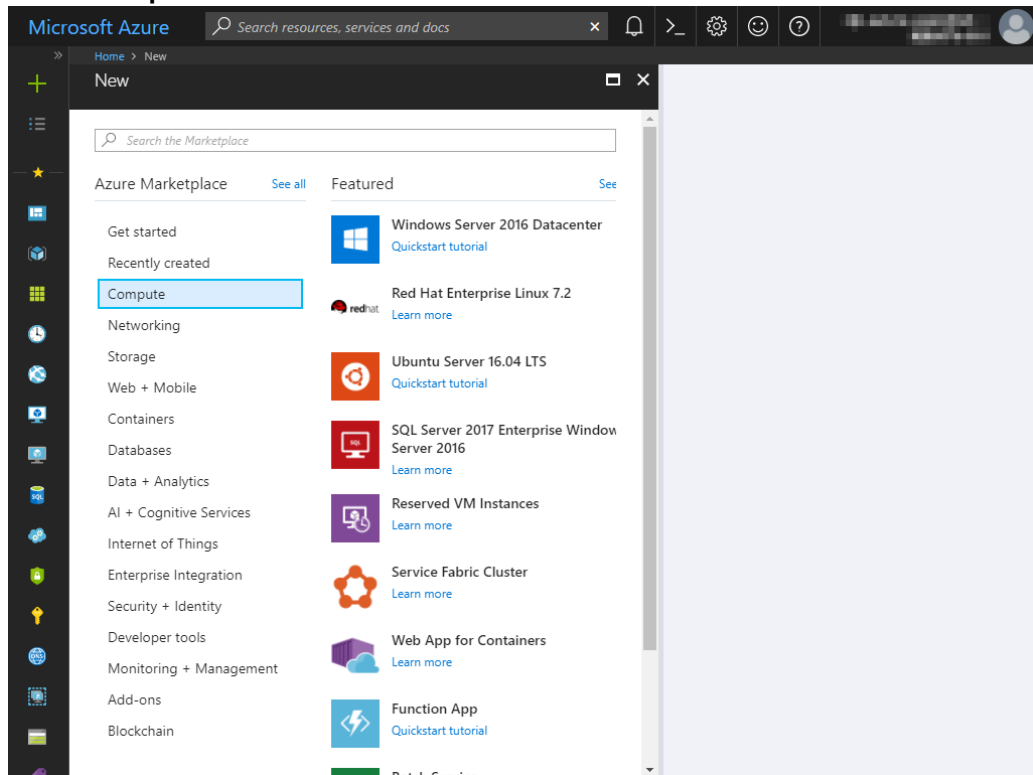
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create virtual machines and disks following the steps below.

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

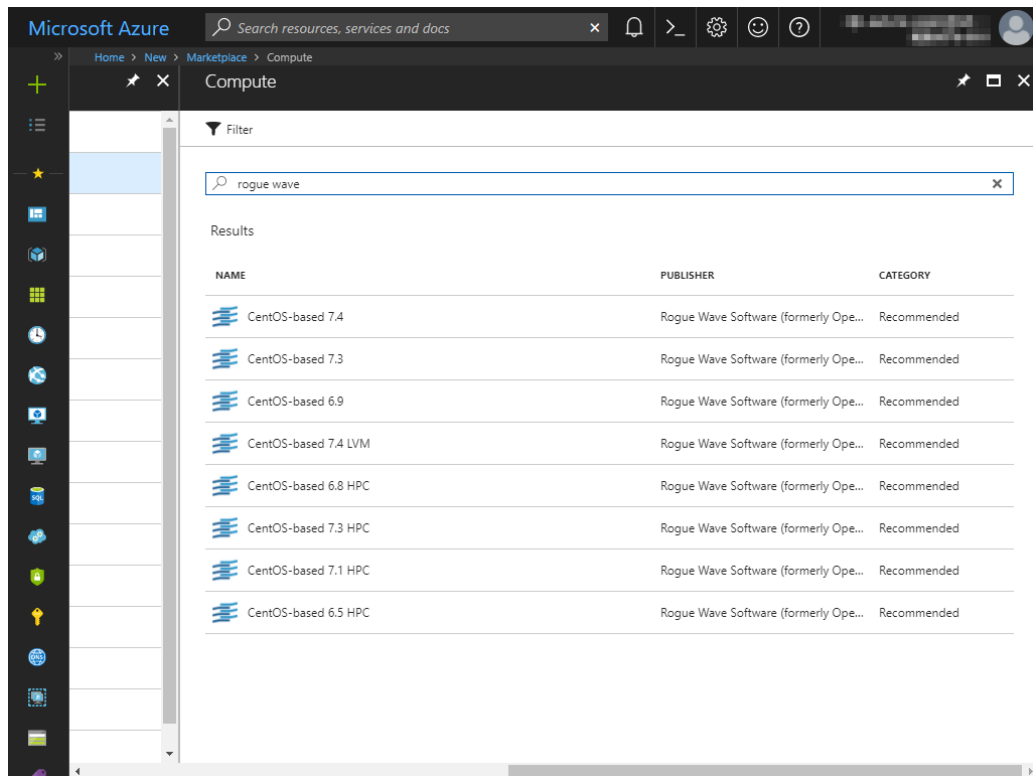
1. Select **+Create a resource** or the **+** icon in the menu on the left side of the window.



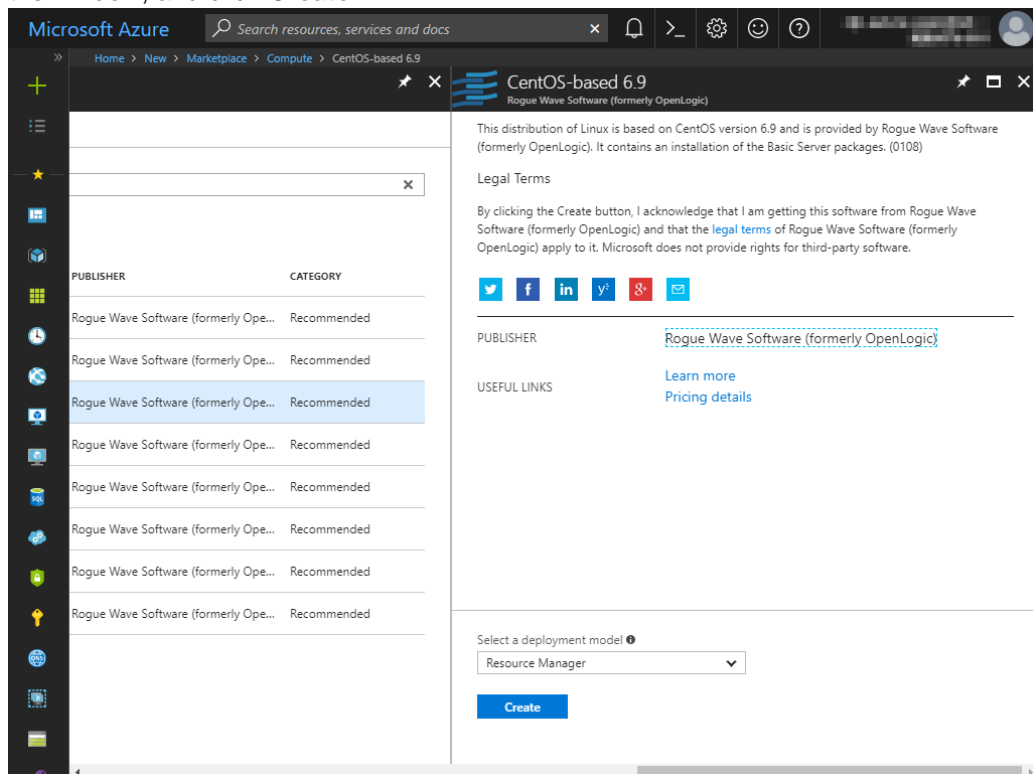
2. Select **Compute** and then **See all**.



3. Select **CentOS-based 6.9** or **CentOS-based 7.4**.



4. Confirm that **Resource Manager** is selected for **Select a deployment model** at the bottom of the window, and click **Create**.



- The **Basics** blade is displayed. Specify **Name**, **VM disk type**, **User name**, **Password**, **Confirm password**, **Subscription**, **Resource group name**, and **Location**, and click **OK**. For **Name**, specify node1 for node1 and node2 for node2.

Microsoft Azure Search resources, services and docs

Home > New > Marketplace > Compute > CentOS-based 6.9 > Create virtual machine > Basics

Create virtual machine Basics

- Basics Configure basic settings
- Size Choose virtual machine size
- Settings Configure optional features
- Summary CentOS-based 6.9

* Name node1 ✓

VM disk type HDD

* User name testlogin

* Authentication type SSH public key Password

* Password

* Confirm password

Subscription

* Resource group Create new Use existing TestGroup1

* Location Japan East

OK

- The **Choose a size** blade is displayed. Select the size appropriate for the usage purpose of the virtual machines from the list and click **Select**. In this guide, **A1 Standard** is selected.

Microsoft Azure Search resources, services and docs

Home > New > Marketplace > Compute > CentOS-based 6.9 > Create virtual machine > Choose a size

Create virtual machine Choose a size

Browse the available sizes and their features

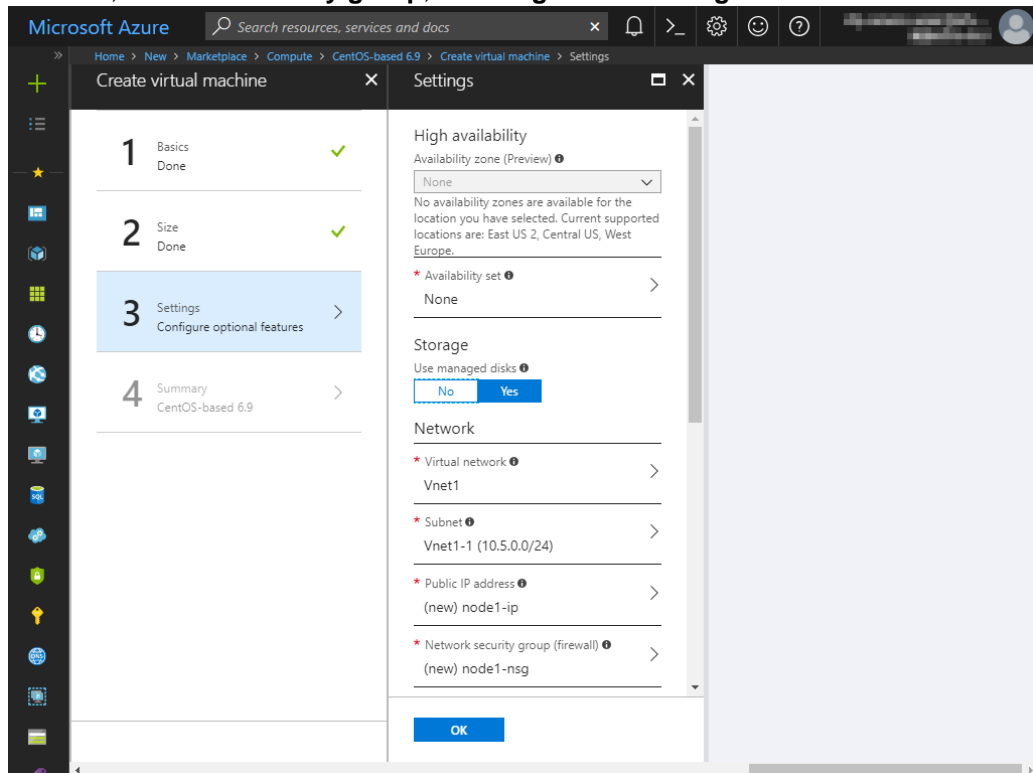
Supported disk type HDD Minimum vCPUs 1 Minimum memory (GiB) 0

★ Recommended | View all

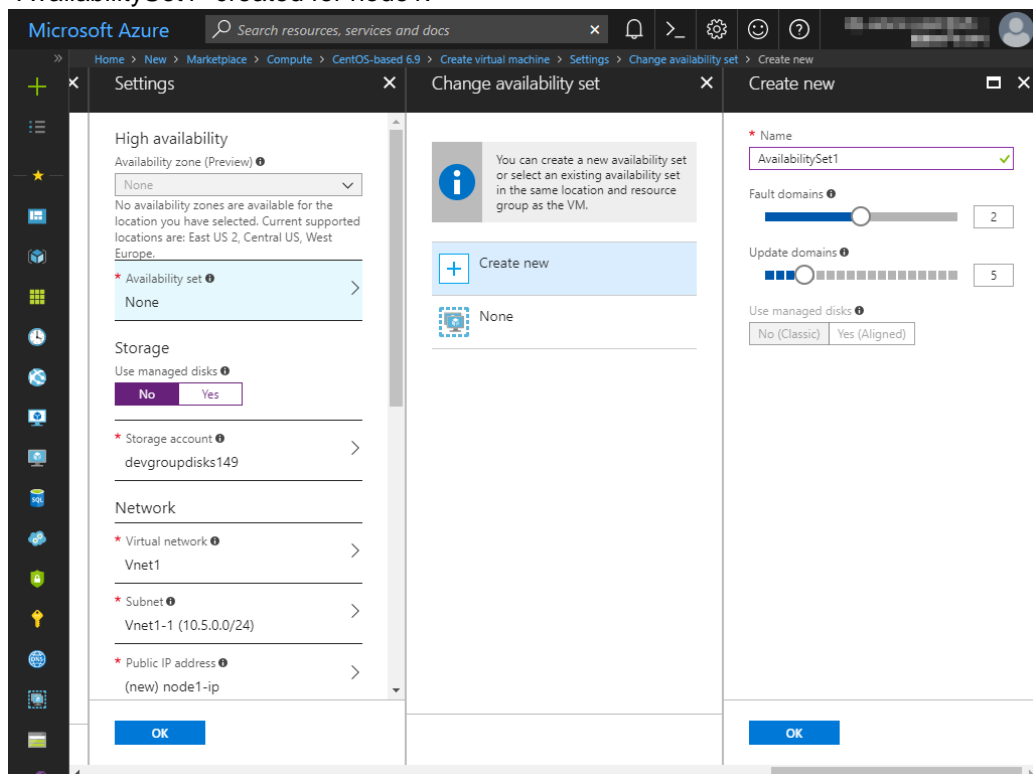
D1_V2 Standard	D1 Standard	A1 Standard
1 vCPU	1 vCPU	1 vCPU
3.5 GB	3.5 GB	1.75 GB
4 Data disks	4 Data disks	2 Data disks
2x500 Max IOPS	2x500 Max IOPS	2x500 Max IOPS
50 GB Local SSD	50 GB Local SSD	
Load balancing	Load balancing	Load balancing
7,015.92 JPY/MONTH (ESTIMATED)	7,343.28 JPY/MONTH (ESTIMATED)	3,935.76 JPY/MONTH (ESTIMATED)

Select

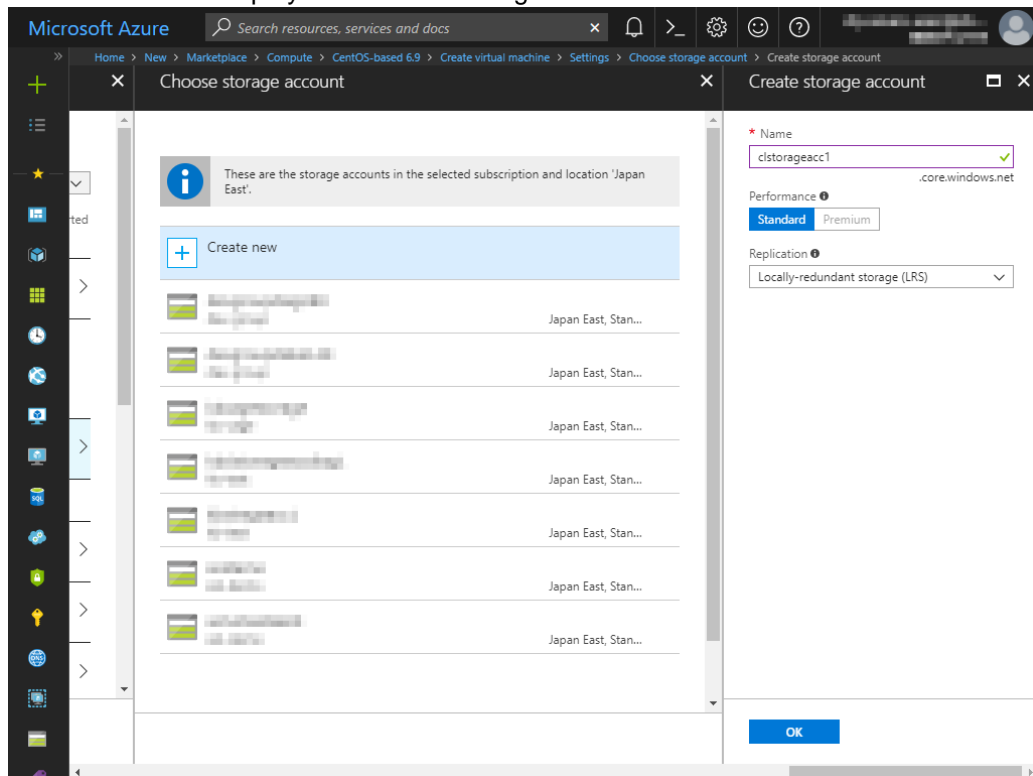
7. The **Settings** blade is displayed. Specify **Availability set**, **Storage account**, **Public IP address**, **Network security group**, and **Diagnostics storage account**.



8. Select **No** for **Use managed disks** for **Storage**.
9. Return to the **Settings** blade and select **Availability set**. For node1, the **Change availability set** blade is displayed. Select **Create new**. Specify **Name**, **Fault domains**, **Update domains**, and click **OK**. For node2, the **Change availability set** blade is displayed. Select "AvailabilitySet1" created for node1.

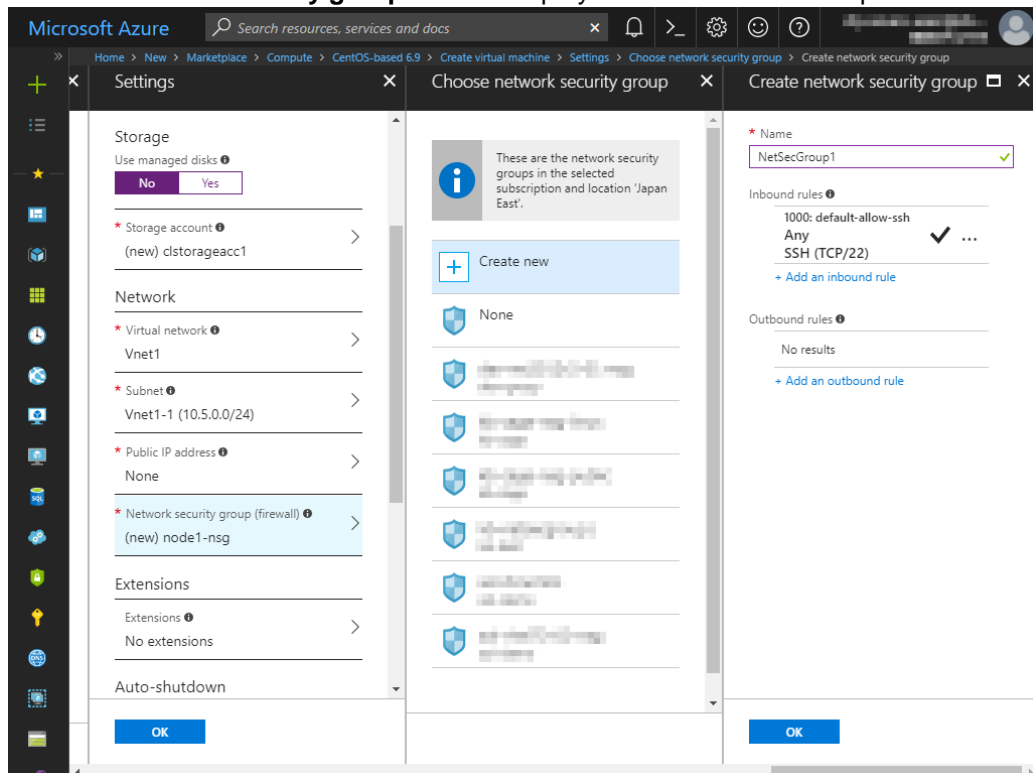


10. Select **Storage account**. For node1, the **Create storage account** blade is displayed. Specify **Name**, **Performance**, and **Replication**, and click **OK**. For node2, the **Choose storage account** blade is displayed. Select "clstorageacc1" created for node1.

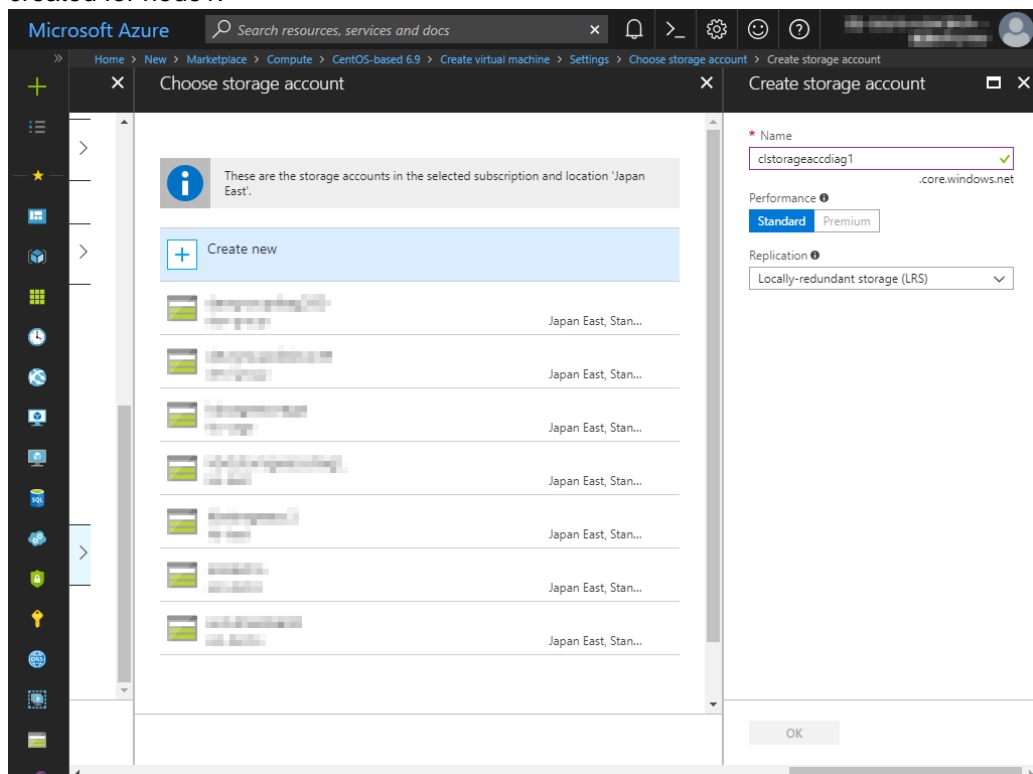


11. Return to the **Settings** blade and select **Public IP address**.
12. The **Choose public IP address** blade is displayed. Select **None**. Ignore the **Create public IP address** blade.

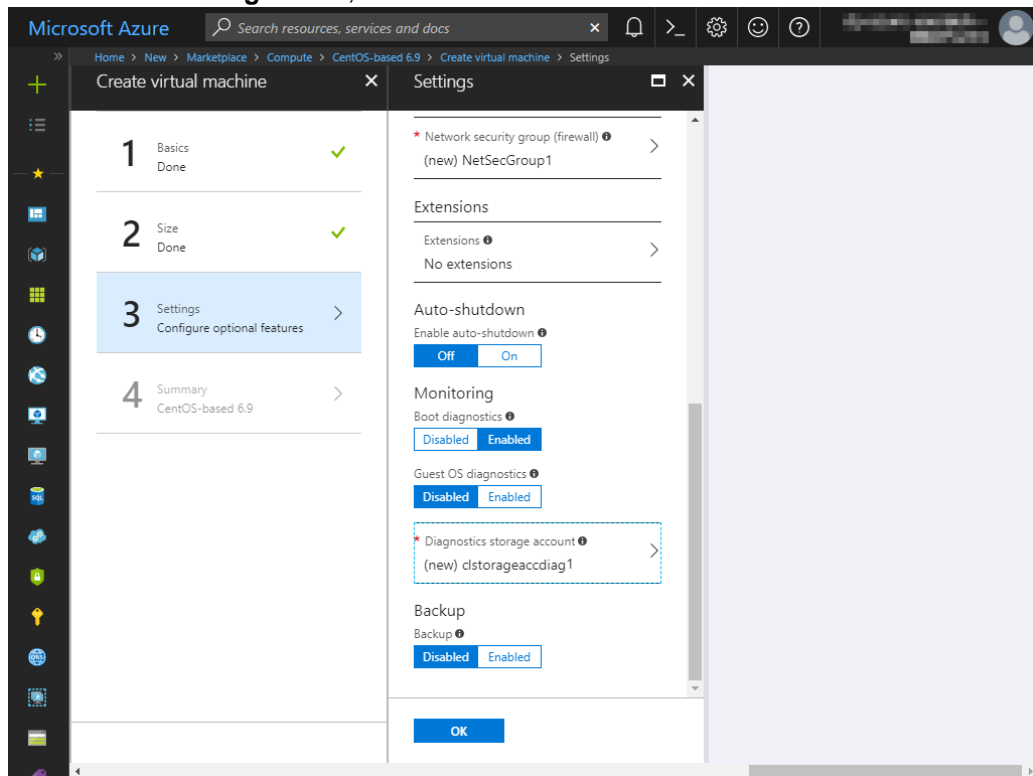
13. Return to the **Settings** blade and select **Network security group**. For node1, the **Create network security group** blade is displayed. Specify **Name**, and click **OK**. For node2, the **Choose network security group** blade is displayed. Select NetSecGroup1 created for node1.



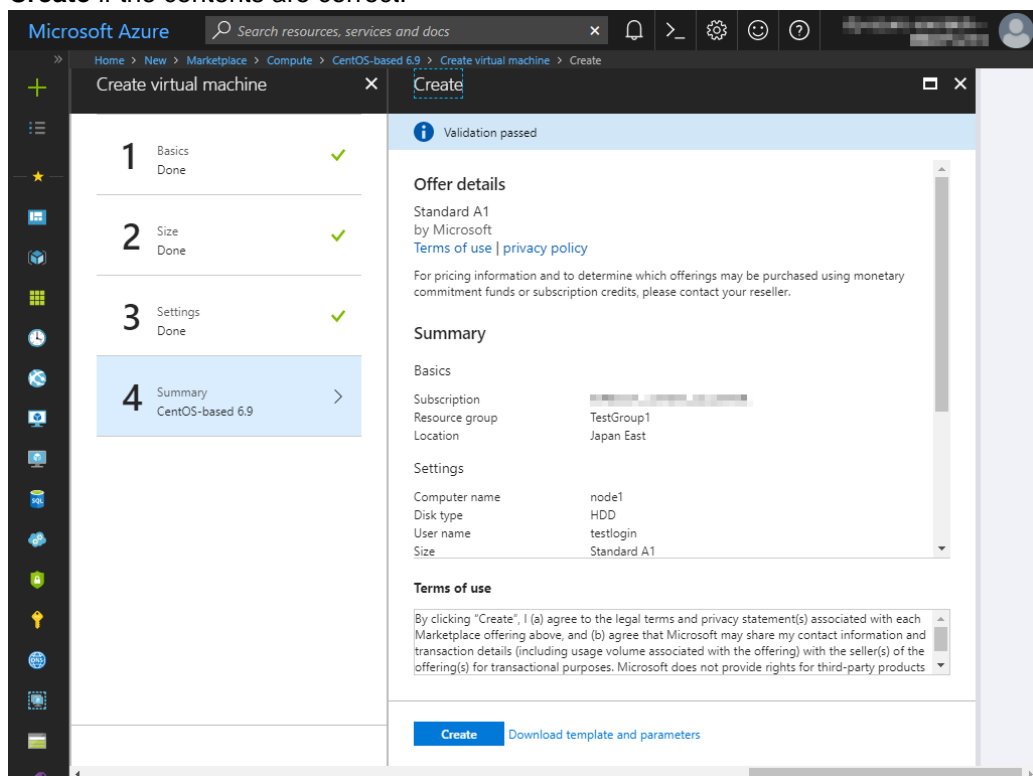
14. Return to the **Settings** blade and select **Diagnostics storage account**. For node1, the **Create storage account** blade is displayed. Specify **Name**, **Performance**, and **Replication**, and click **OK**. For node2, the **Choose storage account** blade is displayed. Select clstorageacctdiag1 created for node1.



15. Return to the **Settings** blade, and click **OK**.



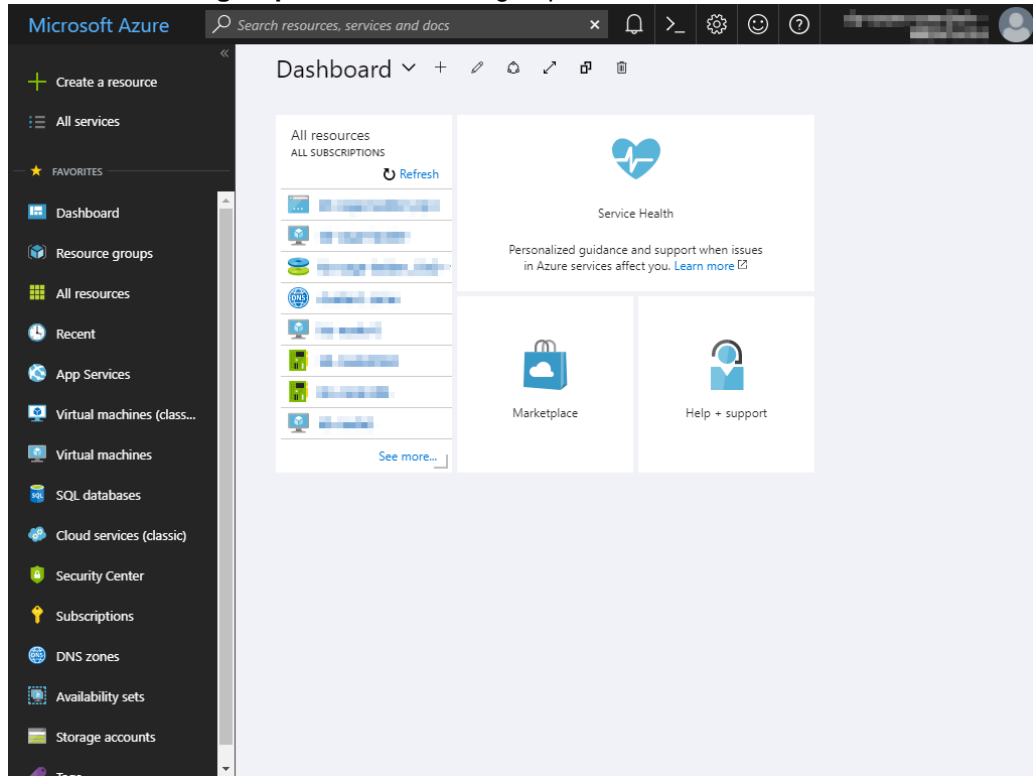
16. The **Create** blade is displayed. Check the contents displayed on the **Create** blade and click **Create** if the contents are correct.



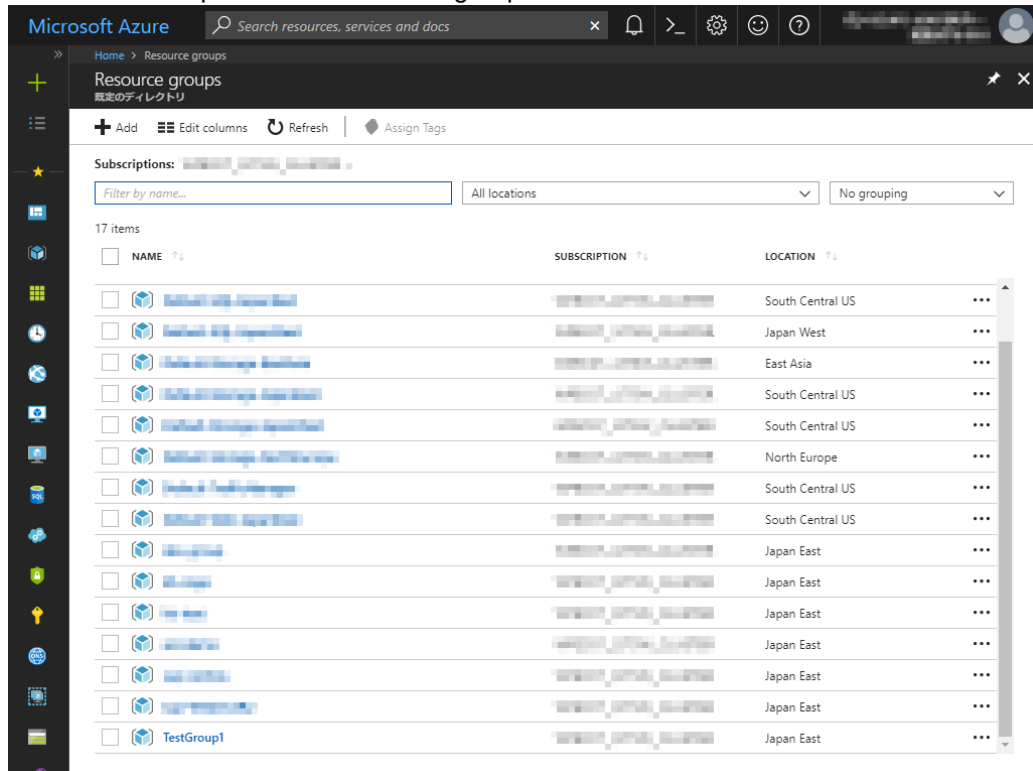
4) Setting a private IP address

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 **Resource groups** or the resource group icon in the menu on the left side of the window.



2. Select **TestGroup1** from the resource group list.



Cluster Creation Procedure (for an HA Cluster Using an Internal Load Balancer)

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

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1

TestGroup1 Resource group

Subscription (change) Deployments 3 Succeeded

Subscription ID

Filter by name... All types All locations No

9 items Show all resources

NAME	TYPE	LOCATION
AvailabilitySet1	Availability set	Japan East
clstorageacct1	Storage account	Japan East
clstorageacctdiag1	Storage account	Japan East
NetSecGroup1	Network security group	Japan East
node1	Virtual machine	Japan East
node1435	Network interface	Japan East
node2	Virtual machine	Japan East
node2680	Network interface	Japan East
Vnet1	Virtual network	Japan East

4. Select **Networking**.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1 > node1 - Networking

node1 - Networking Virtual machine

Attach network interface Detach network interface

Network Interface: node1435 Effective security rules Topology

Virtual network/subnet: Vnet1/Vnet1-1 Public IP: None Private IP: 10.5.0.4

INBOUND PORT RULES

Network security group NetSecGroup1 (attached to network interface: node1435) Impacts 0 subnets, 2 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATI...	ACTION
1000	default-allow-ssh	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNet...	VirtualNet...	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoa...	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

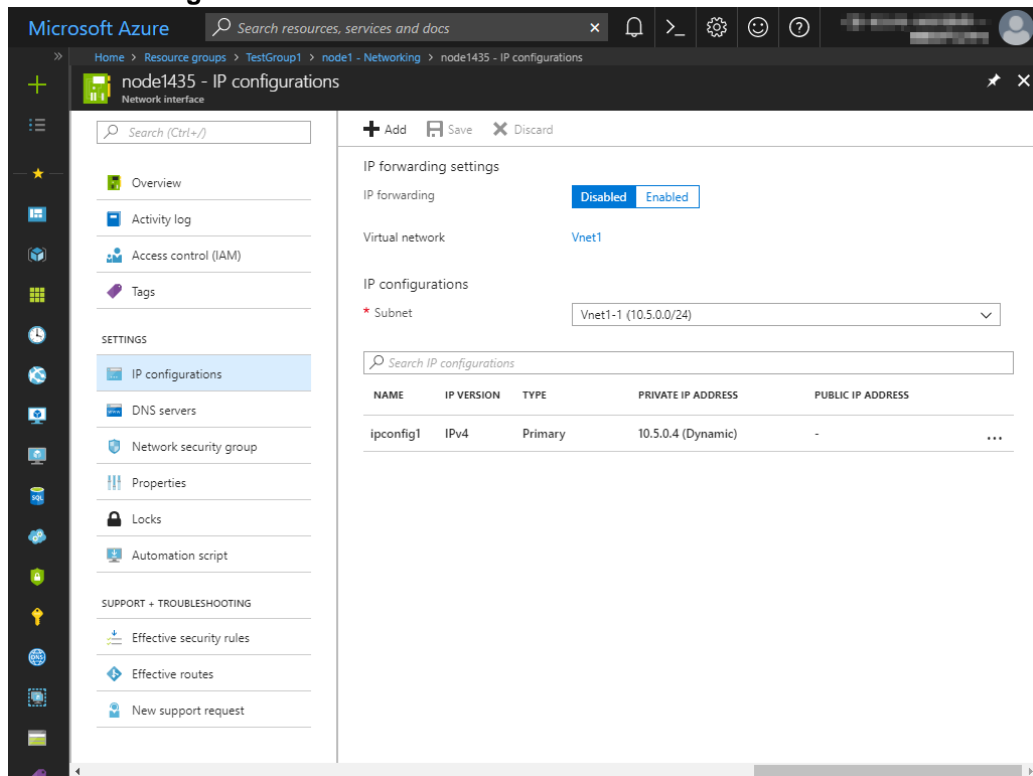
OUTBOUND PORT RULES

Network security group NetSecGroup1 (attached to network interface: node1435) Impacts 0 subnets, 2 network interfaces

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATI...	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNet...	VirtualNet...	Allow
65001	AllowInternetOutBou...	Any	Any	Any	Internet	Allow

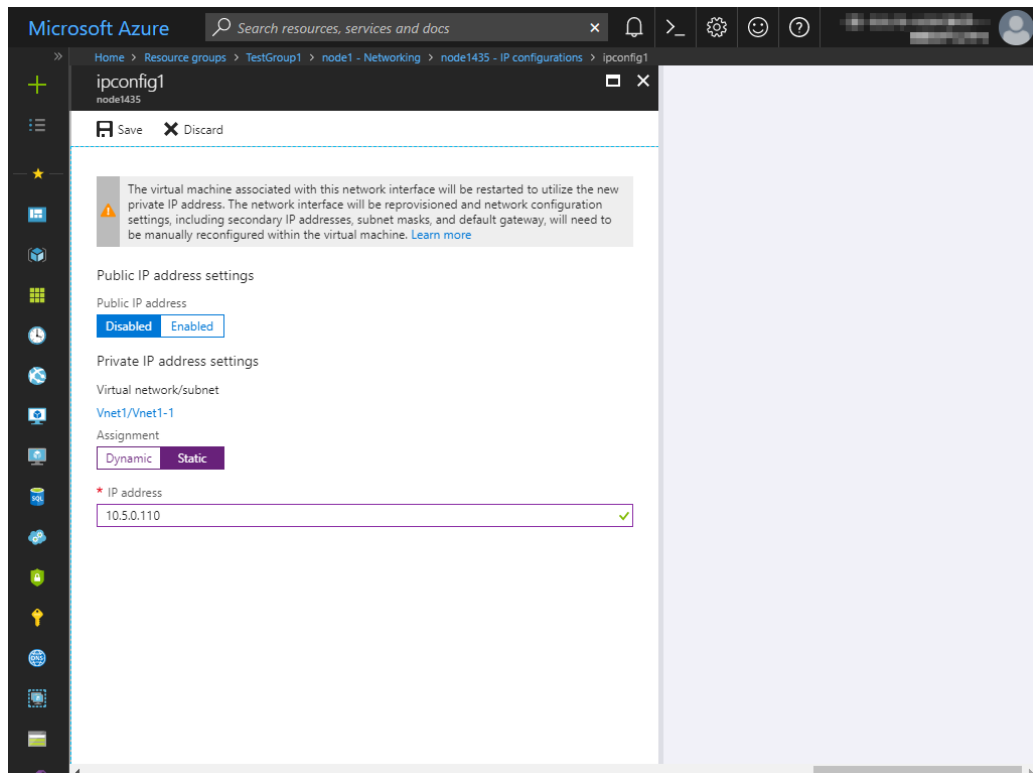
5. Select a network interface displayed in the list. The network interface name is generated automatically.

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.

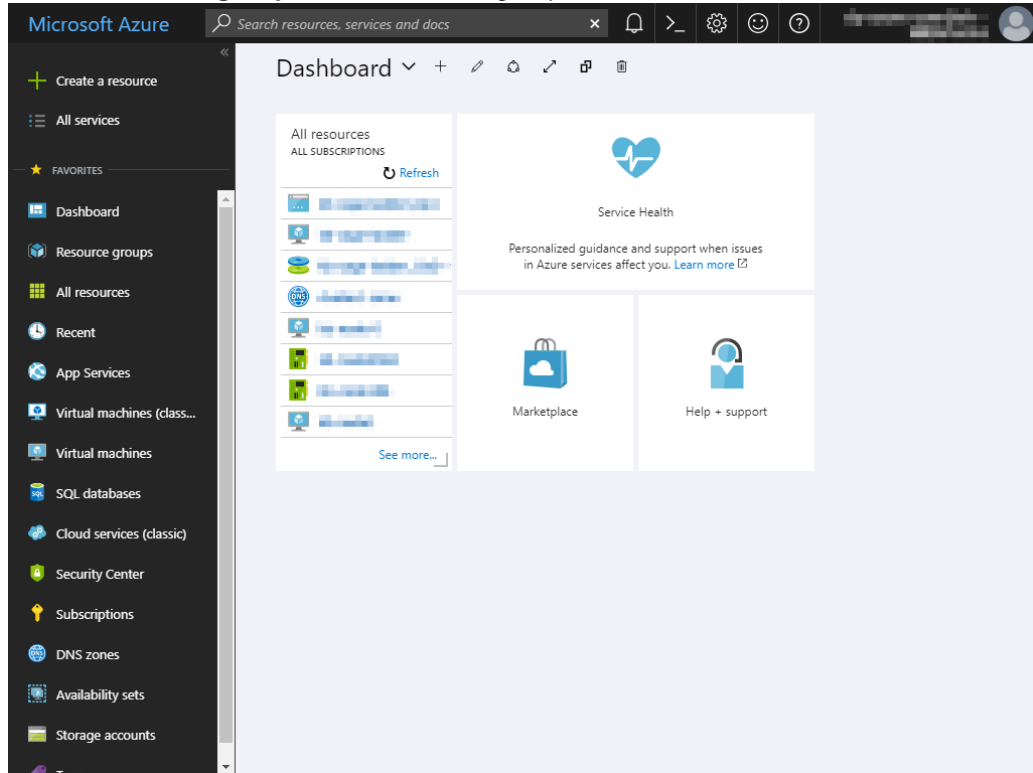


9. The virtual machines restart automatically so that new private IP addresses can be used.

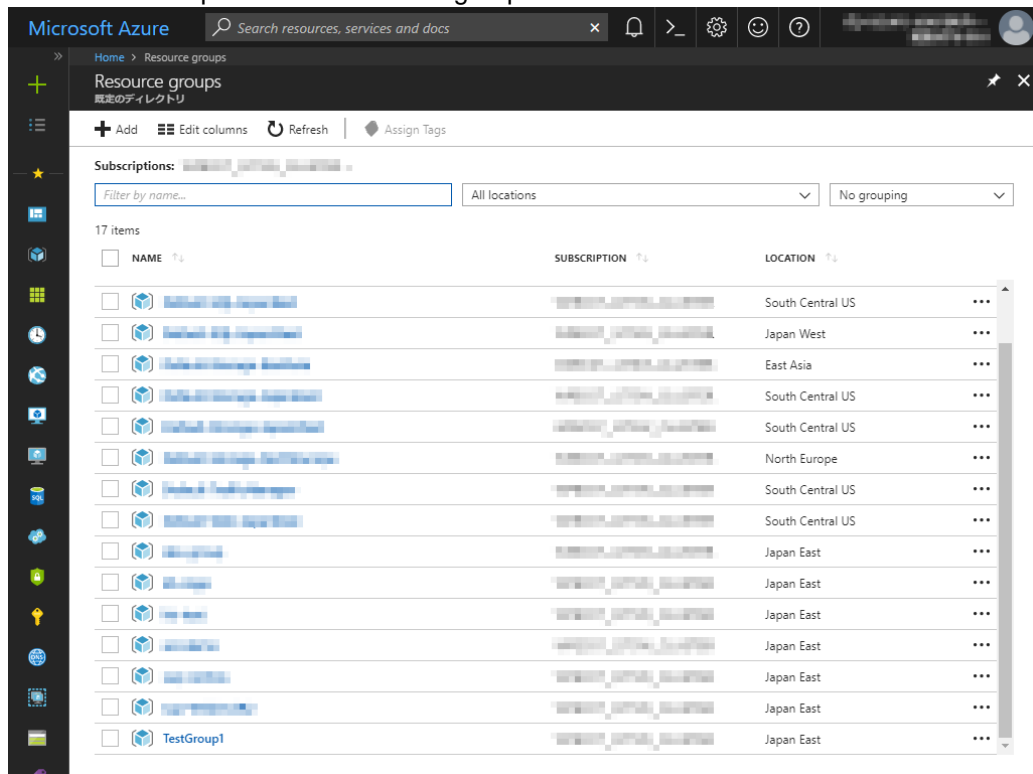
5) Adding Blob storage

Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and add Blob storage to be used for a mirror disk (cluster partition or data partition). Change the settings of node1 and then node2.

1. Select **Resource groups** or the resource group icon in the menu on the left side of the window.



2. Select TestGroup1 from the resource group list.



3. The summary of TestGroup1 is displayed. Select virtual machine node1 or node2 to which to add Blob storage from the item list and select **Disk**.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1

TestGroup1 Resource group

Subscription (change) Deployments 3 Succeeded

Subscription ID

Filter by name... All types All locations No

9 items Show all resources

NAME	TYPE	LOCATION
AvailabilitySet1	Availability set	Japan East
clstorageacct1	Storage account	Japan East
clstorageacctdiag1	Storage account	Japan East
NetSecGroup1	Network security group	Japan East
node1	Virtual machine	Japan East
node1435	Network interface	Japan East
node2	Virtual machine	Japan East
node2680	Network interface	Japan East
Vnet1	Virtual network	Japan East

4. Select **+Add data disk**.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1 > node1 - Disks

node1 - Disks Virtual machine

Edit

OS disk

NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOS
node1	30 GiB	Standard_LRS	Not enabled	Rea

Data disks

None

+ Add data disk

- The **Attach unmanaged disk** blade is displayed. Click **Browse** right to the **Storage container** text box. For **Name** and **Storage blob name**, the automatically generated default values are entered.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1 > node1 - Disks > Attach unmanaged disk

Attach unmanaged disk

* Name
node1-20180215-104728 ✓

* Source type
New (empty disk) ✓

* Account type
Standard (HDD) ✓

* Size (GiB)
1023

ESTIMATED PERFORMANCE
IOPS limit 500
Throughput limit (MB/s) 60

* Storage container
 [Browse](#)

* Storage blob name
node1-20180215-104728.vhd ✓

[OK](#)

- Select clstorageacc1 from the storage account list.

Microsoft Azure Search resources, services and docs

Home > Resource groups > TestGroup1 > node1 - Disks > Attach unmanaged disk > Storage accounts

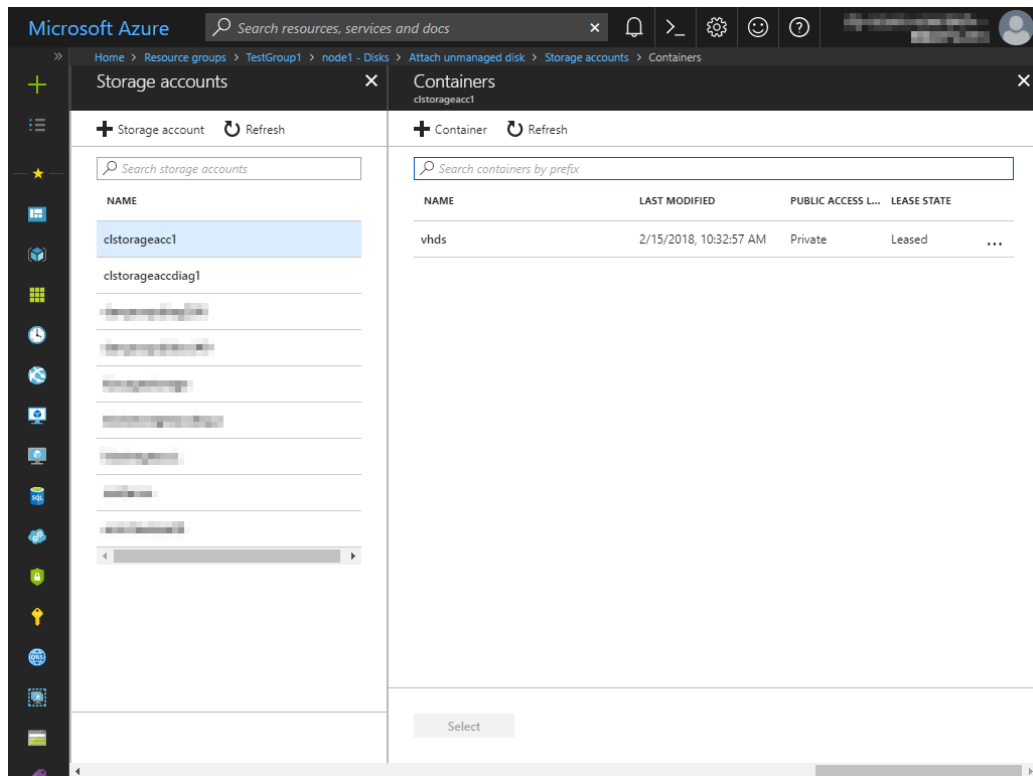
Storage accounts

+ Storage account Refresh

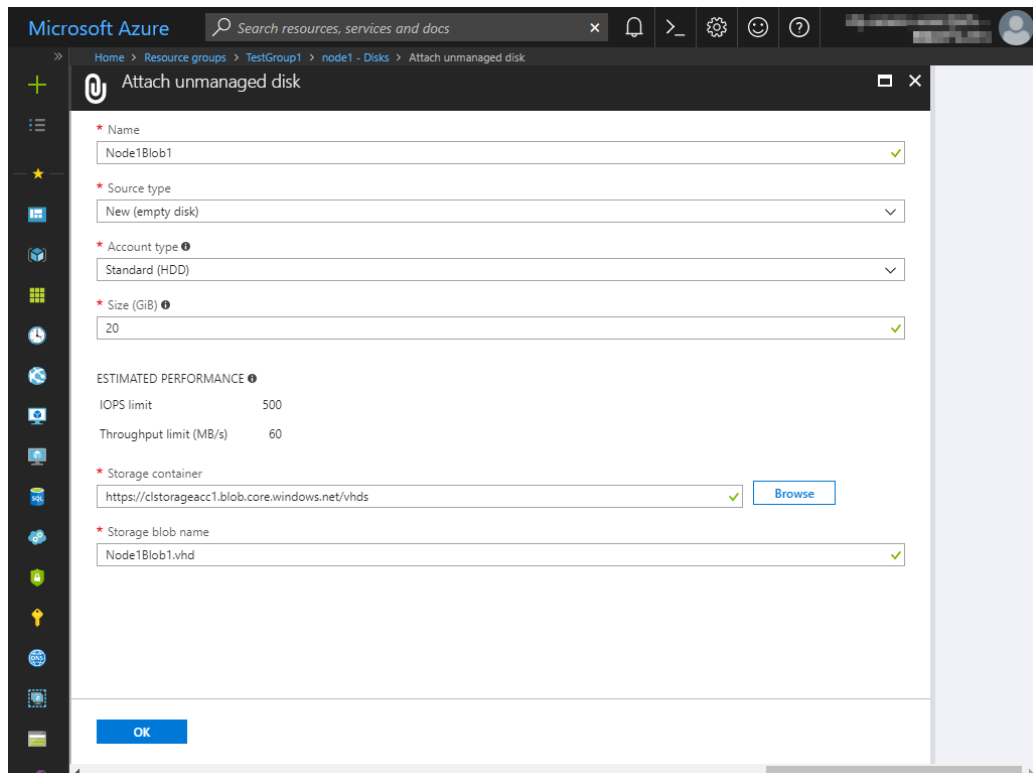
Search storage accounts

NAME	TYPE	RESOURCE GROUP
clstorageacc1	Standard-LRS	TestGroup1
clstorageaccdiag1	Standard-LRS	TestGroup1
clstorageaccdiag2	Standard-LRS	TestGroup1
clstorageaccdiag3	Standard-LRS	TestGroup1
clstorageaccdiag4	Standard-LRS	TestGroup1
clstorageaccdiag5	Standard-LRS	TestGroup1
clstorageaccdiag6	Standard-LRS	TestGroup1
clstorageaccdiag7	Standard-LRS	TestGroup1
clstorageaccdiag8	Standard-LRS	TestGroup1
clstorageaccdiag9	Standard-LRS	TestGroup1

7. Select vhds from the container list and click **Select**.



8. The **Attach unmanaged disk** blade is displayed again. Specify **Name**, **Source type**, **Account type**, **Size**, and **Storage blob name**, and click **OK**. For **Name**, specify Node1Blob for node1 and Node2Blob for node2. For **Storage blob name**, specify Node1Blob.vhd for node1 and Node2Blob.vhd for node2.



9. Click **Save**.

The screenshot shows the Microsoft Azure portal interface for configuring disks for a virtual machine named 'node1'. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and various settings. The main content area shows the 'node1 - Disks' configuration page with a 'Save' button and a 'Discard' button. The page displays the OS disk and a data disk named 'Node1Blob1' with a size of 20 GiB. The 'Save' button is highlighted.

Microsoft Azure Search resources, services and docs

Home > node1 - Disks

node1 - Disks
Virtual machine

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems

SETTINGS

Networking
Disks
Size
Extensions
Availability set
Configuration
Properties
Locks
Automation script

OPERATIONS

Save Discard

OS disk

NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOS
node1	30 GiB	Standard_LRS	Not enabled	Re

Data disks

LUN	NAME	SIZE	STORAGE ACCOUNT TYPE	ENCRYPTION	HOS
0	Node1Blob1	20 GiB	Standard_LRS	Not enabled	Ni

+ Add data disk

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 Blob storage.
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 Chapter 1, "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

8      16      73400320      sdb
8      17      73398272      sdb1
8       0      31459328      sda
8       1      31456256      sda1
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. The following is an example of creating one partition including all areas of /dev/sdc.

```
$ sudo fdisk /dev/sdc
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0xe3c83b13.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.
```

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

The device presents a logical sector size that is smaller than the physical sector size. Aligning to a physical sector (or optimal I/O) size boundary is recommended, or performance may be impacted.

WARNING: DOS-compatible mode is deprecated. It's strongly recommended to switch off the mode (command 'c') and change display units to sectors (command 'u').

Command (m for help): n

Command action

e extended

p primary partition (1-4)

p

Partition number (1-4): 1

First cylinder (1-2610, default 1):

Using default value 1

Last cylinder, +cylinders or +size{K,M,G} (1-2610, default 2610): +1G

Command (m for help): p

```
Disk /dev/sdc: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0xe29ed566
```

Device	Boot	Start	End	Blocks	Id	System
--------	------	-------	-----	--------	----	--------

```
/dev/sdc1      1      132  1060256+ 83 Linux
Partition 1 does not end on cylinder boundary.
Partition 1 does not start on physical sector boundary.
```

```
Command (m for help): n
Command action
  e  extended
  p  primary partition (1-4)
p
Partition number (1-4): 2
First cylinder (132-2610, default 132):
Using default value 132
Last cylinder, +cylinders or +size{K,M,G} (132-2610, default 2610):
Using default value 2610
Command (m for help): p
```

```
Disk /dev/sdc: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 4096 bytes
I/O size (minimum/optimal): 4096 bytes / 4096 bytes
Disk identifier: 0xe29ed566
```

Device	Boot	Start	End	Blocks	Id	System
/dev/sdc1		1	132	1060256+	83	Linux
Partition 1 does not end on cylinder boundary.						
Partition 1 does not start on physical sector boundary.						
/dev/sdc2		132	2610	19904537	83	Linux

```
Command (m for help): w
The partition table has been altered!
```

```
Calling ioctl() to re-read partition table.
Syncing disks.
```

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

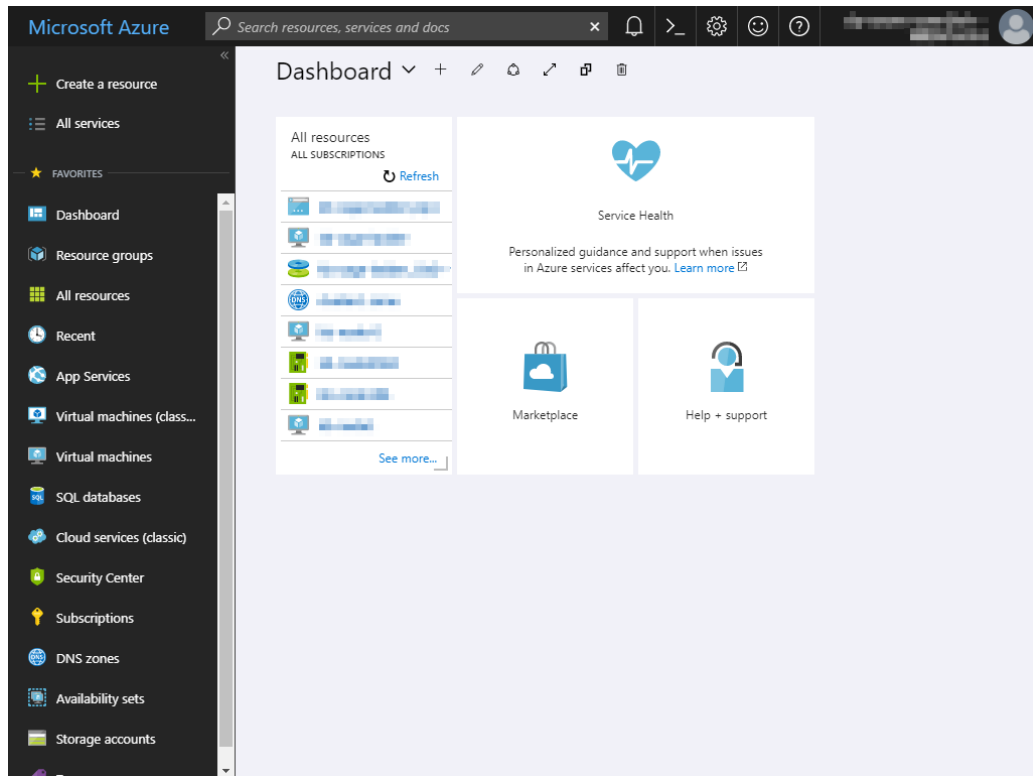
7) Configuring a load balancer

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

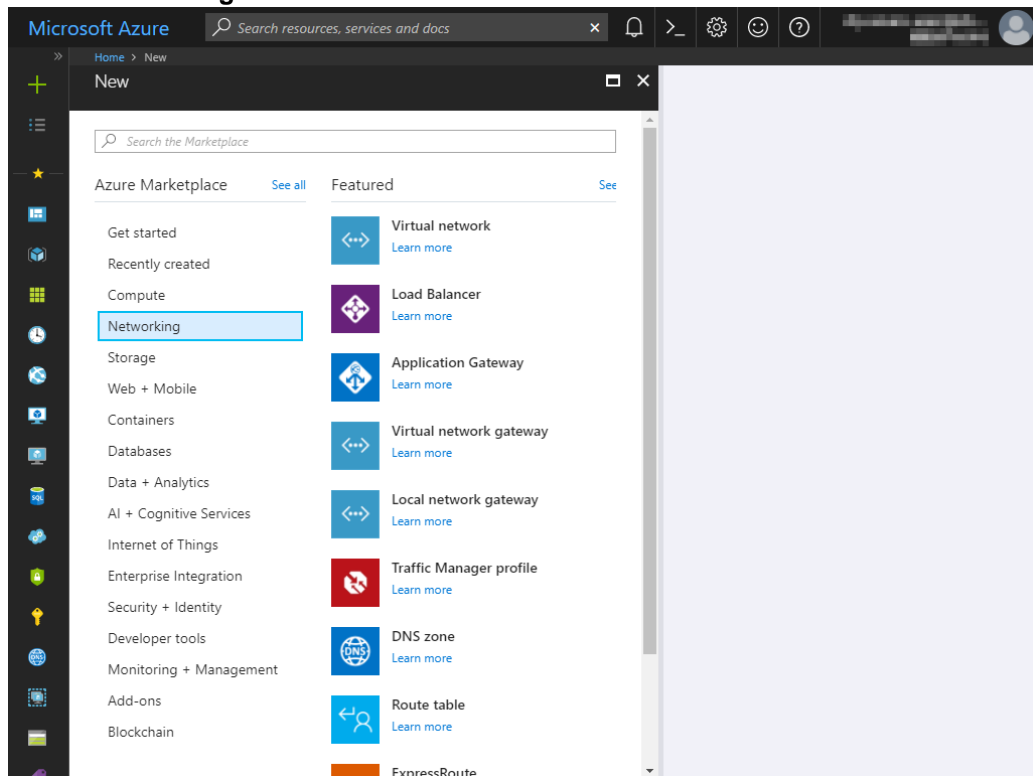
For details, see the following websites:

- Azure Load Balancer overview
<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview>
- Create an Internal load balancer in the Azure portal:
<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-get-started-ilb-arm-portal>

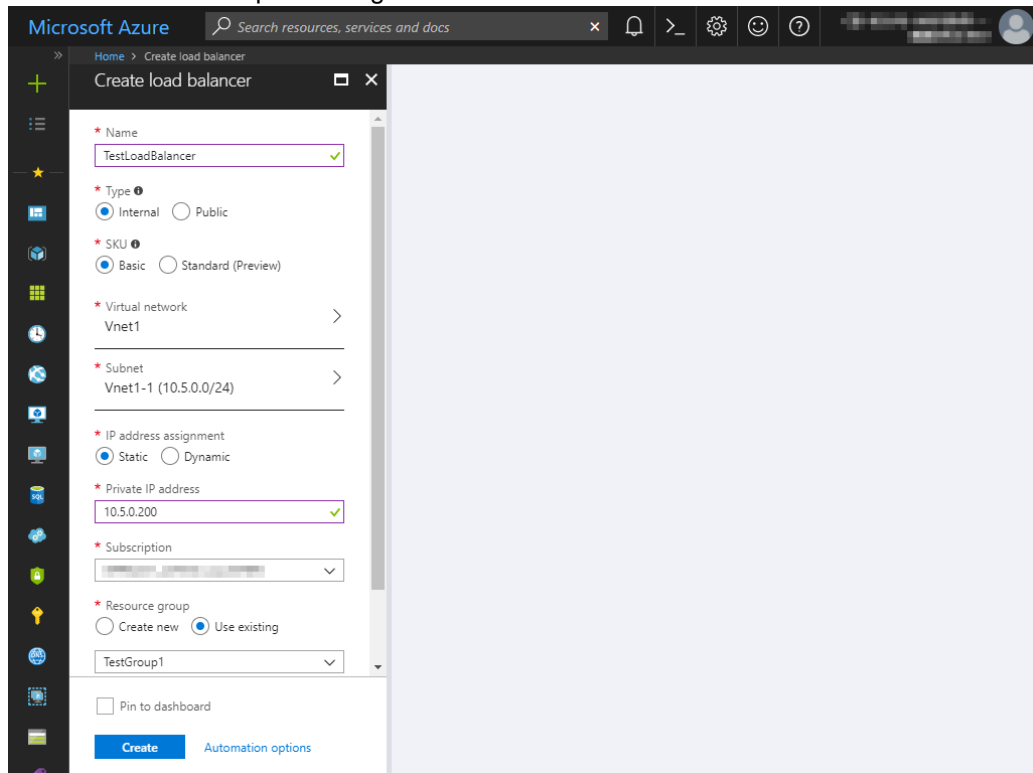
1. Select **+Create a resource** or the **+** icon in the menu on the left side of the window.



2. Select **Networking** and then **Load balancer**.

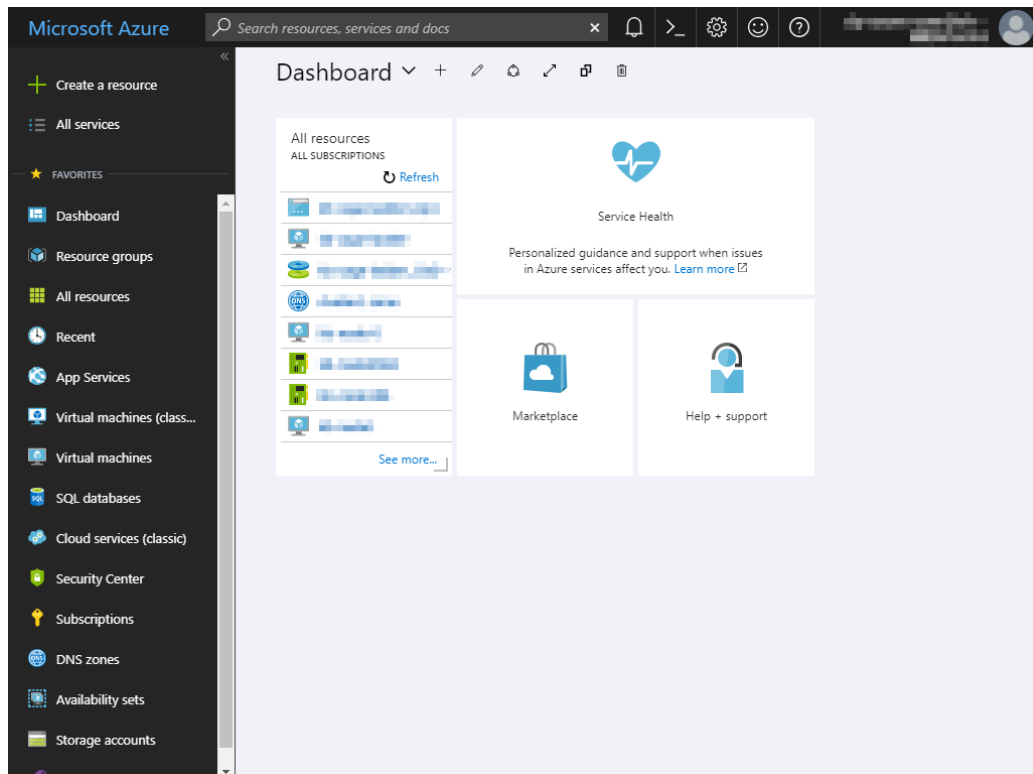


3. The **Create load balancer** blade is displayed. Specify **Name**.
4. Select **Internal** for **Type**.
5. For **Virtual network** and **Subnet**, select the virtual network and subnet created in "2) Creating a virtual network."
6. Specify **Subscription**, **Resource group**, and **Location**, and click **Create**. Deploying the load balancer starts. This processing takes several minutes.

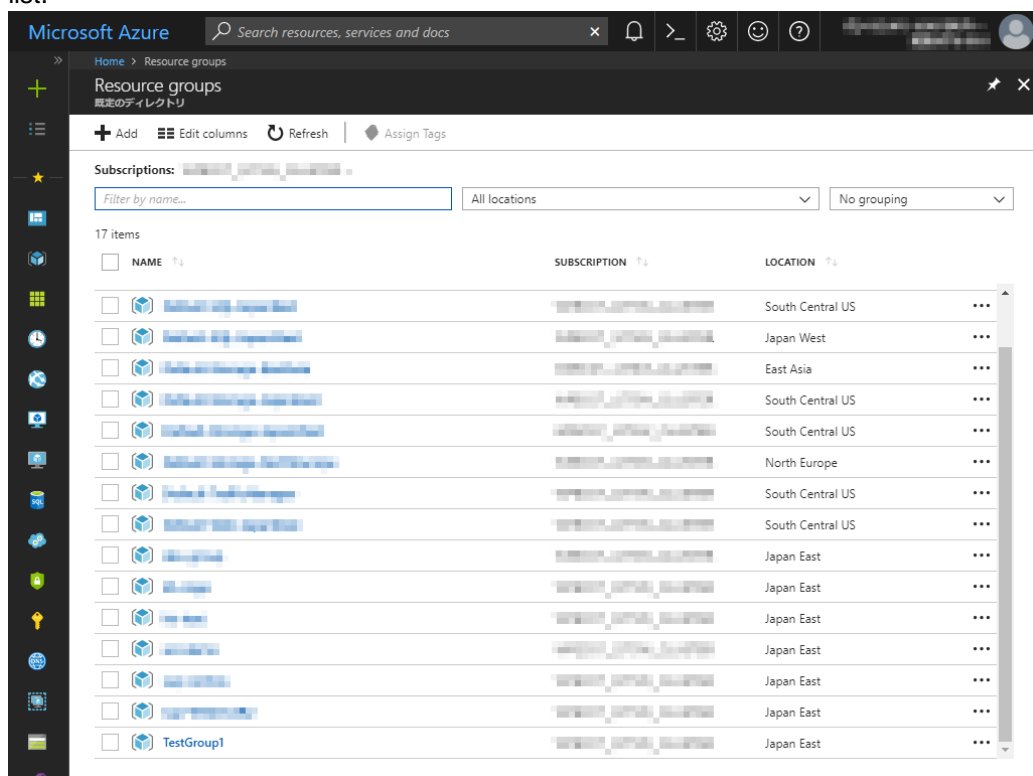


8) Configuring a load balancer (configuring a backend pool)

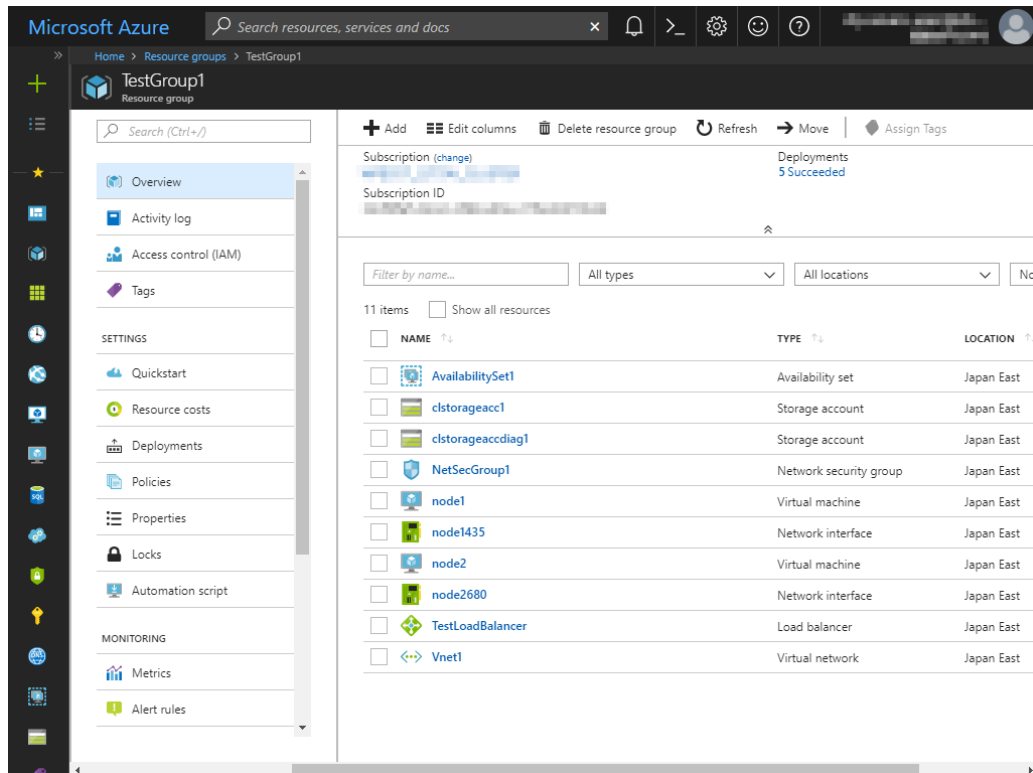
1. Associate a virtual machine registered to the availability set to the load balancer. After the load balancer has been deployed, select **Resource groups** or the resource group icon in the menu on the left side of the window.



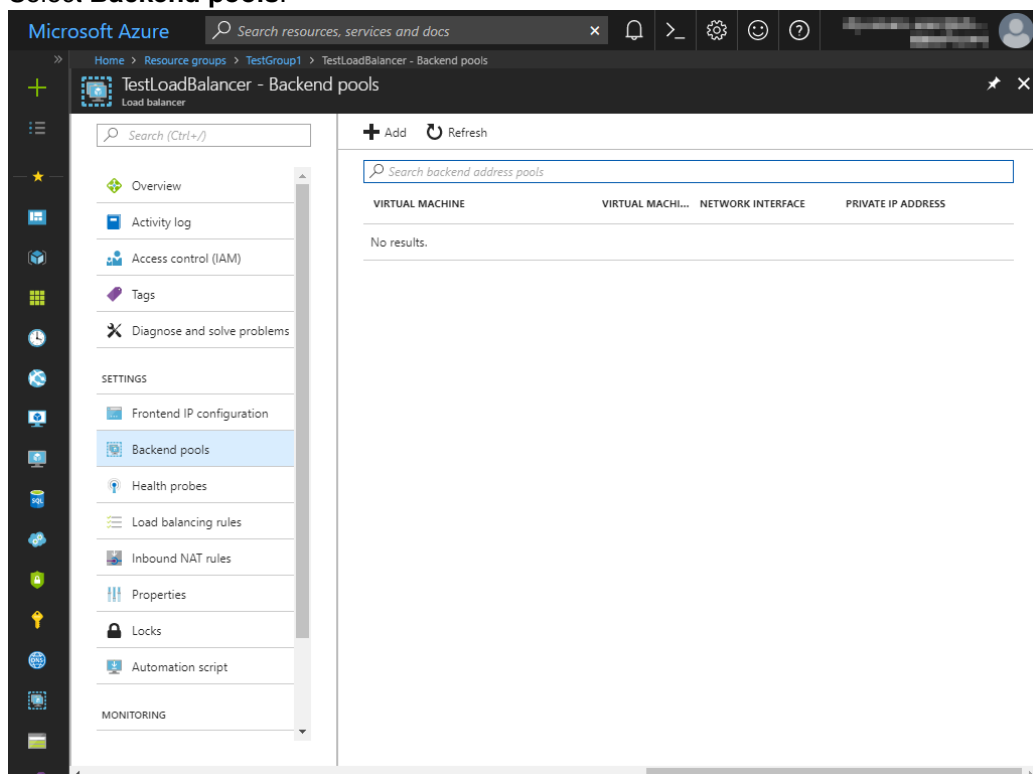
2. Select the resource group to which the created load balancer belongs from the resource group list.



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



4. Select **Backend pools**.



5. Click **Add**.
6. The **Add backend pool** blade is displayed. Specify **Name**.
7. For **Associated to**, select **Availability set**.
8. Specify **Availability set**.
9. Click **Add a target network IP configuration**.
10. Specify the target virtual machine for **Target virtual machine** and **Network IP configuration**.

11. Repeat steps 9 and 10 as many times as the number of target virtual machines.
12. Click **OK**.

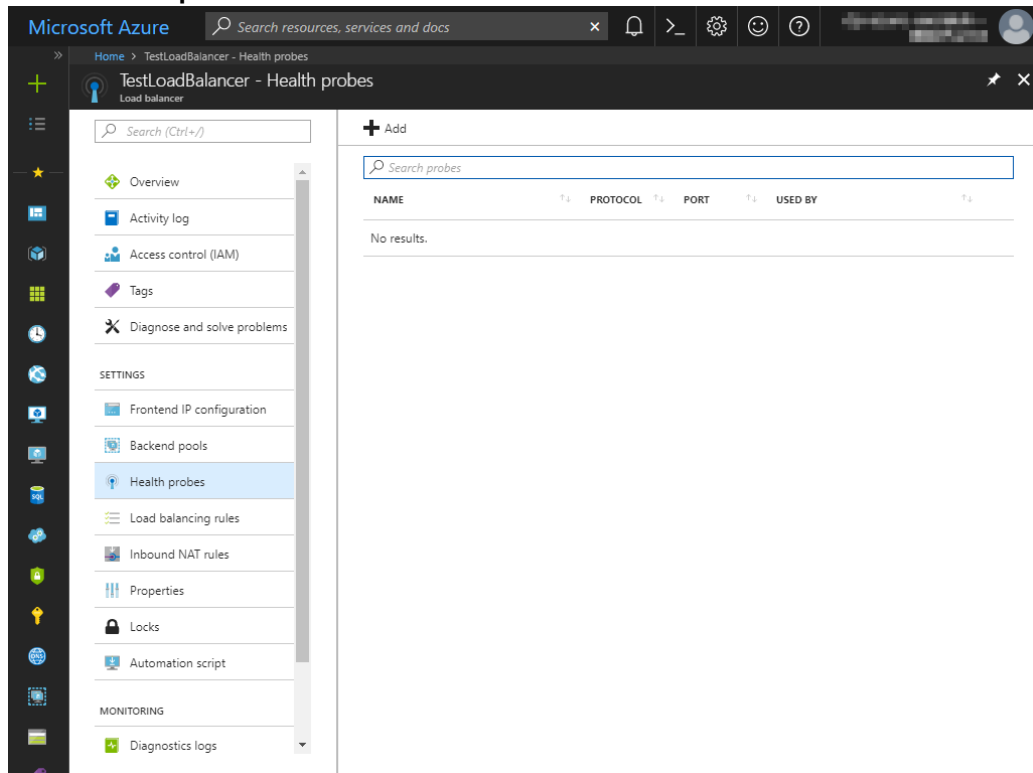
The screenshot shows the 'Add backend pool' configuration window in the Microsoft Azure portal. The breadcrumb navigation at the top indicates the path: Home > Resource groups > TestGroup1 > TestLoadBalancer - Backend pools > Add backend pool. The window title is 'Add backend pool' for 'TestLoadBalancer'.

The configuration fields are as follows:

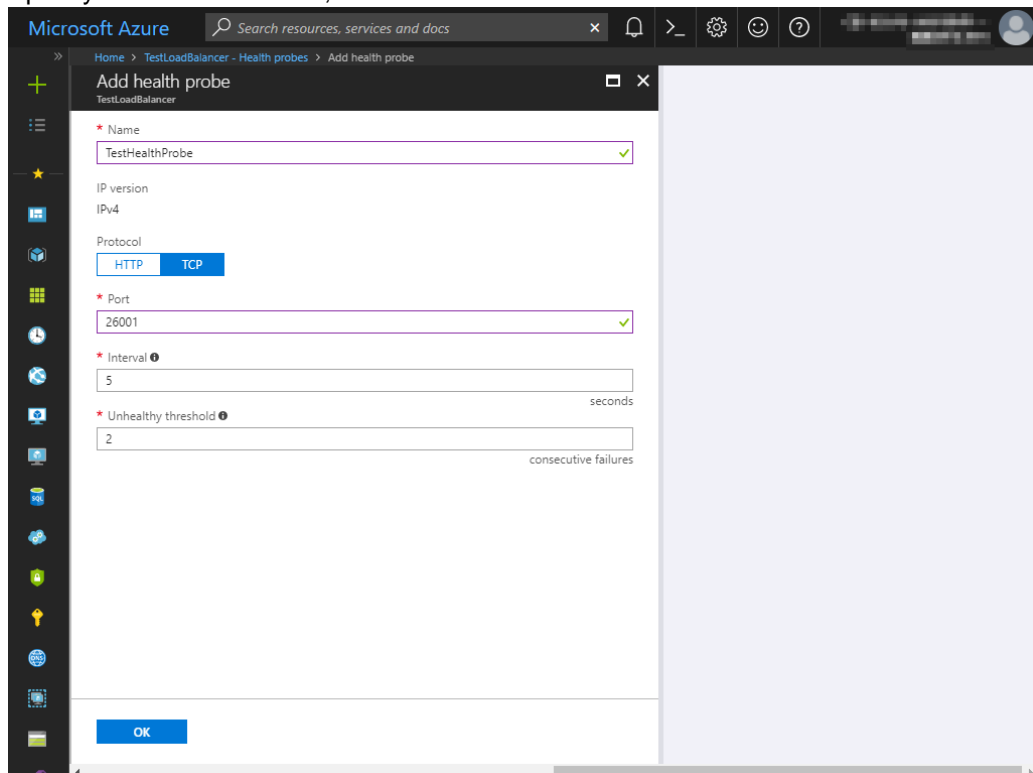
- Name:** TestBackendPool (with a green checkmark icon).
- IP version:** IPv4 (selected) and IPv6 (available).
- Associated to:** Availability set (dropdown menu).
- Availability set:** AvailabilitySet1 (dropdown menu) with a note 'number of virtual machines: 2'.
- Target network IP configurations:** A section with a warning icon and text: 'Only VMs within the current availability set can be chosen. Once a VM is chosen, you can select a network IP configuration related to it.'
- Virtual machine:** node1 (with a trash icon).
Network IP configuration: node1435/ipconfig1 (10.5.0.110) (with a trash icon).
- Target virtual machine:** node2 (dropdown menu) with a note 'size: Standard_A1, network interfaces: 1'.
- Network IP configuration:** ipconfig1 (10.5.0.111) (dropdown menu).
- Buttons:** '+ Add a target network IP configuration' (blue link) and 'OK' (blue button).

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

1. Select **Health probes**.

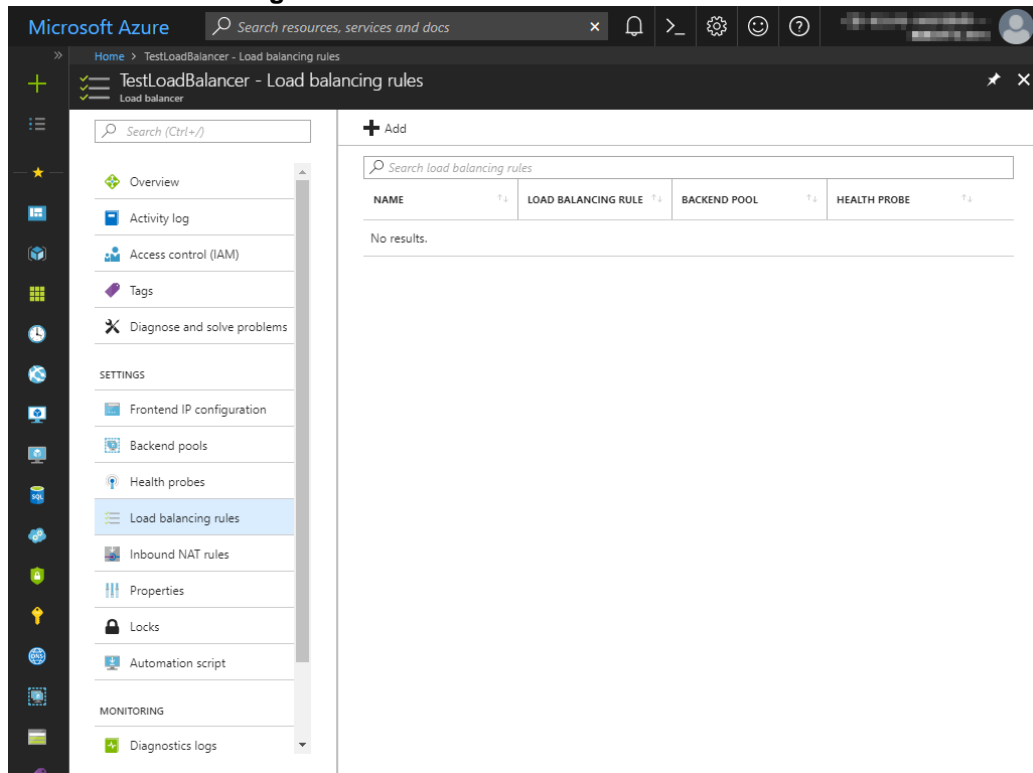


2. Click **Add**.
3. The **Add health probe** blade is displayed. Specify **Name**.
4. Specify **Protocol** and **Port**, and click **OK**.

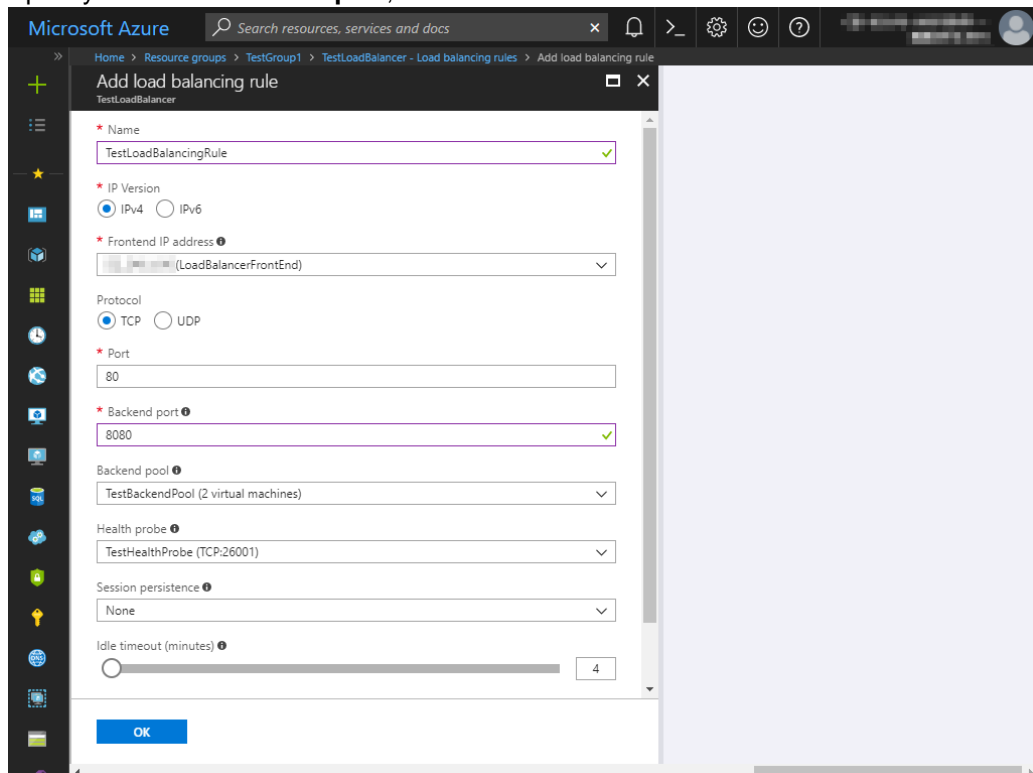


10) Configuring a load balancer (setting the load balancing rules)

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**.



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 Chapter 1, “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

Configure the following on the WebManager cluster generation wizard.

For the WebManager setup and connection procedures, see Chapter 5, "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

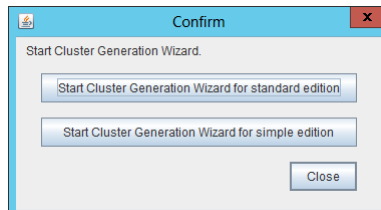
Start the cluster generation wizard to create a cluster.

◆ Creating a cluster

1. Access WebManager. Then, the following dialog box is displayed.
Click **Start cluster generation wizard**.



2. The following dialog box is displayed.
Click **Start Cluster Generation Wizard for standard edition**.



3. The **Cluster Definition** page is displayed.
Enter a desired name in **Cluster Name**.
Select an appropriate language in **Language**. After the setting is applied, the display language of WebManager is changed to the selected language.

The screenshot shows the 'Cluster Definition' page of the 'Cluster Generation Wizard'. On the left, a 'Steps' sidebar lists 'Cluster', 'Server', 'Basic Settings', 'Interconnect', 'NP Resolution', 'Group', and 'Monitor'. The 'Cluster' step is selected. The main area contains the following fields:

- Cluster Name:** A text box containing 'Cluster1'.
- Comment:** An empty text box.
- Language:** A dropdown menu showing 'English'.
- Management IP Address:** An empty text box.

Below these fields is a 'Description' section with the following text:

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

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

4. The **Server Definition** page is displayed.
The instance connected to WebManager is displayed as a registered master server.
Click **Add** to add the remaining instances (by specifying the private IP address of each instance).

The screenshot shows the 'Server Definition' page of the 'Cluster Generation Wizard'. On the left, the 'Steps' sidebar is the same as in the previous screenshot, but 'Server' is now selected. The main area contains the following elements:

- Server Definition List:** A table with two columns: 'Order' and 'Name'.

Order	Name
Master Server	node1
1	node2
- Buttons:** 'Add' and 'Remove' buttons are located to the right of the table. 'Up' and 'Down' buttons are located below the table.
- Server Group:** A section with a 'Server Group Definition' text box and a 'Settings' button.
- Description:** A section with the following text:

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

At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

5. Click **Next**.

6. The **Interconnect** page 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.

Cluster Generation Wizard

Steps

- Cluster
- Server
- Basic Settings
- Interconnect
- NP Resolution
- Group
- Monitor

Interconnect

Priority	Type	MDC	node1	node2
1	Kernel Mode	mdc1	10.5.0.110	10.5.0.111

Buttons: Add, Remove, Properties, Up, Down

Description

Configure the interconnect among the servers constructing the cluster. Click "Add" to add interconnect and select the type. For "Kernel mode", "User mode", "BMC", "DISK" and "COM" settings, configure the route which is used for heartbeat. For "Mirror Communication Only" setting, configure the route which is used only for data mirroring communication. Configuring more than one routes is recommended. Click "Up" or "Down" to configure the priority. For "Mirror Communication Only" settings, click each server column cell to configure IP addresses. For the communication route which is used for data mirroring communication, select the mirror disk connect name to be allocated to the communication route in MDC column.

Buttons: < Back, Next >, Cancel

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

Cluster Generation Wizard

Steps

- Cluster
- Server
- Basic Settings
- Interconnect
- NP Resolution
- Group
- Monitor

NP Resolution

Type	Ping Target	node1	node2
Ping	10.5.0.5	Use	Use

Buttons: Add, Remove, Properties, Tuning

Description

Configure network partition (NP) resolution function. In case Ping method NP resolution, click "Add" to add Ping NP resolution resource and click Ping target column cell to configure IP address of Ping destination. Click each server column cell to configure "Use" or "Do not use". The detailed settings can be verified and changed by clicking "Properties". Click "Tuning" to configure the actions at NP occurrence.

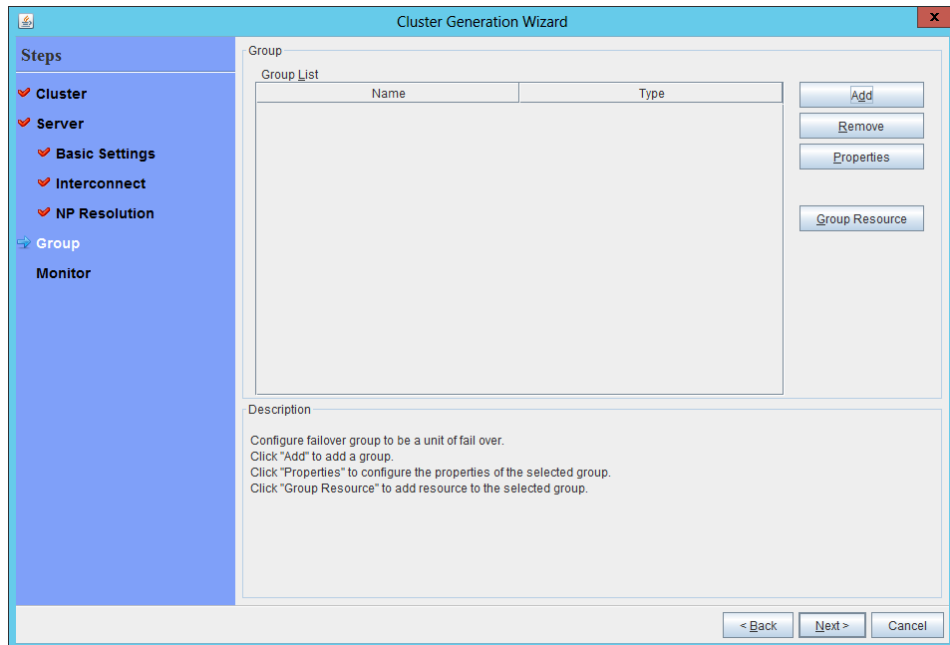
Buttons: < Back, Next >, Cancel

9. Click **Next**.

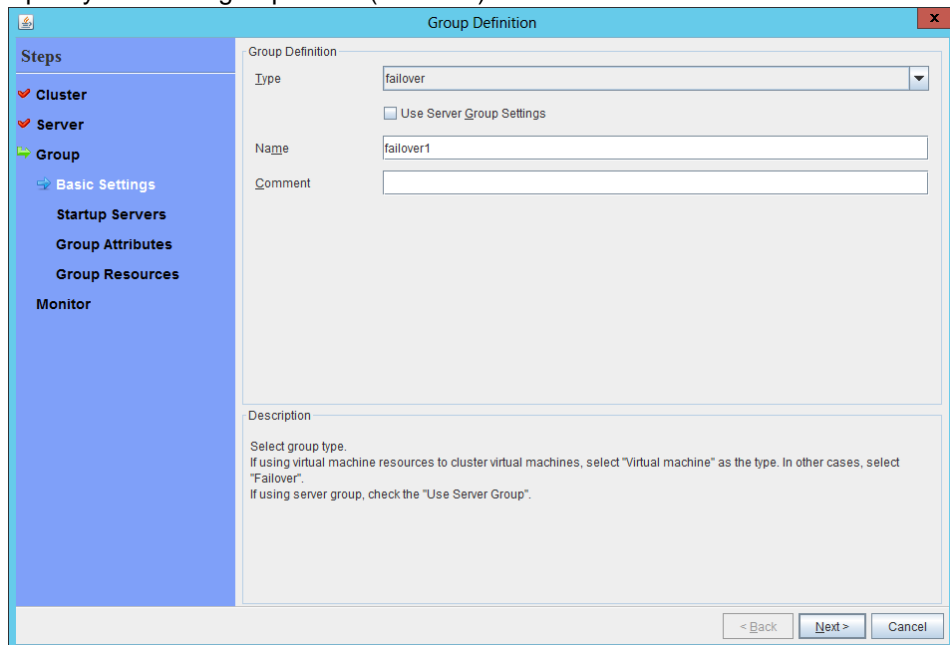
2) Adding a group resource

- ◆ 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**.



3. Click **Next**.

4. The **Servers that can run the Group** page is displayed.
Click **Next** without specifying anything.

The screenshot shows the 'Group Definition(failover1)' dialog box. On the left is a 'Steps' sidebar with options: Cluster, Server, Group (selected), Basic Settings, Startup Servers, Group Attributes, Group Resources, and Monitor. The main area is titled 'Servers that can run the Group'. It contains a checkbox 'Failover is possible on all servers' which is checked. Below this is a list 'Servers that can run the Group' which is currently empty. To the right is a list 'Available Servers' containing 'node1' and 'node2'. Between these lists are buttons: '< Add', 'Remove >', 'Up', and 'Down'. At the bottom of the main area is a 'Description' section with text explaining server selection and priority. At the very bottom of the dialog are buttons: '< Back', 'Next >', and 'Cancel'.

5. The **Group Attribute Settings** page is displayed.
Click **Next** without specifying anything.

The screenshot shows the 'Group Definition(failover1)' dialog box, now on the 'Group Attribute Settings' page. The 'Steps' sidebar remains the same, with 'Group' still selected. The main area contains settings for 'Startup Attribute' (radio buttons for 'Auto Startup' and 'Manual Startup'), 'Failover Attribute' (radio buttons for 'Auto Failover' and 'Manual Failover'), and 'Failback Attribute' (radio buttons for 'Auto Failback' and 'Manual Failback'). Under 'Auto Failover', there are checkboxes for 'Use the startup server settings', 'Failover dynamically', 'Perform a Forced Failover', 'Prioritize failover policy in the server group', and 'Perform a Smart Failover'. There is also a checkbox for 'Prioritize failover policy in the server group' and a checkbox for 'Enable only manual failover among the server groups'. An 'Edit exclusion monitor' button is visible. A 'Description' section at the bottom provides instructions on configuring failover. At the bottom of the dialog are buttons: '< Back', 'Next >', and 'Cancel'.

6. The **Group Resource** page is displayed.
On this page, add a group resource following the procedure below.

The screenshot shows a window titled "Group Definition(failover1)" with a close button (X) in the top right corner. The window is divided into two main sections. On the left is a blue sidebar labeled "Steps" containing a list of steps: "Cluster", "Server", "Group" (which is highlighted with a green arrow), "Basic Settings", "Startup Servers", "Group Attributes", "Group Resources", and "Monitor". The main area on the right is titled "Group Resource" and contains a "Group Resource List" table. The table has two columns: "Name" and "Type". To the right of the table are three buttons: "Add", "Remove", and "Properties". Below the table is a "Description" section with the text: "Click 'Add' to add resources." and "Click 'Properties' to configure the properties of the selected resource." At the bottom of the window are three buttons: "< Back", "Finish", and "Cancel".

Name	Type
------	------

Buttons: Add, Remove, Properties

Description:

Click "Add" to add resources.
Click "Properties" to configure the properties of the selected resource.

Buttons: < Back, Finish, Cancel

- ◆ Mirror disk resource
Create a mirror disk resource.
For details, see “Understanding mirror disk resources” in Chapter 4, “Group resource details” in the *Reference Guide*.

1. Click **Add** on the **Group Resource List** page.
2. The **Resource Definition of Group** 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.

Resource Definition of Group(failover1)

Group Resource Definitions

Type: mirror disk resource

Name: md

Comment:

Get Licence Info

Description: Select the type of group resource and enter its name.

< Back Next > Cancel

3. Click **Next**.
4. The **Dependent Resources** page is displayed.
Click **Next** without specifying anything.

Resource Definition of Group(failover1)

☒ Follow the default dependency

Name	Resource type
---	AWS Elastic I...
---	AWS virtual ip ...
---	Azure probe p...
---	floating ip res...
---	virtual ip reso...

< Add Remove >

Available Resources

< Back Next > Cancel

5. The **Recovery Operation at Activation Failure Detection** and **Recovery Operation at Deactivation Failure Detection** page is displayed.
Click **Next**.

6. The **Details Settings** page 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.

◆ 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 Chapter 4, "Group resource details" in the *Reference Guide*.

1. Click **Add** on the **Group Resource List** page.
2. The **Resource Definition of Group** 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.

Resource Definition of Group(failover1)

Group Resource Definitions

Type: Azure probe port resource

Name: azurepp1

Comment:

Get Licence Info

Description:

Select the type of group resource and enter its name.

< Back Next > Cancel

3. Click **Next**.
4. The **Dependent Resources** page is displayed. Click **Next** without specifying anything.

Resource Definition of Group(failover1)

☒ Follow the default dependency

Dependent Resources

Name	Resource type
------	---------------

< Add Remove >

Available Resources

Name

< Back Next > Cancel

5. The **Recovery Operation at Activation Failure Detection** and **Recovery Operation at Deactivation Failure Detection** page displayed. Click **Next**.

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

7. 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 Chapter 4, "Group resource details" in the *Reference Guide*.

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

- ◆ Azure load balance monitor resource

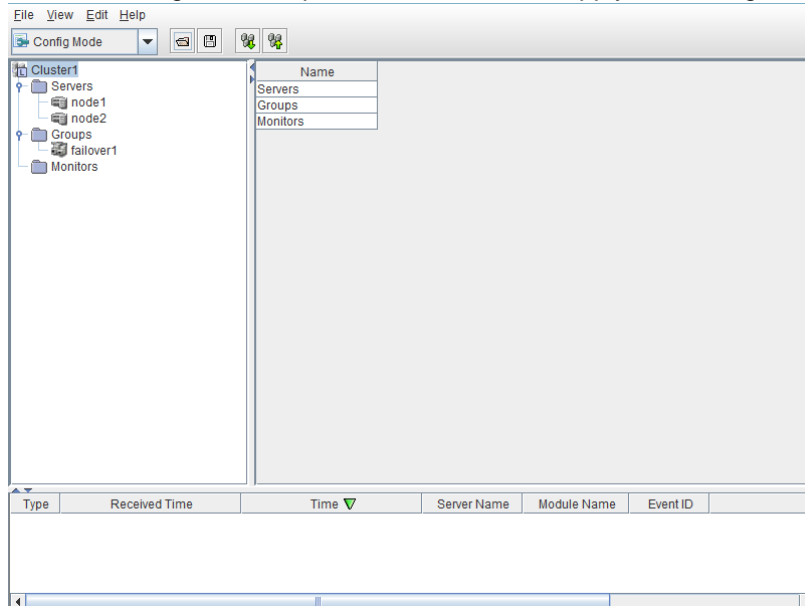
The mechanism to monitor whether the port with the same port number as the probe port is open or not is provided for the node in which the Microsoft Azure probe port resource is not running.

For details about the Azure load balance resource, see "Understanding Azure load balance monitor resources" in Chapter 5 "Monitor resource details" in the *Reference Guide*.

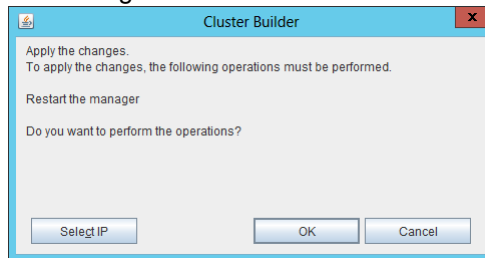
Adding one Azure probe port resource creates one Azure load balance monitor resource automatically.

4) Applying the settings and starting the cluster

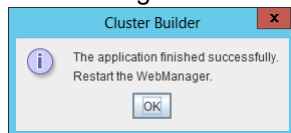
1. After all settings are complete, click the icon to apply the settings under the menu.



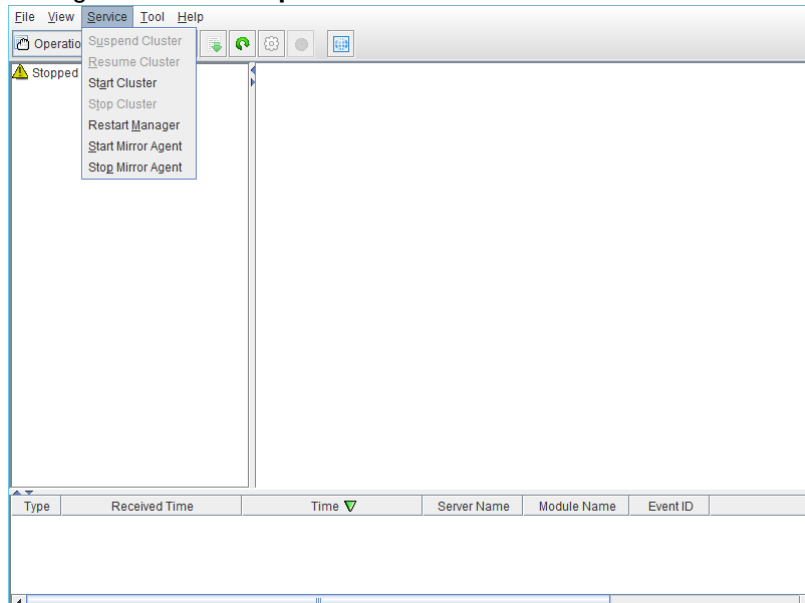
2. The dialog box to confirm to restart the manager is displayed.



3. Click **OK**.
4. Click **OK** again on the following dialog box.



5. Change the mode to **Operation Mode** and click **Start Cluster** from the **Service** menu.



5.4 Verifying the created environment

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

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

1. Start the failover group (failover1) on the active node (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 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.

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

Chapter 6 Error Messages

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

- Chapter 12, “Error messages” in the *Reference Guide*.

Chapter 7 Notes and Restrictions

7.1 HA cluster using Azure DNS

7.1.1 Notes on Microsoft Azure

- There is a tendency for the performance difference (performance deterioration rate) to increase in a multi-tenant cloud environment compared to a physical environment or general virtualization environment (non-cloud environment). Therefore, pay careful attention to this point when designing a performance-oriented system.
- Even if a virtual machine is just shut down, its status is **Stopped** and billing continues. Execute **Stop** on the virtual machine setting window of the Microsoft Azure portal to change the virtual machine state to **Stopped (Deallocated)**.
- An availability set can be set only when creating a virtual machine. To move a virtual machine to and from the availability set, it is necessary to create an availability set again.
- To set up EXPRESSCLUSTER to work with Microsoft Azure, a Microsoft Azure organizational account is required. An account other than the organizational account cannot be used because an interactive login is required when executing the Azure CLI.

7.1.2 Notes on EXPRESSCLUSTER

Please refer the following for notes for EXPRESSCLUSTER on Azure:

EXPRESSCLUSTER X Getting Started Guide

- "Communication port number" in Chapter 5, "Notes and Restrictions"
- "Azure DNS resources" in Chapter 5, "Notes and Restrictions"
- "Setting up Azure DNS resources" in Chapter 5, "Notes and Restrictions"

EXPRESSCLUSTER X Reference Guide

- "Notes on Azure DNS resources" in Chapter 4, "Group resource details"
- "Notes on Azure DNS monitor resources" in Chapter 5, "Monitor resource details"

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 Chapter 5, "Notes and Restrictions"

EXPRESSCLUSTER X Reference Guide

- "Timeout tab" in Chapter 2, "Functions of the Builder"
- "Monitor tab" in Chapter 2, "Functions of the Builder"

7.2 HA cluster using a load balancer

7.2.1 Notes on Microsoft Azure

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

7.2.2 Notes on EXPRESSCLUSTER

Please refer the following for notes for EXPRESSCLUSTER on Azure:

EXPRESSCLUSTER X Getting Started Guide

- "Communication port number" in Chapter 5, "Notes and Restrictions"
- "Azure probe port resources" in Chapter 5, "Notes and Restrictions"
- "Setting up Azure probe port resources" in Chapter 5, "Notes and Restrictions"
- "Setting up Azure load balance monitor resources" in Chapter 5, "Notes and Restrictions"

EXPRESSCLUSTER X Reference Guide

- "Notes on Azure probe port resources" in Chapter 4, "Group resource details"
- "Notes on Azure probe port monitor resources" in Chapter 5, "Monitor resource details"
- "Note on Azure load balance monitor resources" in Chapter 5, "Monitor resource details"

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 Chapter 5, "Notes and Restrictions"

EXPRESSCLUSTER X Reference Guide

- "Timeout tab" in Chapter 2, "Functions of the Builder"
- "Monitor tab" in Chapter 2, "Functions of the Builder"