

# **EXPRESSCLUSTER® X 4.1**

## HA Cluster Configuration Guide for Microsoft Azure (Windows)

April 10, 2019  
1st Edition



## Revision History

Edition	Revised Date	Description
1st	Apr 10, 2019	New guide

© Copyright NEC Corporation 2019. 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.

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

<b>Preface</b>	<b>v</b>
<b>Chapter 1 Overview</b>	<b>9</b>
1.1 Functional overview	9
1.2 Basic configuration	10
1.3 Network partition resolution	16
1.4 Differences between on-premises and Microsoft Azure	18
<b>Chapter 2 Operating Environments</b>	<b>23</b>
2.1 HA cluster using Azure DNS	23
2.2 HA cluster using a load balancer	23
<b>Chapter 3 Cluster Creation Procedure (for an HA Cluster Using Azure DNS)</b>	<b>24</b>
3.1 Creation example	24
3.2 Configuring Microsoft Azure	27
3.3 Configuring the EXPRESSCLUSTER settings	49
3.4 Verifying the created environment	66
<b>Chapter 4 Cluster Creation Procedure (for an HA Cluster Using an Public Load Balancer)</b>	<b>67</b>
4.1 Creation example	67
4.2 Configuring Microsoft Azure	70
4.3 Configuring the EXPRESSCLUSTER settings	98
4.4 Verifying the created environment	117
<b>Chapter 5 Cluster Creation Procedure (for an HA Cluster Using an Internal Load Balancer)</b>	<b>118</b>
5.1 Creation example	118
5.2 Configuring Microsoft Azure	120
5.3 Configuring the EXPRESSCLUSTER settings	145
5.4 Verifying the created environment	154
<b>Chapter 6 Error Messages</b>	<b>155</b>
<b>Chapter 7 Notes and Restrictions</b>	<b>156</b>
7.1 HA cluster using Azure DNS	156
7.1.1 Notes on Microsoft Azure	156
7.1.2 Notes on EXPRESSCLUSTER	156
7.2 HA cluster using a load balancer	157
7.2.1 Notes on Microsoft Azure	157
7.2.2 Notes on EXPRESSCLUSTER	157



# Preface

## Who Should Use This Guide

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

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

## Scope of application

This guide covers the following product versions.

- EXPRESSCLUSTER X 4.1 for Windows (Internal version: 12.10)
- Windows Server 2016 Datacenter
- Microsoft Azure portal: Environment as of January 16, 2019
- Azure CLI 2.0

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

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

## 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 public 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 X manuals consist of the following six guides. The title and purpose of each guide is described below:

## **Getting Started Guide**

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

## **Installation and Configuration Guide**

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

## **Reference Guide**

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

## **Maintenance Guide**

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

## **Hardware Feature Guide**

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

## **Legacy Feature Guide**

This guide is intended for administrators and for system engineers who want to build EXPRESSCLUSTER-based cluster systems. The guide describes EXPRESSCLUSTER X 4.0 WebManager, Builder, and EXPRESSCLUSTER Ver 8.0 compatible commands.

## 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
<b>Bold</b>	Indicates graphical objects, such as text boxes, list boxes, menu selections, buttons, labels, icons, etc.	Click <b>Start</b> . <b>Properties</b> 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 Windows user has logged on as root user.	<code>&gt; clpstat</code>
Monospace (Courier)	Indicates path names, commands, system output (message, prompt, etc.), directory, file names, functions and parameters.	<code>C:\Program Files</code>
<b>Monospace bold</b> (Courier)	Indicates the value that a user actually enters from a command line.	Enter the following: <code>&gt; 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>&gt; ping &lt;IP address&gt;</code>

## **Contacting NEC**

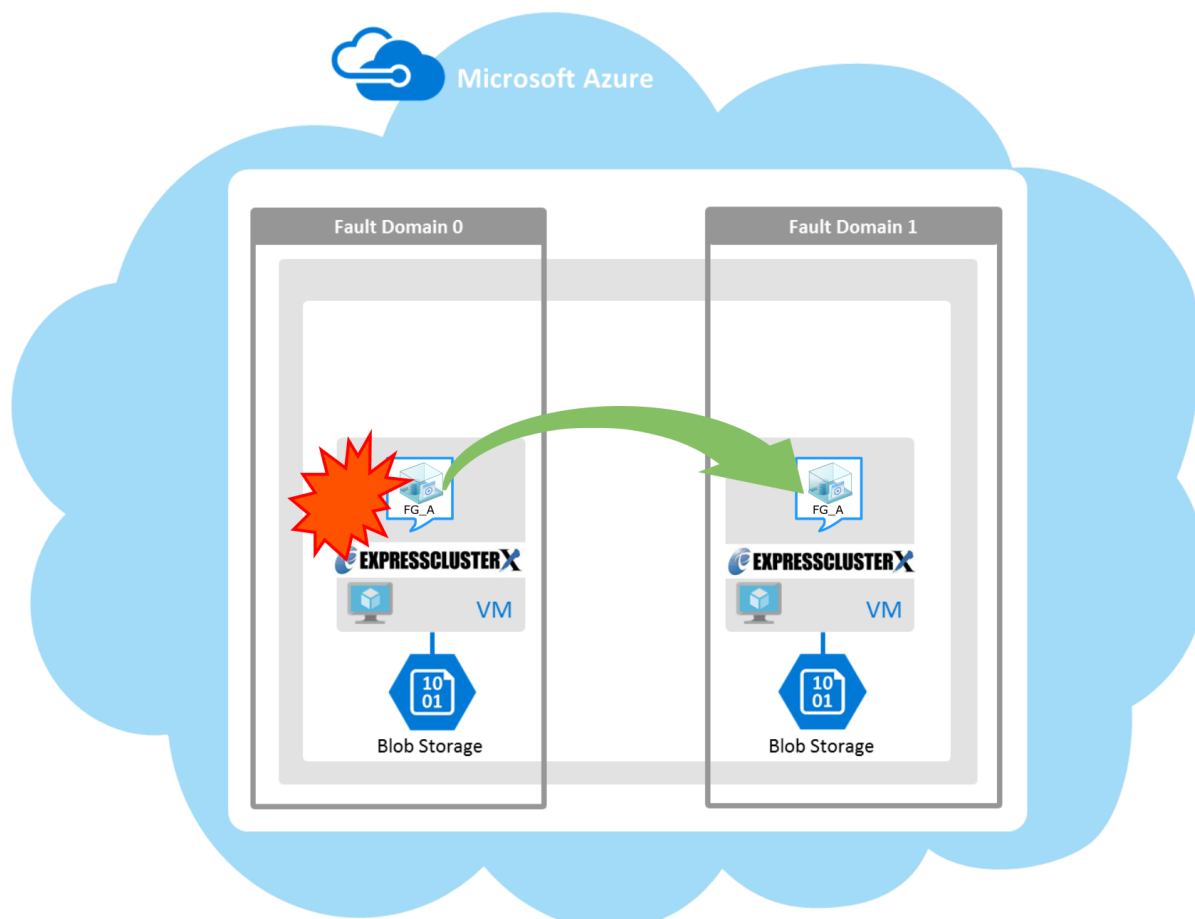
For the latest product information, visit our website below:

<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 Windows virtual machines in Azure:  
<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/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.

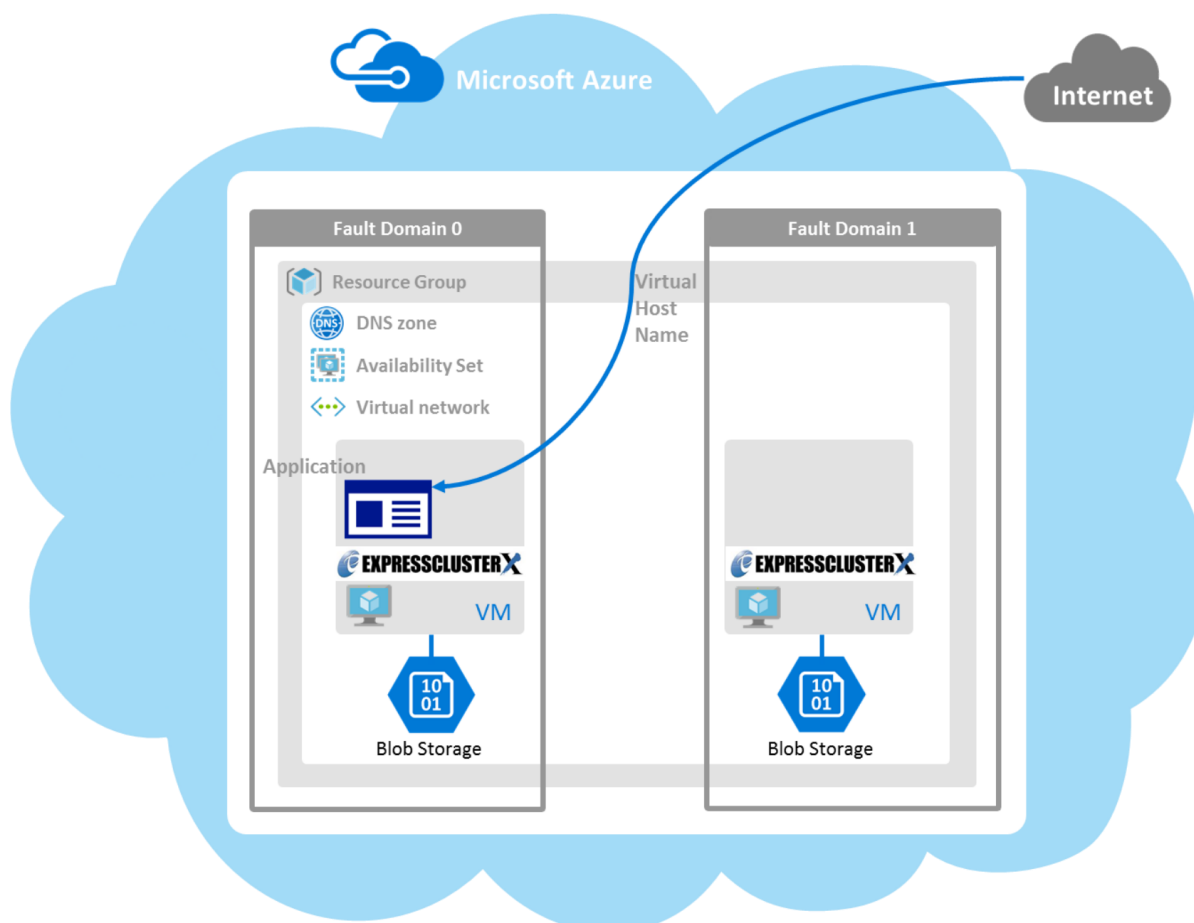
Purpose	EXPRESSCLUSTER resource to use
Accessing the cluster by using a DNS name (Use Azure DNS recordset)	Azure DNS resource
Accessing the cluster by using a virtual IP address(global IP address) (Use public load balancer)	Azure probe port resource
Accessing the cluster by using a virtual (private) IP address (Use internal load balancer)	Azure probe port resource
Accessing the cluster by using a virtual (private) IP address, with the clustered application configured as Always On (Use internal load balancer and configure Direct Server Return, hereinafter called "DSR")	Azure probe port resource

Refer to the following when creating a DSR configuration.  
<https://jpn.nec.com/clusterpro/blog/20181031.html> (Japanese only)

## 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.

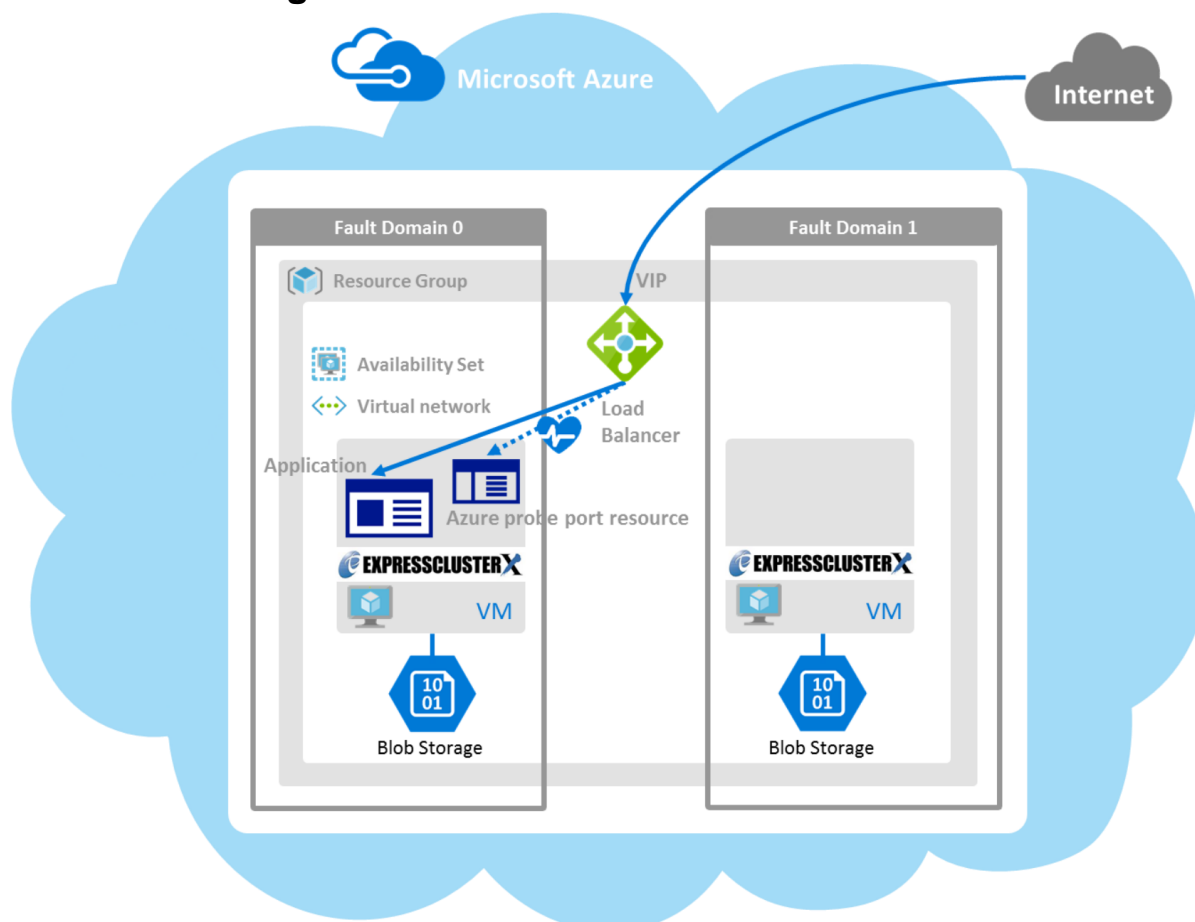
The cluster in Figure 1-2 is accessed by using the DNS name of the Azure DNS zone. EXPRESSCLUSTER manages record sets and DNS A records of the Azure DNS zone to find an IP address according to the DNS name. A client need not be conscious about the switching of virtual machines upon failover occurrence 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 the record sets (A records) of the Azure DNS zone to find an IP address according to the DNS name.	Required
Azure DNS monitor resource	Monitors that the results of name resolution are normal in relation to the Azure DNS record set.	Required
IP monitor resource	Monitors whether communication with the Microsoft Azure Service Management API is possible, and also monitors health of communication with an external network.	When an public load balancer is used, required to monitor communication between clusters that are configured with virtual machines, and also to monitor health of communication with an internal network.
Custom monitor resource	Monitors communication between clusters that are configured with virtual machines, and also monitors health of communication with an internal network.	When an public load balancer is used, required to monitor whether communication with the Microsoft Azure Service Management API is possible, and also to monitor health of communication with an external network.
Multi target monitor resource	Monitors the statuses of both the IP monitor resource and custom monitor resource. If the statuses of both monitor resources are abnormal, a script in which a process for network partition resolution (NP resolution) is described is executed.	When an public load balancer is used, required to monitor health of communication between an internal network and external network.
Other resources and monitor resources	Depends on the configuration of application, such as a mirror disk, that is used in an HA cluster.	Optional



## HA cluster using a load balancer



**Figure 1-3 HA Cluster Using an Public Load Balancer**

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

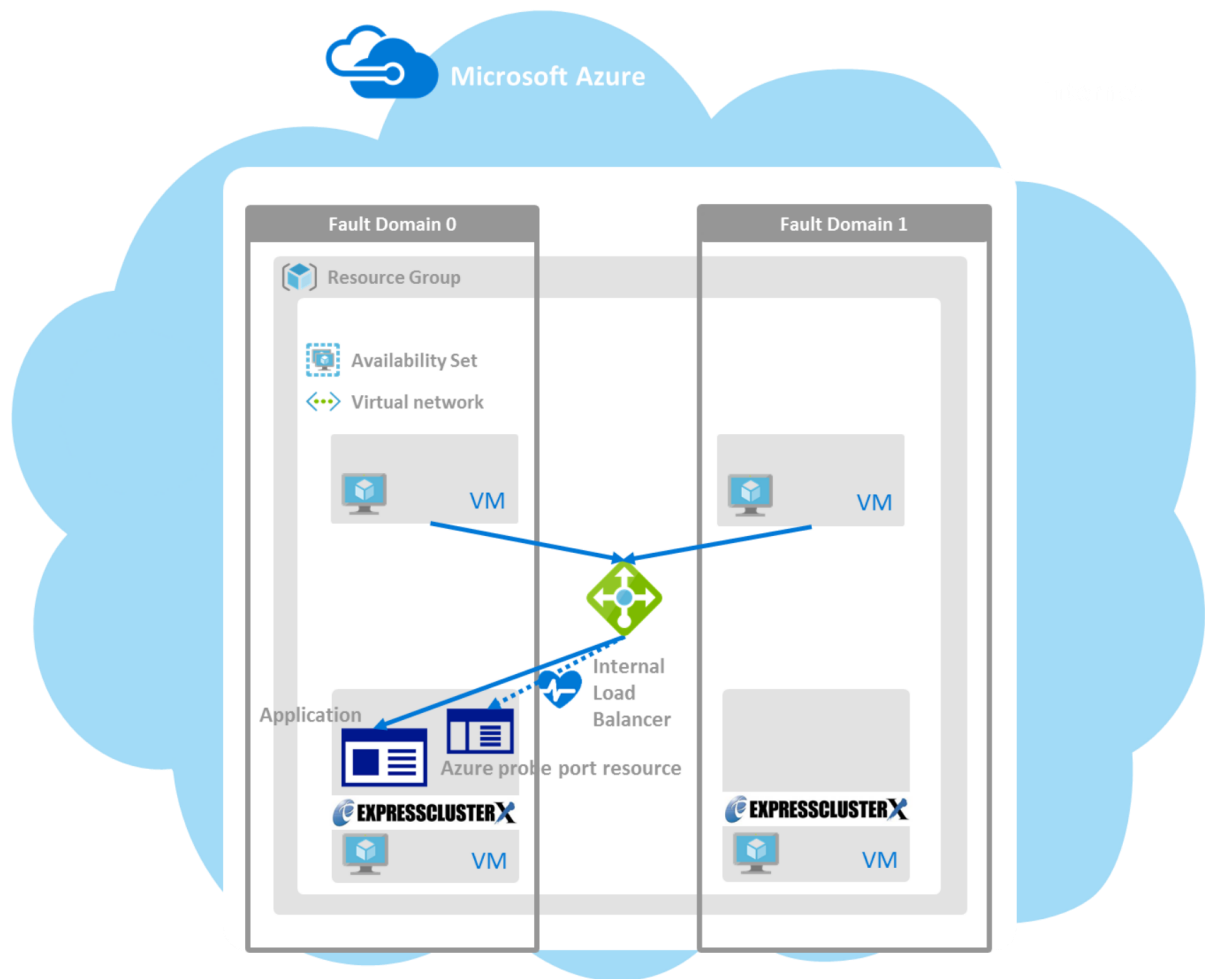
A cluster built in a Microsoft Azure environment in Figure 1-3 is accessed by specifying a global IP address of the Microsoft Azure Load Balancer (Load Balancer in Figure 1-3).

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	Public load balancer	See " Chapter 4 Cluster Creation Procedure (for an HA Cluster Using an Public 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 public load balancer is used, required to monitor communication between clusters that are configured with virtual machines, and also to monitor health of communication with an external network.
Custom monitor resource	Monitors communication between clusters that are configured with virtual machines, and also monitors health of communication with an internal network.	When an public load balancer is used, required to monitor whether communication with the Microsoft Azure Service Management API is possible, and also to monitor health of communication with an external network.
Multi target monitor resource	Monitors the statuses of both the IP monitor resource and custom monitor resource. If the statuses of both monitor resources are abnormal, a script in which a process for network partition resolution (NP resolution) is described is executed.	When an public load balancer is used, required to monitor health of communication between an internal network and external network.
PING network partition resolution resource	When an internal load balancer (ILB) is used, monitors health of communication between subnets by checking whether to communicate with a device that is always on and can return a response to ping (ping device).	When an internal load balancer (ILB) is used, required to monitor health of communication between subnets.
Other resources and monitor resources	Depends on the configuration of application, such as a mirror disk, that is used in an HA cluster.	Optional

## 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 used on Microsoft Azure described in the following table.

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

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

For details about NP resolution, see the following:

- Chapter 5, “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 check the TCP port listening status. Use this command as **Script created with this product** of the custom monitor resource or multi target monitor resource.

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

## Checking the TCP port listening status (clpazure\_port\_checker command)

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

### Command line

`clpazure_port_checker -h hostname -p port`

**Description** This command checks whether a LISTEN port exists among TCP ports of the server specified for an argument.  
If there is no response five seconds (fixed) after the command execution, it is judged that an error (timeout) has occurred.  
In case of an error, an error message is output to the standard output.  
Executing this command from the custom monitor resource makes it possible to judge the network partition status.  
For the configuration example of network partition resolution using this command, see "3.3 Configuring the EXPRESSCLUSTER settings" and "5.3 Configuring the EXPRESSCLUSTER settings"

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

<b>Return values</b>	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 Resource Manager deployment model
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 17 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 the OS or DNS server.	Not required
8	Setting a partition for the mirror disk resource	See the following: <ul style="list-style-type: none"><li>"Settings after configuring hardware" in Chapter 1, "Determining a system configuration" in the <i>Installation and Configuration Guide</i>.</li><li>"Understanding mirror disk resources" in the <i>Reference Guide</i>.</li></ul>	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 firewall setting		
12	Synchronizing the server time		
13	Disabling the power saving function		
14	Installing the Azure CLI	Not required	See "3.2 Configuring Microsoft Azure" in this guide.
15	Registering the service principal	Not required	See "3.2 Configuring Microsoft Azure" in this guide.
16	Installing EXPRESSCLUSTER	See Chapter 3, "Installing EXPRESSCLUSTER." in the <i>Installation and Configuration Guide</i> .	Same as "On-premise"
After installing EXPRESSCLUSTER			
17	Registering the EXPRESSCLUSTER license	See Chapter 4, "Registering the license." in the <i>Installation and Configuration Guide</i> .	Same as "On-premise"
18	Creating a cluster: Setting the heartbeat method	See "Creating the configuration data of a 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.
19	Creating a cluster: Setting the NP resolution processing	The network partition resolution resource is used. See the following: <ul style="list-style-type: none"> <li>"Creating the configuration data of a node cluster" in Chapter 5, "Creating the cluster configuration data".in the <i>Installation and Configuration Guide</i>.</li> <li>Chapter 5, "Network partition resolution resources details" in the <i>Reference Guide</i>.</li> </ul>	See "5.3 Configuring the EXPRESSCLUSTER settings" in this guide.
20	Creating a cluster: Creating a failover group and monitor resource	See "Creating the configuration data of a node cluster" in Chapter 5, "Creating the cluster configuration data".in the <i>Installation and Configuration Guide</i> .	In addition to the references for on-premises, see the following: <ul style="list-style-type: none"> <li>➤ "Understanding Azure DNS resources" in the Reference Guide.</li> <li>➤ "Understanding Azure DNS monitor resources" in the Reference Guide.</li> <li>➤ "3.3 Configuring the EXPRESSCLUSTER settings" in this guide.</li> </ul>

## HA cluster using a load balancer

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

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

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"> <li>• "4.2 Configuring Microsoft Azure" in this guide</li> <li>• "5.2 Configuring Microsoft Azure" in this guide</li> </ul>
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"> <li>• "4.2 Configuring Microsoft Azure" in this guide</li> <li>• "5.2 Configuring Microsoft Azure" in this guide</li> </ul>
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"> <li>• "4.2 Configuring Microsoft Azure" in this guide</li> <li>• "5.2 Configuring Microsoft Azure" in this guide</li> </ul>
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"> <li>• "4.2 Configuring Microsoft Azure" in this guide</li> <li>• "5.2 Configuring Microsoft Azure" in this guide</li> </ul>
5	Adding Blob storage	Not required	See either of the following depending on the load balancer to use: <ul style="list-style-type: none"> <li>• "4.2 Configuring Microsoft Azure" in this guide</li> <li>• "5.2 Configuring Microsoft Azure" in this guide</li> </ul>
6	Setting a partition for the mirror disk resource	See the following: <ul style="list-style-type: none"> <li>• "Settings after configuring hardware" in Chapter 1, "Determining a system configuration" in the <i>Installation and Configuration Guide</i></li> <li>• "Understanding mirror disk resources" in the <i>Reference Guide</i>.</li> </ul>	See either of the following depending on the load balancer to use: <ul style="list-style-type: none"> <li>• "4.2 Configuring Microsoft Azure" in this guide</li> <li>• "5.2 Configuring Microsoft Azure" in this guide</li> </ul>
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"> <li>• "4.2 Configuring Microsoft Azure" in this guide</li> </ul>



Step No.	Procedure	On-premise	Microsoft Azure
			<ul style="list-style-type: none"> <li>• "5.2 Configuring Microsoft Azure" in this guide</li> </ul>
8	Setting the inbound security rules	Not required	<ul style="list-style-type: none"> <li>• "4.2 Configuring Microsoft Azure" in this guide</li> </ul>
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 firewall setting		
12	Synchronizing the server time		
13	Disabling the power saving function		
14	Installing EXPRESSCLUSTER	See Chapter 3, "Installing EXPRESSCLUSTER" in the <i>Installation and Configuration Guide</i> .	Same as "On-premise"
After installing EXPRESSCLUSTER			
15	Registering the EXPRESSCLUSTER license	See Chapter 4, "Registering the license" in the <i>Installation and Configuration Guide</i> .	Same as "On-premise"
16	Creating a cluster: Setting the heartbeat method	See "Creating the configuration data of a 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.
17	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"> <li>• "Creating the configuration data of a node cluster" in Chapter 5, "Creating the cluster configuration data" in the <i>Installation and Configuration Guide</i></li> <li>• Chapter 5, "Network partition resolution resources details" in the <i>Reference Guide</i>.</li> </ul>	<p>See either of the following depending on the load balancer to use:</p> <ul style="list-style-type: none"> <li>• See "4.3 Configuring the EXPRESSCLUSTER settings" in this guide.</li> <li>• See "5.3 Configuring the EXPRESSCLUSTER settings" in this guide.</li> </ul>
18	Creating a cluster: Creating a failover group and monitor resource	See "Creating the configuration data of a node cluster" in Chapter 5, "Creating the cluster configuration data" in the <i>Installation and Configuration Guide</i> .	<p>See the following in addition to the description of "On-premise."</p> <ul style="list-style-type: none"> <li>• "Understanding Azure probe port resources" in the <i>Reference Guide</i>.</li> <li>• "Understanding Azure load balance monitor resources" in the <i>Reference Guide</i>.</li> <li>• "Understanding Azure load balance monitor resources" in the <i>Reference Guide</i>.</li> </ul> <p>See either of the following depending on the load balancer to use:</p>

Step No.	Procedure	On-premise	Microsoft Azure
			<ul style="list-style-type: none"> <li>• See "4.3 Configuring the EXPRESSCLUSTER settings" in this guide.</li> <li>• See "5.3 Configuring the EXPRESSCLUSTER settings" in this guide.</li> </ul>

## 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	Windows Server 2016 DataCenter
EXPRESSCLUSTER	EXPRESSCLUSTER X 4.1 for Windows(Internal version: 12.10)
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	2.0
Python	2.7

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

Python is installed together with the Azure CLI 2.0.

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

Get started with Azure CLI:

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

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

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

### 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 node-1 is used as an active server.

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

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

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

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

Setting item	Setting value	
	node-1	node-2
Virtual machine setting		
Disk type	Standard HDD	
User name	testlogin	
Password	PassWord_123	
Resource group	TestGroup1	
Region	Japan East	
Network security group setting		
Name	NetSecGroup-1	
Availability set setting		
Name	AvailabilitySet-1	
Update domains	5	
Fault domains	2	
Diagnostics storage account setting		
Name	Automatically generated (testgroup1diag679)	
Replication	Locally-redundant storage (LRS)	
IP configuration setting		
IP address	10.5.0.120	10.5.0.121
Blob storage setting		
Name	node-1Blob1	node-2Blob1
Source type	None (empty disk)	
Account type	Standard HDD	

- EXPRESSCLUSTER settings (cluster properties)

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

- EXPRESSCLUSTER settings (failover group)

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

- EXPRESSCLUSTER settings (monitor resource)

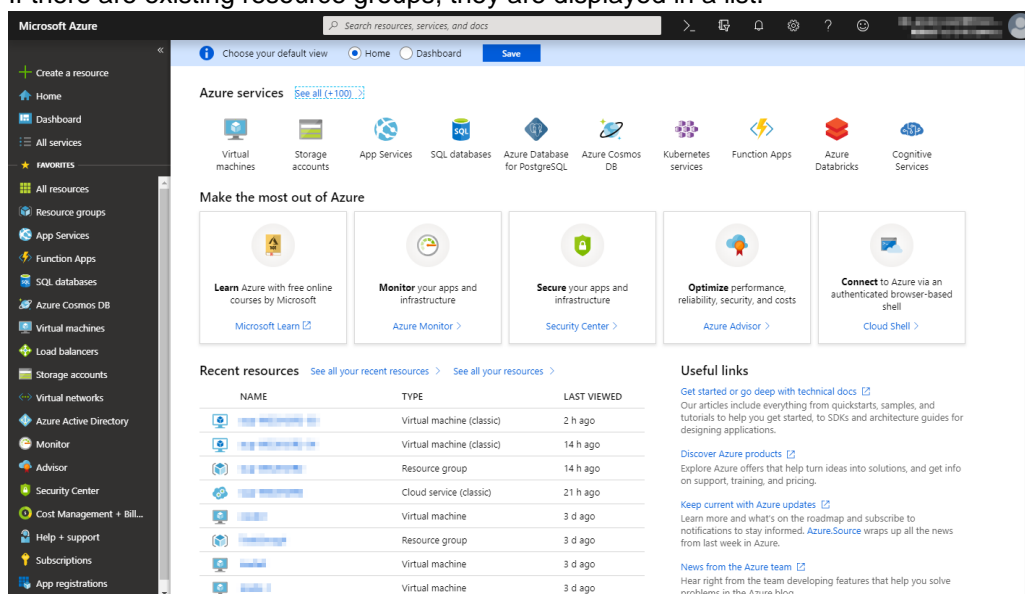
Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	-	-
Azure DNS monitor resource	Name	azurednsw1
Custom monitor resource	Name	genw1
	Script created with this product	On
	Monitor Type	Synchronous
	Normal Return Value	0
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
IP monitor resource	Name	ipw1
	Server to monitor	node-1
	IP address	10.5.0.121
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
IP monitor resource	Name	ipw2
	Server to monitor	node-2
	IP address	10.5.0.120
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer
Multi target monitor resource	Name	mtw1
	Monitor resource list	genw1 ipw1 ipw2
	Recovery Action	Execute only the final action
	Recovery Target	LocalServer

## 3.2 Configuring Microsoft Azure

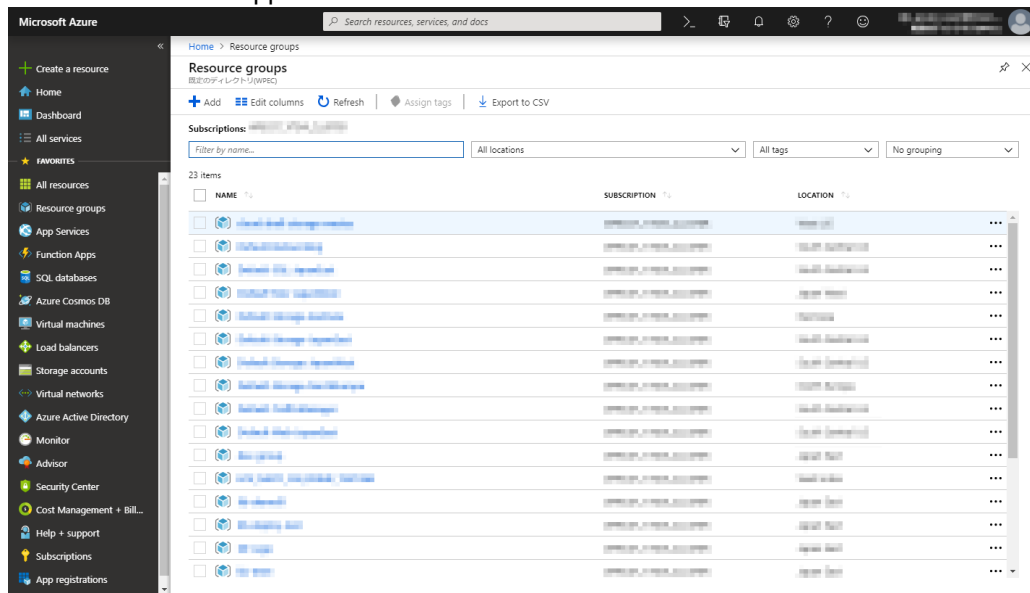
### 1) Creating a resource group

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

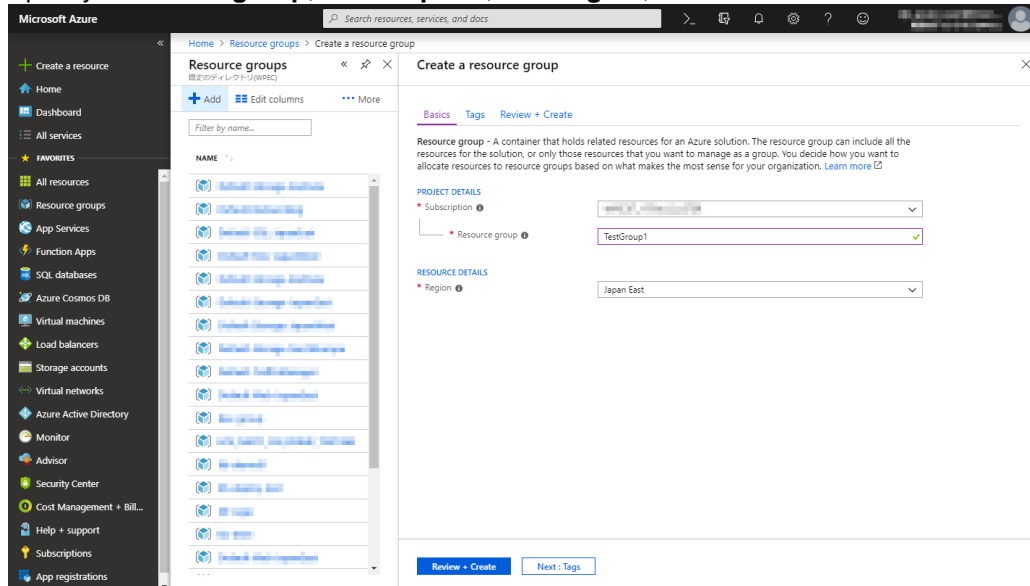
1. Select **Resource groups** or the resource group icon in the menu on the left side of the window. If there are existing resource groups, they are displayed in a list.



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



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

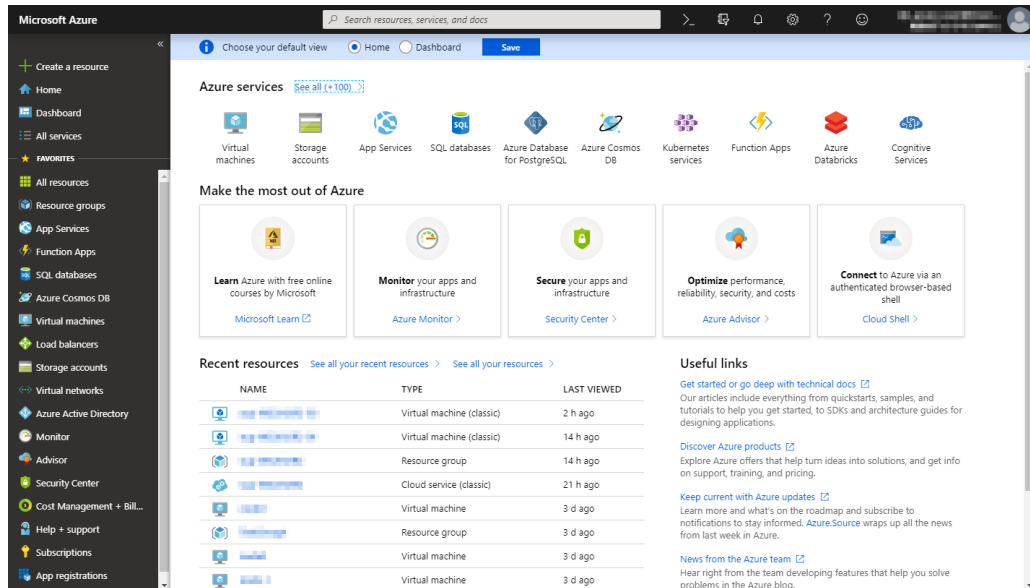




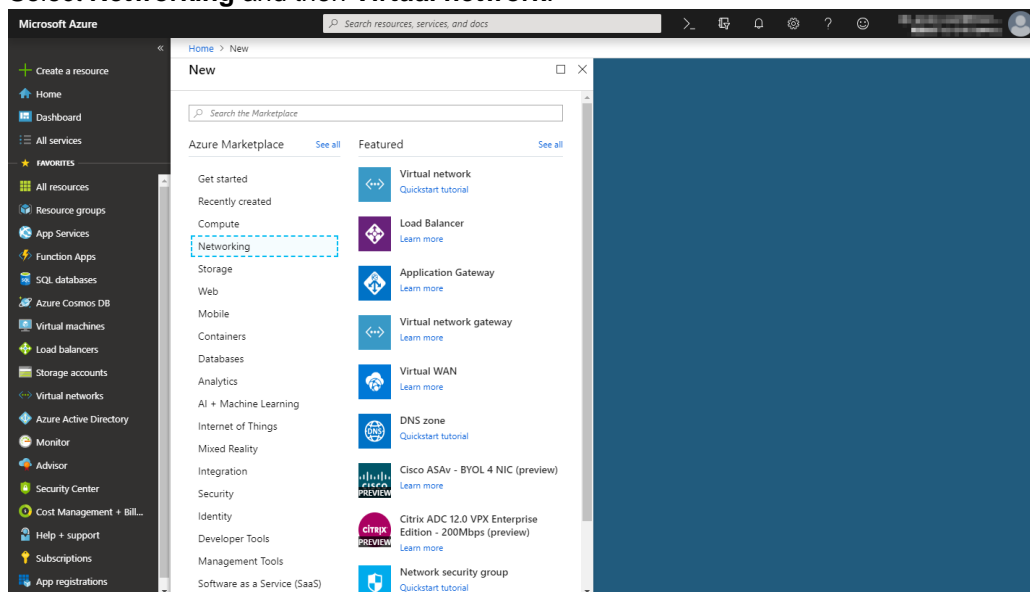
### 2) Creating a virtual network

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

1. Select **+Create a resource** 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**, **Location**, **Name of Subnet**, and **Address range**, and click **Create**.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The left sidebar contains the navigation menu with 'Virtual networks' selected. The main pane displays the configuration form for a new virtual network. The form includes the following fields and options:

- Name:** Vnet1
- Address space:** 10.5.0.0/16 (10.5.0.0 - 10.5.255.255 (65536 addresses))
- Subscription:** (selected)
- Resource group:** TestGroup1
- Location:** Japan East
- Subnet:**
  - Name:** Vnet1-1
  - Address range:** 10.5.0.0/24 (10.5.0.0 - 10.5.0.255 (256 addresses))
- DDoS protection:** Basic (selected), Standard (unselected)
- Service endpoints:** Disabled (selected), Enabled (unselected)
- Firewall:** Disabled (selected), Enabled (unselected)

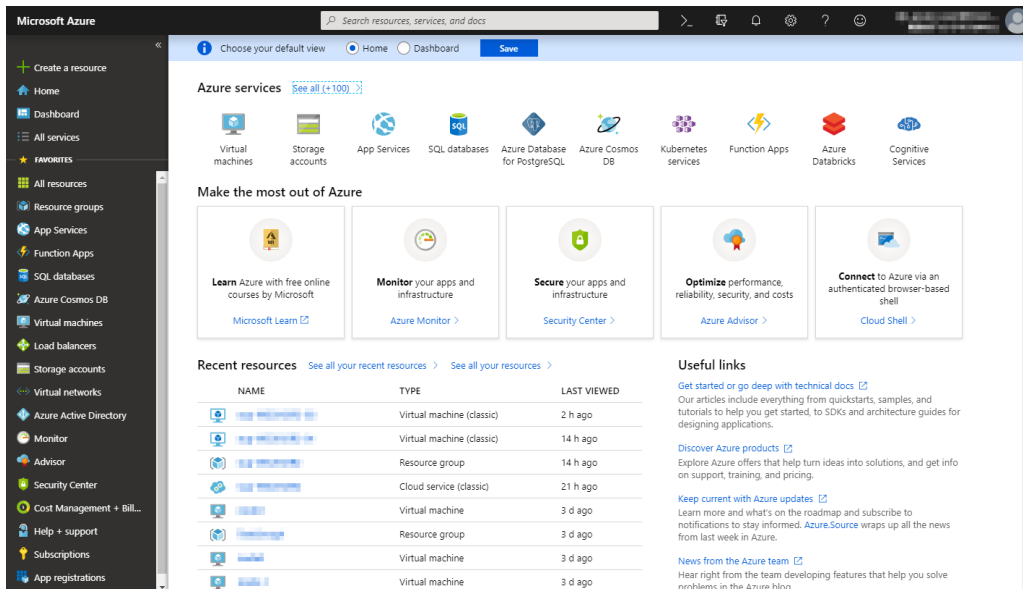
The 'Create' button is located at the bottom of the form, with a link to 'Automation options' next to it.

### 3) Creating a virtual machine

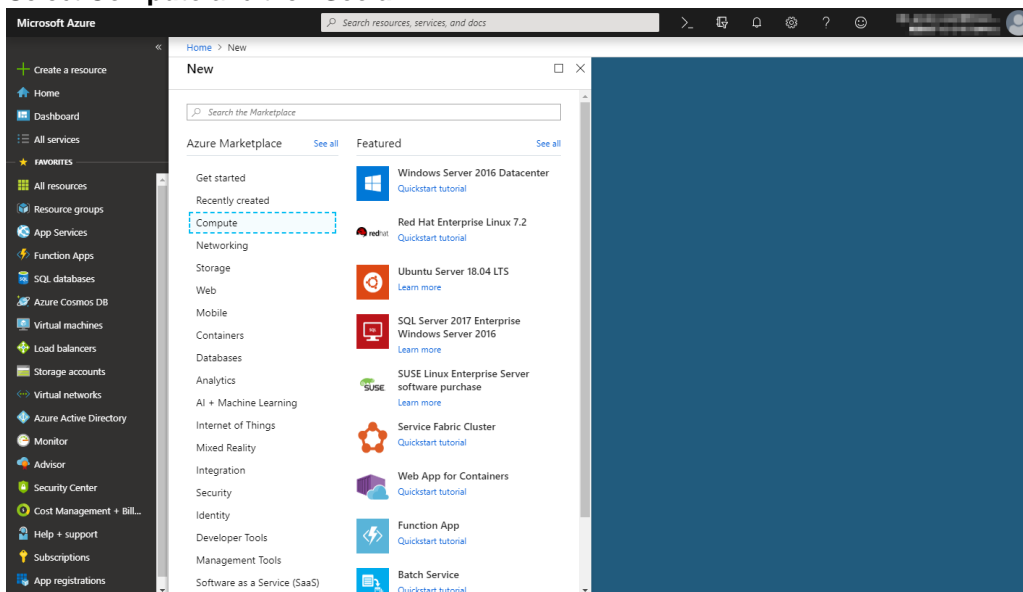
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create virtual machines and disks following the steps below.

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

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



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



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

Microsoft Azure

Home > New > Create a virtual machine

### Create a virtual machine

Basics Disks Networking Management Guest config Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Looking for classic VMs? [Create VM from Azure Marketplace](#)

**PROJECT DETAILS**  
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

\* Subscription

\* Resource group  [Create new](#)

**INSTANCE DETAILS**

\* Virtual machine name

\* Region

Availability options

\* Availability set  [Create new](#)

\* Image  [Browse all images and disks](#)

\* Size

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

Microsoft Azure

Home > New > Create a virtual machine

### Create a virtual machine

Basics Disks Networking Management Guest config Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Looking for classic VMs? [Create VM from Azure Marketplace](#)

**PROJECT DETAILS**  
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

\* Subscription

\* Resource group  [Create new](#)

**INSTANCE DETAILS**

\* Virtual machine name

\* Region

Availability options

\* Availability set  [Create new](#)

\* Image  [Browse all images and disks](#)

\* Size

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

**Create new**

Group two or more VMs in an availability set to ensure that at least one is available during planned or unplanned maintenance events. [Learn more](#)

\* Name

Fault domains

Update domains

Use managed disks ☐ No (Classic) ☒ Yes (Aligned)

[OK](#)

5. Click **Change size** to display the **Select a VM size** blade. From the list, choose a size (**A1 - Standard** in this guide) suitable for your virtual machine and click **Select**. Regarding the **Virtual machine name**, node-1 is for node-1, and node-2 is for node-2. Click **Next: Disks** >

VM SIZE	OFFERING	FAMILY	vCPUS	RAM (GB)	DATA DISKS	MAX IOPS	TEMPORARY STORAGE	PREMIUM DISK SUPP.	COST/MONTH (ESTL.)
A0	Standard	General purpose	1	0.75	1	1x500		No	¥2,001
A0	Basic	General purpose	1	0.75	1	1x300		No	¥1,838
A1	Standard	General purpose	1	1.75	2	2x500		No	¥8,839
A1	Basic	General purpose	1	1.75	2	2x300		No	¥3,415
A1_v2	Standard	General purpose	1	2	2	2x500		No	¥6,748
A2	Standard	General purpose	2	3.5	4	4x500		No	¥17,677
A2	Basic	General purpose	2	3.5	4	4x300		No	¥12,083
A2_v2	Standard	General purpose	2	4	4	4x500		No	¥14,173
A2m_v2	Standard	General purpose	2	16	4	4x500		No	¥19,426
A3	Standard	General purpose	4	7	8	8x500		No	¥35,347
A3	Basic	General purpose	4	7	8	8x300		No	¥31,680
A4	Standard	General purpose	8	14	16	16x500		No	¥70,687
A4	Basic	General purpose	8	14	16	16x300		No	¥63,359

6. When the **Disks** tab appears, go through the following steps to add a blob to be used for a mirror disk (cluster partition or data partition). From the **DATA DISKS** list, click **Create and attach a new disk**.

**DISK OPTIONS**

OS disk type: Standard SSD

Enable Ultra SSD compatibility (Preview): ☐ Yes ☒ No

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

**DATA DISKS**

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

LUN	NAME	SIZE (GiB)	DISK TYPE	HOST CACHING
Create and attach a new disk   Attach an existing disk				

**ADVANCED**

Review + create | Previous | Next: Networking >

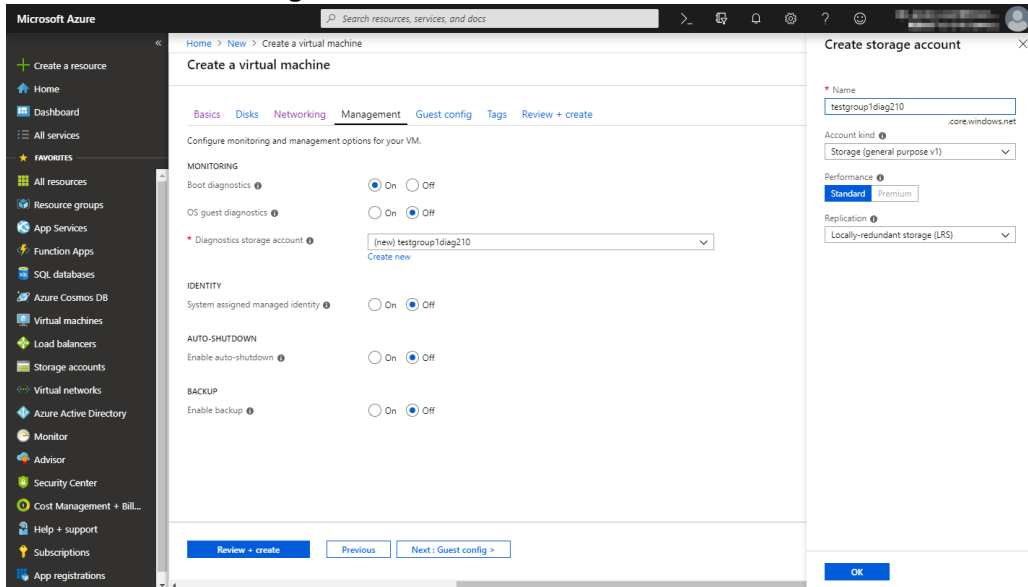
7. The **Create a new disk** blade appears. Specify the settings of **Disk type**, **Name**, **Size (GiB)**, and **Source type**. Then click **OK**. Click **Next: Networking** >.

The screenshot shows the 'Create a new disk' blade in the Microsoft Azure portal. The left sidebar contains the navigation menu with 'Create a resource' at the top. The main content area has a breadcrumb trail: 'Home > New > Create a virtual machine > Create a new disk'. Below the breadcrumb, there's a title 'Create a new disk' and a close button. The main section contains instructions: 'Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions. [Learn more about Azure Managed Disks](#)'. There are four input fields: 'Disk type' (Standard HDD), 'Name' (node-1blob1), 'Size (GiB)' (empty), and 'Source type' (None (empty disk)). Below these fields is the 'ESTIMATED PERFORMANCE' section showing 'IOPS limit' as 500 and 'Throughput limit (MB/s)' as 60. At the bottom, there is an 'OK' button.

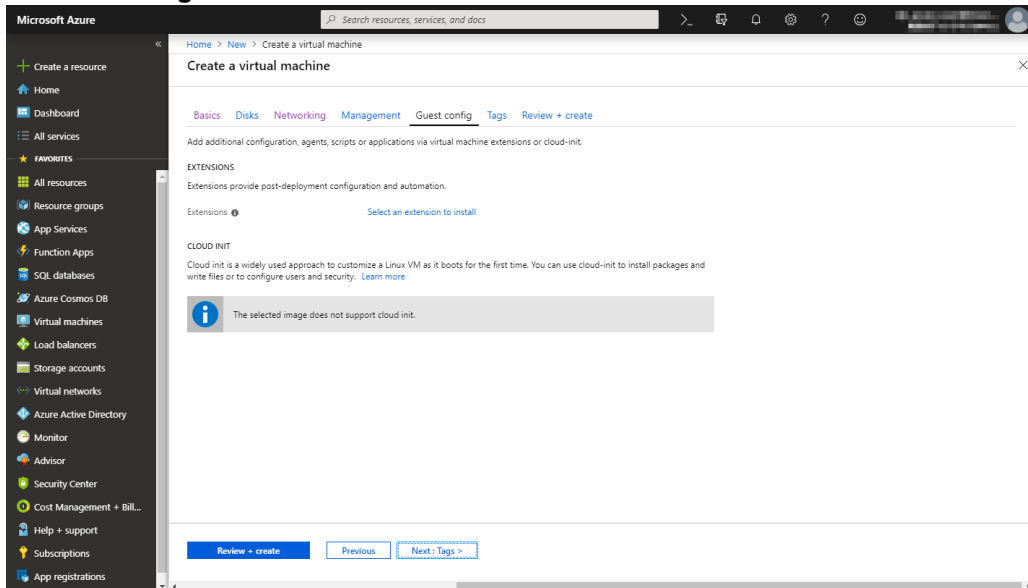
8. The **Networking** tab appears. Specify the settings of **Virtual network**, **Subnet**, **Network security group**, and **Configure network security group**. Click **Create new** under the **Configure network security group** field to display the **Create network security group** blade. Specify the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

The screenshot shows the 'Create network security group' blade in the Microsoft Azure portal. The left sidebar is the same as in the previous screenshot. The main content area has a breadcrumb trail: 'Home > New > Create a virtual machine > Create network security group'. Below the breadcrumb, there's a title 'Create network security group' and a close button. The main section contains instructions: 'When configuring network interface card (NIC) settings, you can control ports, inbound and outbound traffic, and place behind an existing load balancing solution. [Learn more](#)'. There are several input fields: 'Name' (NetSecGroup-1), 'Virtual network' (new), 'Subnet' (new), 'Address range' (10.0.0.0/24), 'Subnet configuration' (new), 'Network security group' (new), 'Accelerated networking' (Off), and 'Load balancing' (No). At the bottom, there is a 'Next: Management >' button and an 'OK' button.

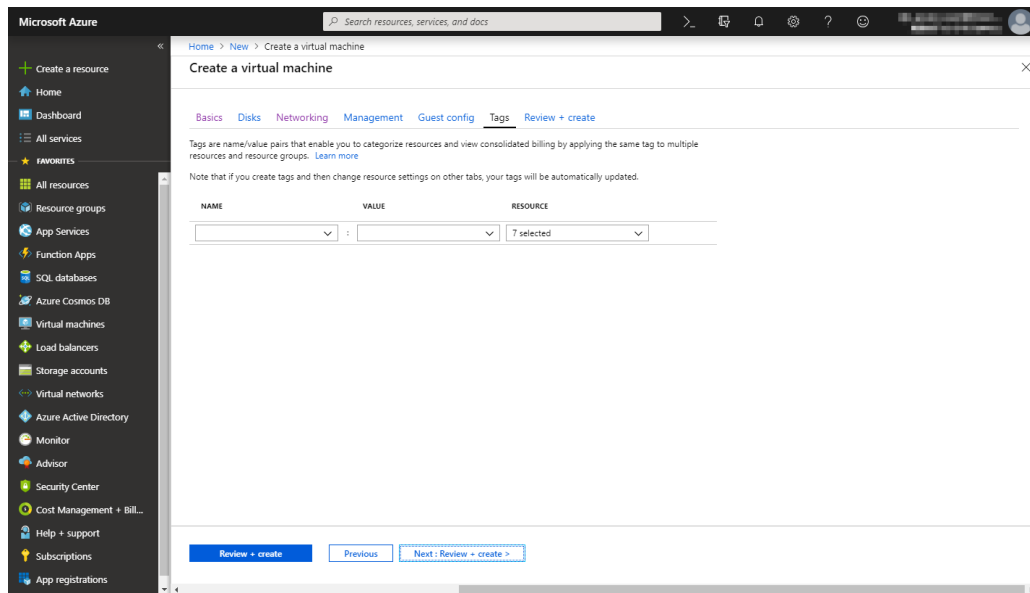
9. The **Management** tab appears.  
Click **Create new** under the **Diagnostics storage account** field to display the **Create storage account** blade.  
Specify the settings of **Name**, **Account kind**, and **Replication**. Then click **OK**.  
In the **Diagnostics storage account** field, the default value is automatically generated and entered.  
Click Next: **Guest config** >.



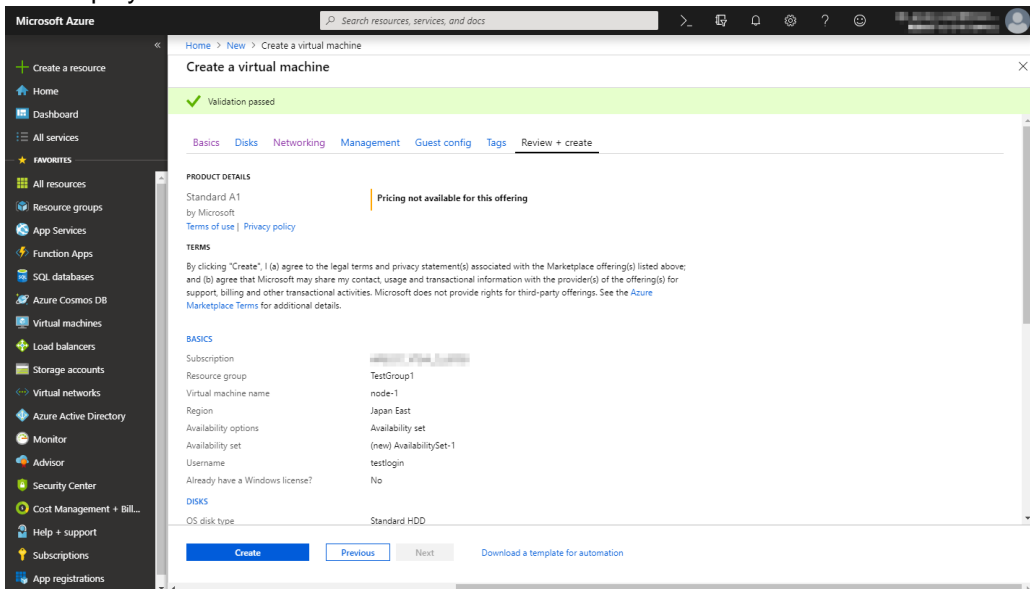
10. Click Next: **Tags** >.



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



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

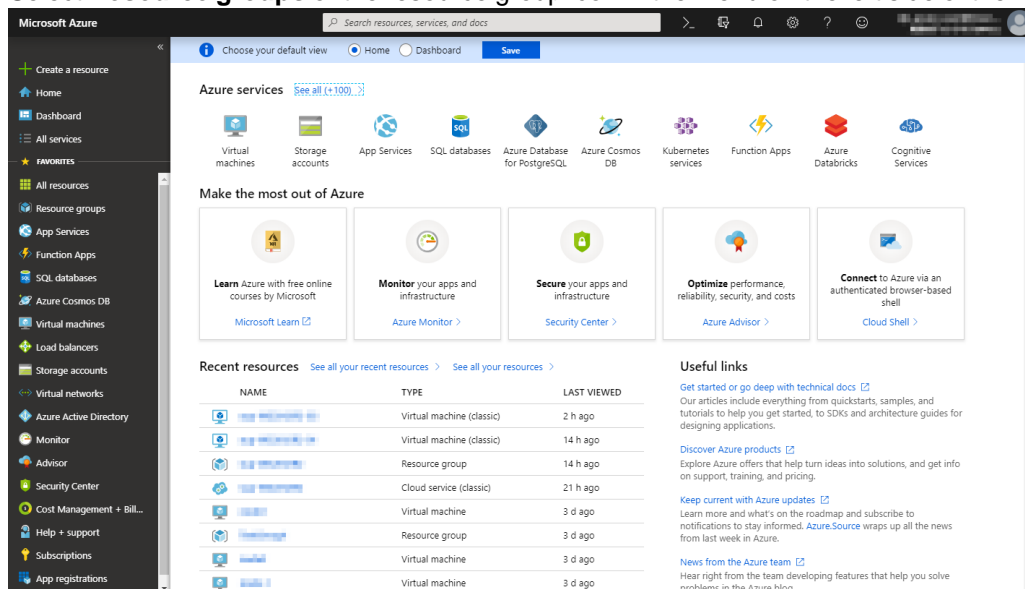




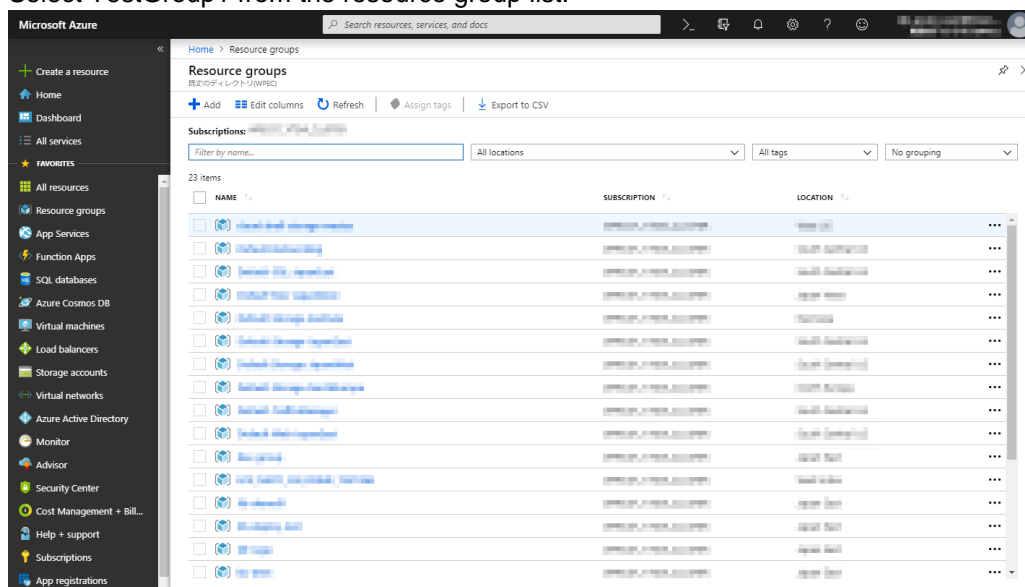
#### 4) Setting a private IP address

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

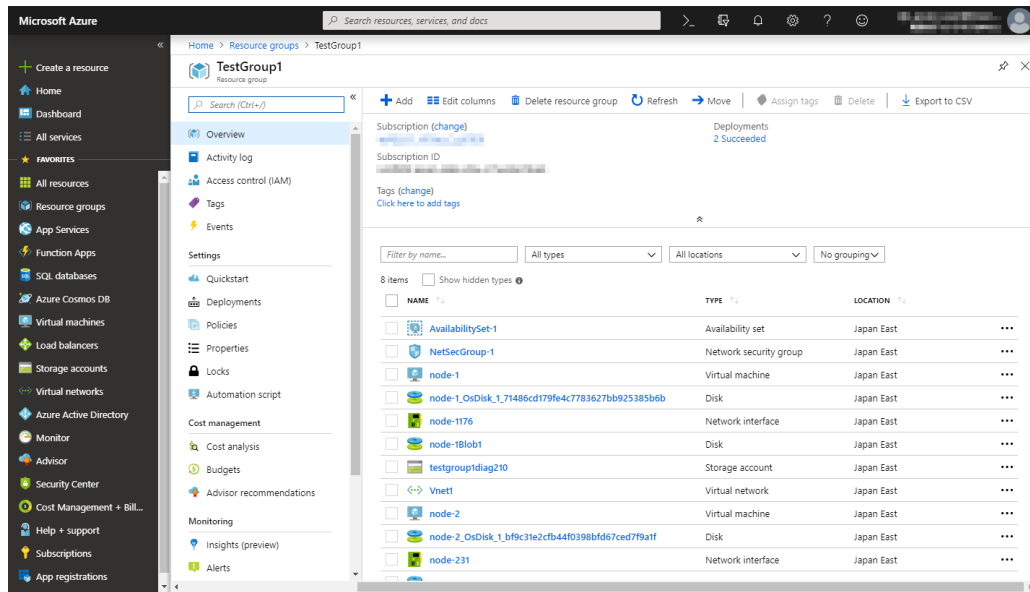
1. Select **Resource groups** or the resource group icon in the menu on the left side of the window.



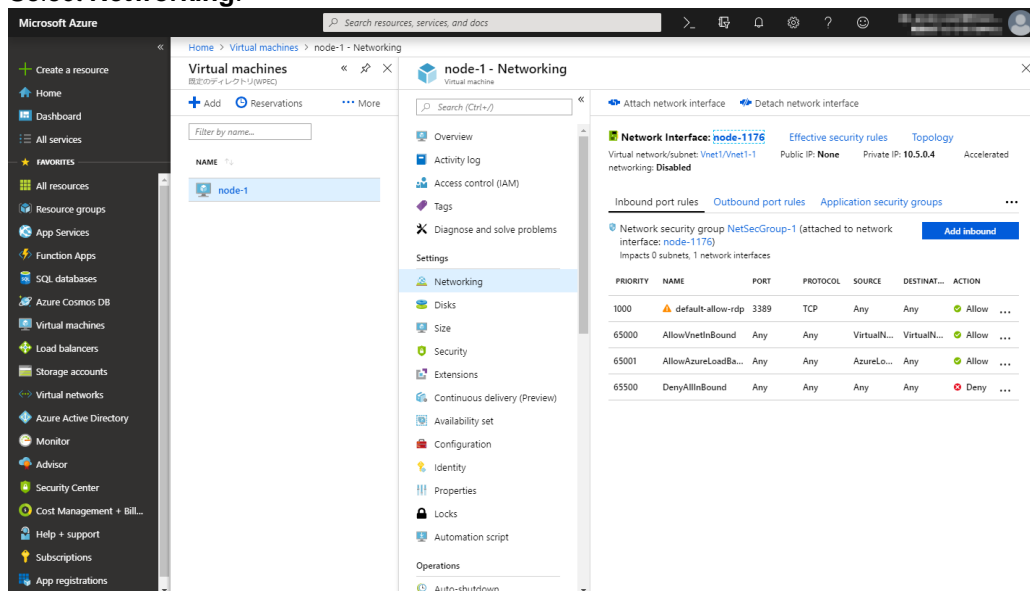
2. Select **TestGroup1** from the resource group list.



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

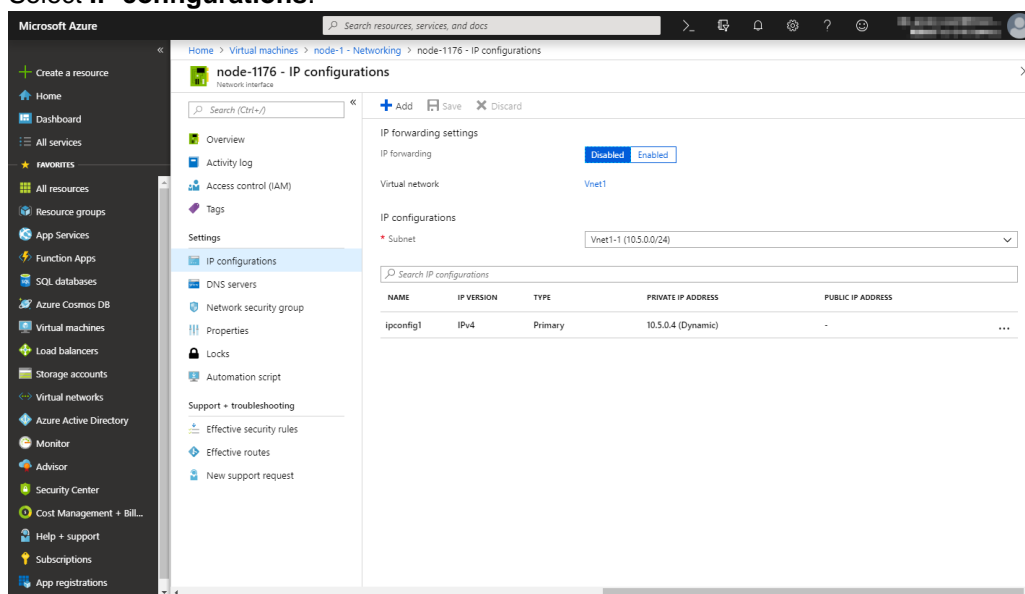


- Select Networking.

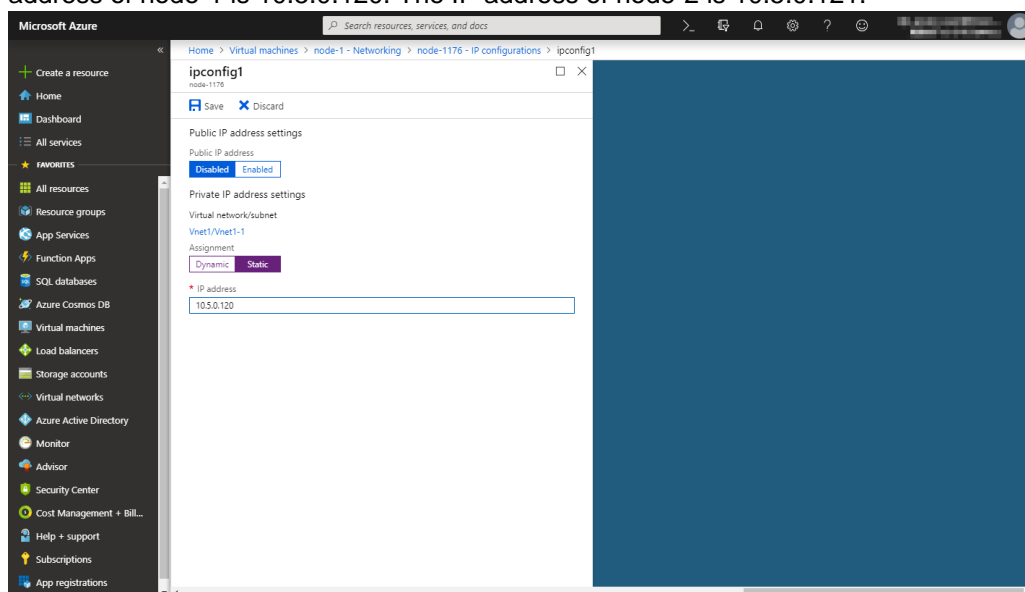


- Select a network interface displayed in the list. The network interface name is generated automatically.

## 6. Select IP configurations.



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

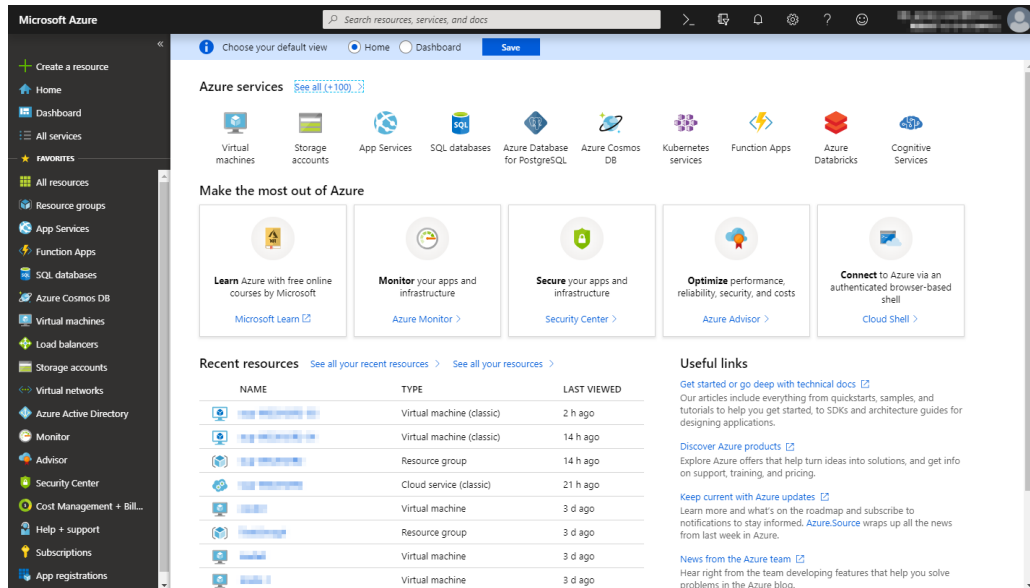
8. Select **Static** for **Assignment** under **Private IP address settings**. Enter the IP address to be assigned statically in the **IP address** text box and click **Save** at the top of the window. The IP address of node-1 is 10.5.0.120. The IP address of node-2 is 10.5.0.121.

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

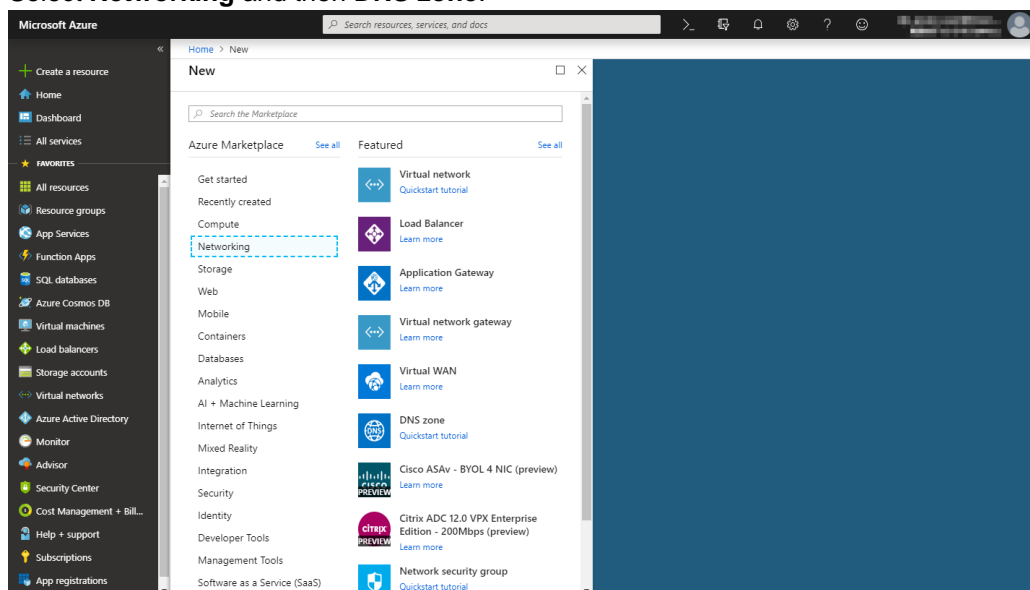
## 5) Creating a DNS zone

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

1. Select **+Create a resource** 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 **Review+create**.

Microsoft Azure

Home > New > Create DNS zone

### Create DNS zone

Basics Tags Review + create

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more](#)

**PROJECT DETAILS**

Subscription: [Dropdown menu]

Resource group: TestGroup1 [Create new](#)

**INSTANCE DETAILS**

Name: cluster1.zone ✓

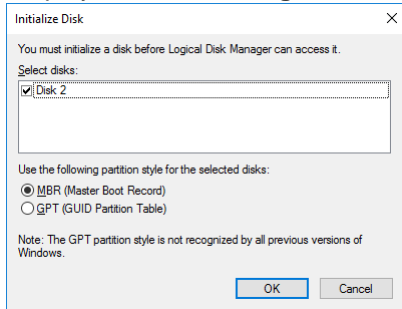
Resource group location: Japan East

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

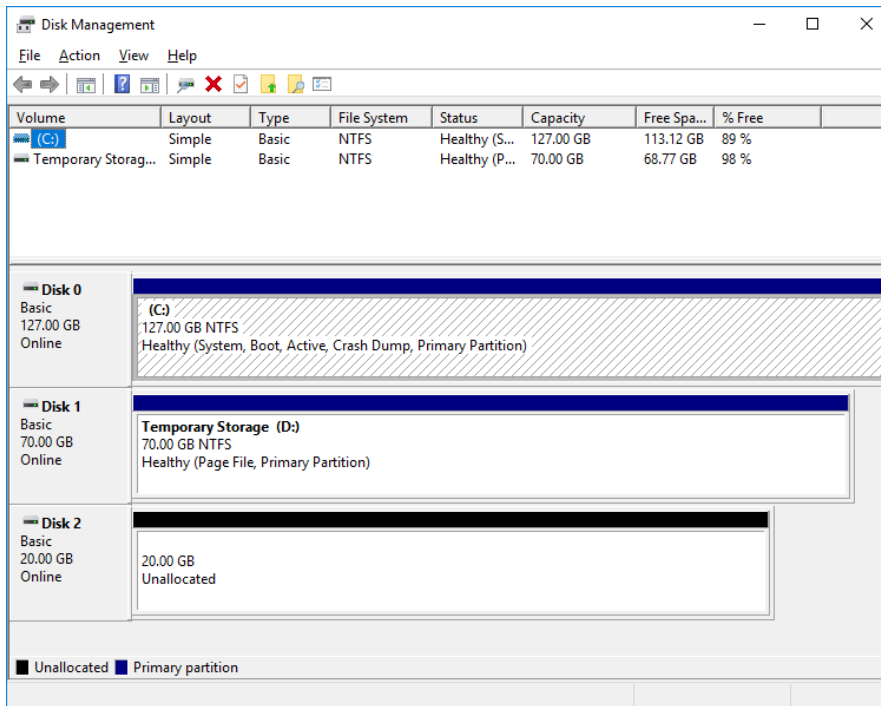
## 6) Configuring virtual machines

Log in to the created node-1 and node-2 and specify the settings following the procedure below. Set a partition for the mirror disk resource. Create a file system in the added Blob storage. 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*.

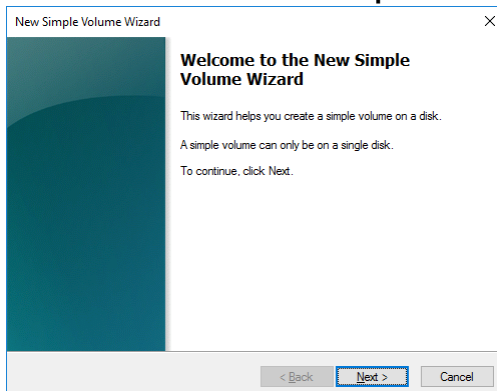
1. Display the **Disk Management** window. The **Initialize Disk** dialog box is displayed.



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



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



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

The screenshot shows the 'Specify Volume Size' step of the 'New Simple Volume Wizard'. The window title is 'New Simple Volume Wizard'. Below the title bar, the section is 'Specify Volume Size' with the instruction 'Choose a volume size that is between the maximum and minimum sizes.' The main area contains three labels: 'Maximum disk space in MB:' with a value of 20477, 'Minimum disk space in MB:' with a value of 8, and 'Simple volume size in MB:' with a text box containing '1024' and a spinner control. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

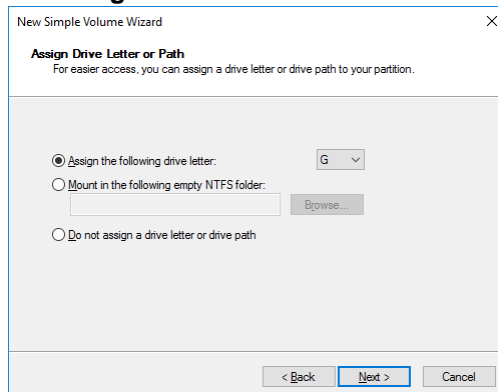
6. The **Assign Drive Letter or Path** window is displayed. Select the F drive for **Assign the following drive letter:**. Use the disk as a raw partition without formatting.

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

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

The screenshot shows the 'Specify Volume Size' step of the 'New Simple Volume Wizard'. The window title is 'New Simple Volume Wizard'. Below the title bar, the section is 'Specify Volume Size' with the instruction 'Choose a volume size that is between the maximum and minimum sizes.' The main area contains three labels: 'Maximum disk space in MB:' with a value of 19453, 'Minimum disk space in MB:' with a value of 8, and 'Simple volume size in MB:' with a text box containing '19453' and a spinner control. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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



New Simple Volume Wizard

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

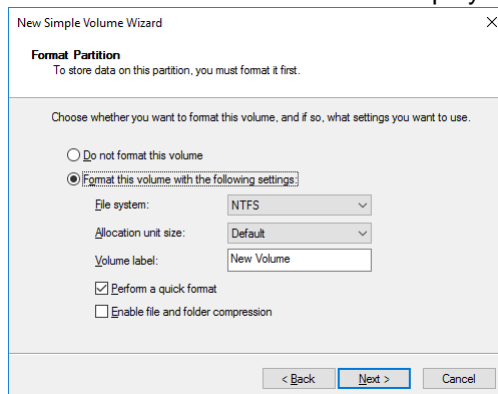
☒ Assign the following drive letter: G

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

☐ Do not assign a drive letter or drive path

< Back Next > Cancel

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



New Simple Volume Wizard

**Format Partition**  
To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

☐ Do not format this volume

☒ Format this volume with the following settings:

File system: NTFS

Allocation unit size: Default

Volume label: New Volume

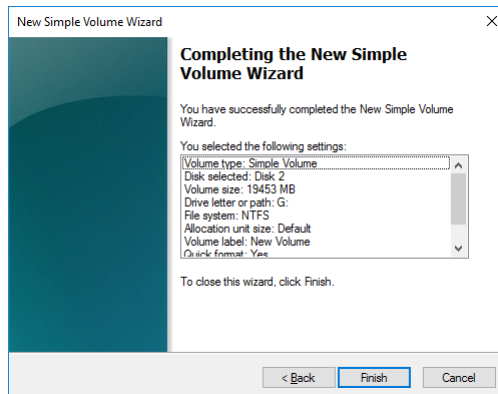
☒ Perform a quick format

☐ Enable file and folder compression

< Back Next > Cancel

12. Click **Next**.

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



New Simple Volume Wizard

**Completing the New Simple Volume Wizard**

You have successfully completed the New Simple Volume Wizard.

You selected the following settings:

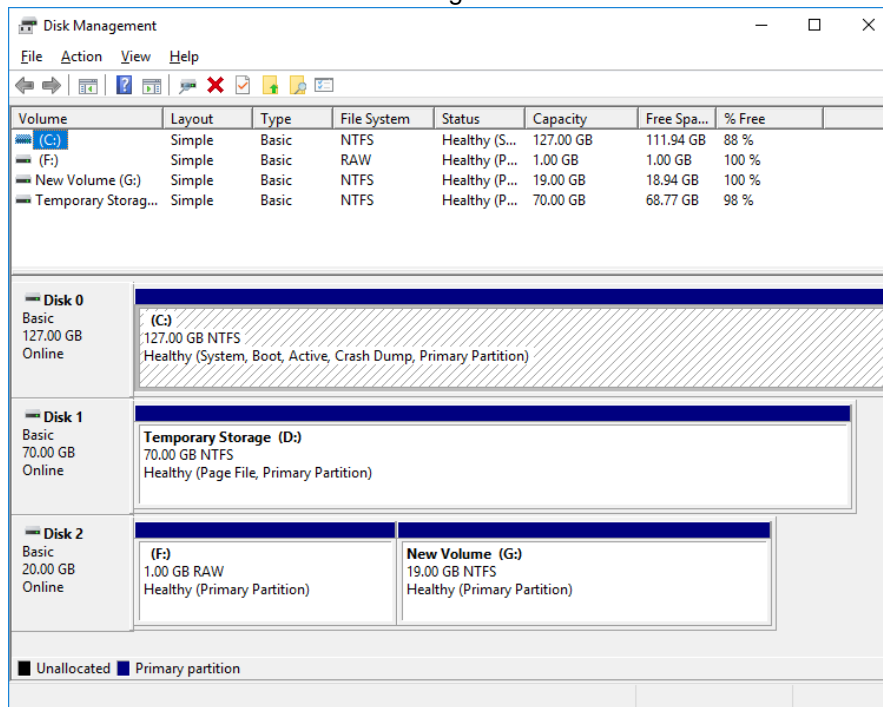
- Volume type: Simple Volume
- Disk selected: Disk 2
- Volume size: 19453 MB
- Drive letter or path: G:
- File system: NTFS
- Allocation unit size: Default
- Volume label: New Volume
- Quick format: Yes

To close this wizard, click Finish.

< Back Finish Cancel



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



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

For each procedure, see "Settings after configuring hardware" in Chapter 1, "Determining a system configuration" in the *Installation and Configuration Guide*.

**8) Installing the Azure CLI**

Install the Azure CLI.

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

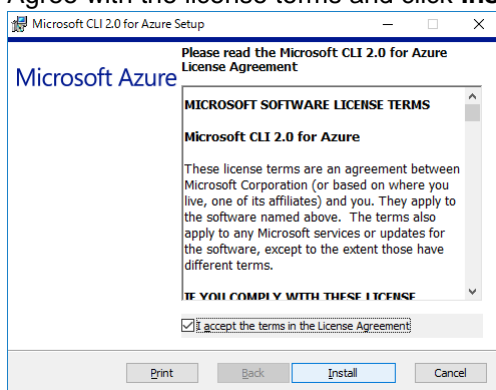
For details about this procedure and other procedures, see the following website:

Install the Azure CLI:

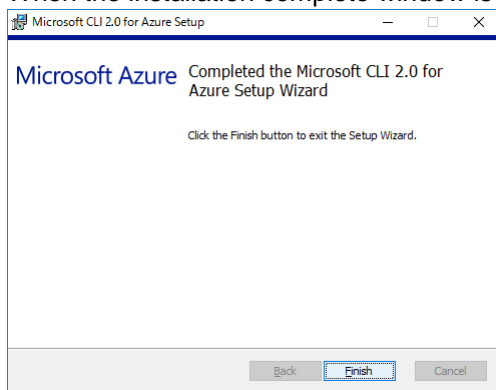
<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli?view=azure-cli-latest>

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

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



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



**9) Creating a service principal**

Create a service principal using the Azure CLI.

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

Please note that certificates have an expiration date.

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

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

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

Sign in with Azure CLI:

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

Create an Azure service principal with Azure CLI:

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

1. Log in with an organizational account.

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

2. Create and register a service principal. Write down the displayed name and tenant because it is necessary to set them in the Azure environment configuration file. In the following example, a service principal is created in `C:\Users\testlogin\examplecert.pem`.

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

3. Log out.

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

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

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

The following is displayed upon successful sign-in.

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

5. Log out.

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

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

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

**10) Installing EXPRESSCLUSTER**

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

**11) Registering the EXPRESSCLUSTER license**

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

## 3.3 Configuring the EXPRESSCLUSTER settings

For the Cluster WebUI 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)
- IP monitor resource (for NP resolution)
- Multi target monitor resource (for NP resolution)

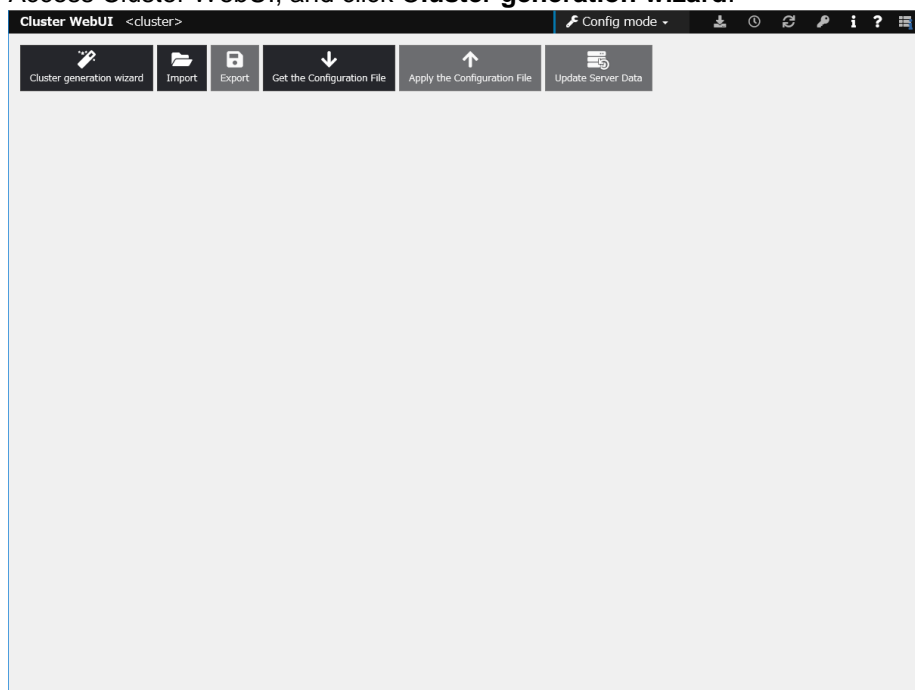
or the settings of other resources and monitor resources, see the *Installation and Configuration Guide* and the *Reference Guide*.

### 1) Creating a cluster

Start the cluster generation wizard to create a cluster.

#### ◆ Creating a cluster

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



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

Cluster generation wizard

Cluster

Basic Settings

Interconnect

NP Resolution

Group

Monitor

Cluster Name\*

Cluster1

Comment

Language\*

English

Management IP Address

Start generating the cluster.

Enter the cluster name, and then select the language (locale) of the environment that runs WebManager.

If using the integrated WebManager to manage multiple clusters, specify a unique cluster name to identify the cluster.

The management IP address is a floating IP address used for a WebManager connection. If establishing connections by specifying each server IP address, the management IP address can be omitted.

To continue, click [Next].

Back

Next

Cancel

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

Add server

Server Name or IP Address\*

10.5.0.121

Enter an IP address or a server name.

When entering a server name, name resolution is necessary.

Both IPv4 and IPv6 for IP address can be used.

When entering an IP address, the server name is automatically acquired.

OK

Cancel

Cluster generation wizard

Cluster

Basic Settings

Interconnect

NP Resolution

Group

Monitor

Add

Remove

Server Definitions

Order	Name
Master server	node-1
1	node-2

Up

Down

Server Group Definition

Settings

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.

Back

Next

Cancel

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

Cluster generation wizard

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

Properties Add Remove

Interconnect List

Priority	Type	MDC	node-1	node-2
1	Kernel Mode	Do Not Use	10.5.0.120	10.5.0.121

↑ ↓

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

Back Next Cancel

5. The **NP Resolution** window is displayed.  
Note that NP resolution is not configured on this window. The equivalent feature is achieved by adding the IP monitor resource, custom monitor resource, and multi target monitor resource. Configure NP resolution in "3)Adding a monitor resource"  
You need to examine the NP resolution destination and method depending on the location of clients accessing a cluster system and the condition for connecting to an on-premise environment (for example, using a dedicated line). Additionally, you can use network partition resolution resources for NP resolution.  
Click **Next**.

Cluster generation wizard

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

Properties Add Remove

NP Resolution List

Type	Ping Target	node-1	node-2
No NP resolutions			

Tuning

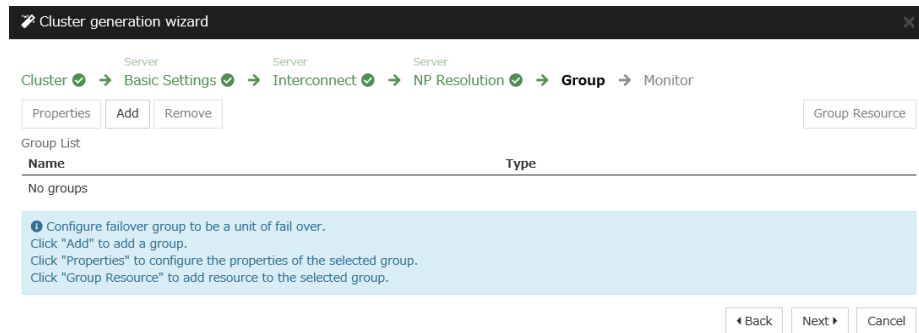
Configure network partition (NP) resolution function.  
 Click "Add" to add NP resolution resource and select the type.  
 For "COM" setting, click each server column cell to configure COM port.  
 For "DISK" setting, click each server column cell to configure driver letter of the partition for disk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

Back Next Cancel

## 2) Adding a group resource

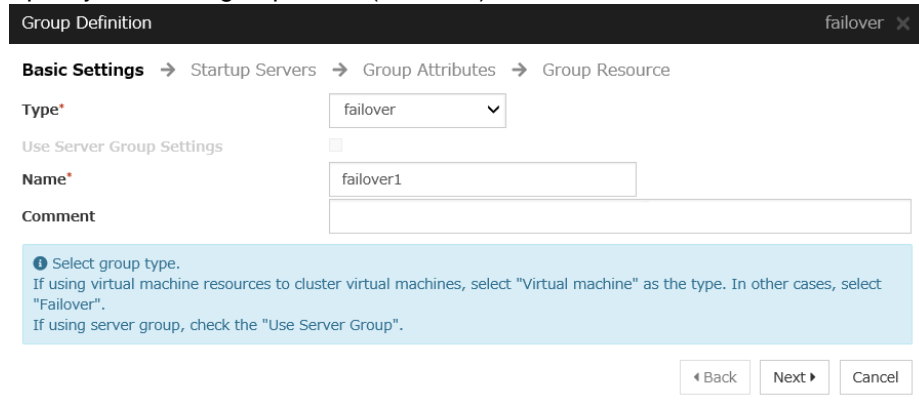
- ◆ Defining a group  
Create a failover group.

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



The screenshot shows the 'Cluster generation wizard' window. The progress bar indicates the following steps: Cluster (checked), Basic Settings (checked), Interconnect (checked), NP Resolution (checked), **Group** (active), and Monitor. Below the progress bar, there are buttons for 'Properties', 'Add', and 'Remove'. A 'Group List' table is shown with columns 'Name' and 'Type', and it currently contains no groups. A blue information box provides instructions: 'Configure failover group to be a unit of fail over. Click "Add" to add a group. Click "Properties" to configure the properties of the selected group. Click "Group Resource" to add resource to the selected group.' At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

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



The screenshot shows the 'Group Definition' window. The progress bar indicates the following steps: Basic Settings (active), Startup Servers, Group Attributes, and Group Resource. The 'Type' dropdown is set to 'failover'. The 'Use Server Group Settings' checkbox is unchecked. The 'Name' field contains 'failover1'. There is a 'Comment' text area. A blue information box provides instructions: 'Select group type. If using virtual machine resources to cluster virtual machines, select "Virtual machine" as the type. In other cases, select "Failover". If using server group, check the "Use Server Group".' At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.



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

The screenshot shows the 'Group Definition' window with the 'failover' tab selected. The breadcrumb trail is 'Basic Settings' → 'Startup Servers' → 'Group Attributes' → 'Group Resource'. Below the breadcrumb are buttons for 'Properties', 'Add', and 'Remove'. A 'Group Resource List' table is shown with columns 'Name' and 'Type', and it currently contains 'No resources'. A blue information box states: 'Click "Add" to add resources. Click "Properties" to configure the properties of the selected resource.' At the bottom right are buttons for 'Back', 'Finish', and 'Cancel'.

◆ **Mirror disk resource**

Create a mirror disk resource.

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

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

The screenshot shows the 'Resource Definition of Group | failover1' window with the 'md' tab selected. The breadcrumb trail is 'Info' → 'Dependency' → 'Recovery Operation' → 'Details'. The 'Type' dropdown is set to 'Mirror disk resource' and the 'Name' text box contains 'md'. There is a 'Comment' text box and a 'Get license information' button. A blue information box states: 'Select the type of group resource and enter its name.' At the bottom right are buttons for 'Back', 'Next', and 'Cancel'.

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

5. The **Details** window is displayed.  
Select a server name in the **Name** column of **Servers that can run the group** and click **Add**.

Resource Definition of Group | failover1 md ✕

Info ✔ → Dependency ✔ → Recovery Operation ✔ → **Details**

Mirror Disk No.\*  
Data Partition Drive Letter\*  
Cluster Partition Drive Letter\*  
Cluster Partition Offset Index\*  
Mirror Disk Connect

1 ▼  
  
  
0 ▼  
Select

Servers that can run the group

Name	Data Partition	Cluster Partition
node-1		
node-2		

←  
Add  
→  
Remove

Edit

Add Servers that can run the group

Tuning

◀ Back

Finish

Cancel

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

Selection of partition

Obtain information

Connect

Data Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	71678MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

Cluster Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	71678MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

OK

Cancel

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

◆ Azure DNS resource

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

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

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

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

5. Enter the values for each of the following: **Record Set Name**, **Zone Name**, **IP Address**, **Resource Group Name**, **User URI**, **Tenant ID**, **File Path of Service Principal**, **Azure CLI File Path**. When using the IP address of each server, enter the IP address in the tab for each server. When setting up the servers separately, enter any IP address of the servers in the **Common** tab and then make settings for other servers.

Resource Definition of Group | failover1

azuredns

Info → Dependency → Recovery Operation → Details

Common node-1 node-2

Record Set Name\*

test-record1

Zone Name\*

cluster1.zone

IP Address\*

10.5.0.120

TTL\*

3600

sec

Resource Group Name\*

TestGroup1

Account

User URI\*

http://azure-test

Tenant ID\*

00000000-0000-0000-0000-000000000000

File Path of Service Principal\*

Azure CLI File Path\*

Delete a record set at deactivation

☒

Tuning

Back

Finish

Cancel

6. Click **Finish**.

### 3) Adding a monitor resource

◆ Azure DNS monitor resource

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

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

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

◆ Custom monitor resource

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

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

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

Monitor Resource Definition genw1 ✕

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

Type\* Custom monitor

Name\* genw1

Comment

Get Licence Info

Select the type of monitor resource and enter its name.

◀ Back Next ▶ Cancel

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

Monitor Resource Definition genw1 ✕

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

Interval\* 60 sec

Timeout\* 120 sec

Do Not Retry at Timeout Occurrence ☐

Do Not Execute Recovery Action at Timeout Occurrence ☐

Retry Count\* 1 time

Wait Time to Start Monitoring\* 3 sec

Monitor Timing

☒ Always

☐ Active

Target Resource  Browse

Choose servers that execute monitoring Server

◀ Back Next ▶ Cancel

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

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

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

Monitor Resource Definition genw ✕

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

☐ User Application  
☒ Script created with this product

File:  Edit View Replace

Monitor Type: ☒ Synchronous  
☐ Asynchronous

Normal Return Value\*:

Kill the application when exit: ☐

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

◀ Back Next ▶ Cancel

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

Monitor Resource Definition genw ✕

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

Recovery Action:  ▼

Recovery Target\*:  Browse

Recovery Script Execution Count:  time

Execute Script before Reactivation: ☐

Maximum Reactivation Count:  time

Execute Script before Failover: ☐

Execute migration before Failover: ☐

Failover Target Server: ☒ Stable server  
☐ Maximum priority server

Maximum Failover Count:  time

Execute Script before Final Action: ☐

Final Action:  ▼

Script Settings

◀ Back Finish Cancel

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

## ◆ IP monitor resource

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

For details about the IP monitor resource, see “Understanding IP monitor resources” in the *Reference Guide*.

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

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

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

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

Monitor Resource Definition ipw X

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

Edit Add Remove

IP Address List

**IP Address**

No Ip Address

Please add a IP Address.

ping Timeout\* 5000 msec

◀ Back Next ▶ Cancel

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

IP Address Settings

**IP Address\*** 10.5.0.121

OK Cancel

Monitor Resource Definition ipw X

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

Edit Add Remove

IP Address List

**IP Address**

10.5.0.121

ping Timeout\* 5000 msec

◀ Back Next ▶ Cancel



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

The screenshot shows the 'Monitor Resource Definition' window with the 'Recovery Action' tab selected. The breadcrumb trail is 'Info → Monitor(common) → Monitor(special) → Recovery Action'. The 'Recovery Action' dropdown is set to 'Execute only the final action'. The 'Recovery Target' is set to 'LocalServer' with a 'Browse' button. Below this, there are several sections with checkboxes and input fields: 'Recovery Script Execution Count' (0), 'Execute Script before Reactivation' (unchecked), 'Maximum Reactivation Count' (0), 'Execute Script before Failover' (unchecked), 'Execute migration before Failover' (unchecked), 'Failover Target Server' (radio buttons for 'Stable server' and 'Maximum priority server', with 'Stable server' selected), and 'Maximum Failover Count' (0). At the bottom, 'Execute Script before Final Action' is unchecked, and the 'Final Action' dropdown is set to 'No operation'. On the right side, there is a 'Script Settings' button and a row of three buttons: 'Back', 'Finish' (highlighted in black), and 'Cancel'.

6. Click **Finish** to finish setting.
7. Then, create a monitor resource on the other server. Click **Add** on the **Monitor Resource List** page.
8. Select the monitor resource type (IP monitor) from the **Type** box and enter the monitor resource name (ipw2) in the **Name** box. Click **Next**.
9. The **Monitor (common)** window is displayed.  
Confirm that **Monitor Timing** is **Always**.  
Select one available server for **Choose servers that execute monitoring**. Click **OK** and Click **Next**.
10. The **Monitor (special)** window is displayed.  
On the **Common** tab, select **Add of IP Address** and set an IP address of a server other than the server selected in step 9. Click **Next**.
11. The **Recovery Action** window is displayed.  
Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final action**.
12. Click **Finish** to finish setting.

◆ **Multi target monitor resource**

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

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

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

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

Monitor Resource Definition mtw ×

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

**Type\*** Multi target monitor

**Name\*** mtw1

**Comment**

Get Licence Info

Select the type of monitor resource and enter its name.

◀ Back Next ▶ Cancel

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

Monitor Resource Definition mtw ×

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

**Interval\*** 60 sec

**Timeout\*** 60 sec

Do Not Retry at Timeout Occurrence ☐

Do Not Execute Recovery Action at Timeout Occurrence ☐

**Retry Count\*** 1 time

**Wait Time to Start Monitoring\*** 0 sec

**Monitor Timing**

☒ Always

☐ Active

Target Resource  Browse

Choose servers that execute monitoring

◀ Back Next ▶ Cancel

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

The screenshot shows the 'Monitor Resource Definition' window with the 'Monitor(special)' tab selected. The breadcrumb trail is 'Info > Monitor(common) > Monitor(special) > Recovery Action'. On the left, the 'Monitor Resource List' table contains three entries: 'genw1' (type 'genw'), 'ipw1' (type 'ipw'), and 'ipw2' (type 'ipw'). The 'genw1' row is highlighted. Between the two tables are 'Add' and 'Remove' buttons. On the right, the 'Available Monitor Resources' table contains one entry: 'userw' (type 'userw'). At the bottom right are 'Back', 'Next', and 'Cancel' buttons. A 'Tuning' button is located at the bottom left of the main content area.

Monitor Resource	Type
genw1	genw
ipw1	ipw
ipw2	ipw

Monitor Resource	Type
userw	userw

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

The screenshot shows the 'Monitor Resource Definition' window with the 'Recovery Action' tab selected. The breadcrumb trail is 'Info > Monitor(common) > Monitor(special) > Recovery Action'. The 'Recovery Action' dropdown is set to 'Execute only the final action'. The 'Recovery Target' is set to 'LocalServer'. Below these are several configuration sections: 'Recovery Script Execution Count' (0), 'Execute Script before Reactivation' (unchecked), 'Maximum Reactivation Count' (0), 'Execute Script before Failover' (unchecked), 'Execute migration before Failover' (unchecked), 'Failover Target Server' (Stable server selected), and 'Maximum Failover Count' (0). At the bottom, 'Execute Script before Final Action' is unchecked, and the 'Final Action' dropdown is set to 'Stop the cluster service and shutdown OS'. At the bottom right are 'Script Settings', 'Back', 'Finish', and 'Cancel' buttons.

Recovery Action: Execute only the final action

Recovery Target: LocalServer

Recovery Script Execution Count: 0 time

Execute Script before Reactivation: ☐

Maximum Reactivation Count: 0 time

Execute Script before Failover: ☐

Execute migration before Failover: ☐

Failover Target Server: ☒ Stable server ☐ Maximum priority server

Maximum Failover Count: 0 time

Execute Script before Final Action: ☐

Final Action: Stop the cluster service and shutdown OS

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

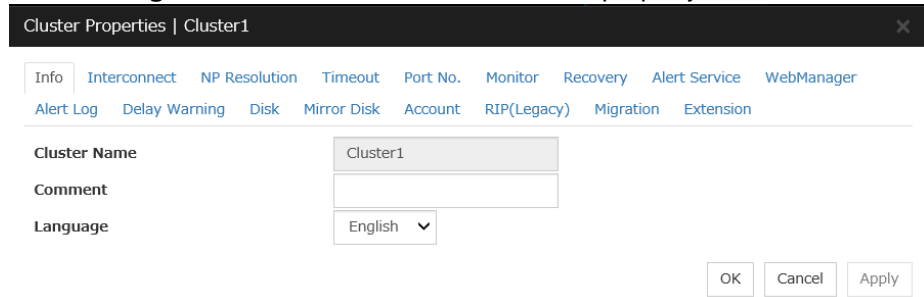
#### 4) Setting the cluster properties

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

##### ◆ Cluster properties

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

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



Cluster Properties | Cluster1

Info Interconnect NP Resolution Timeout Port No. Monitor Recovery Alert Service WebManager  
Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration Extension

Cluster Name Cluster1

Comment

Language English

OK Cancel Apply

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

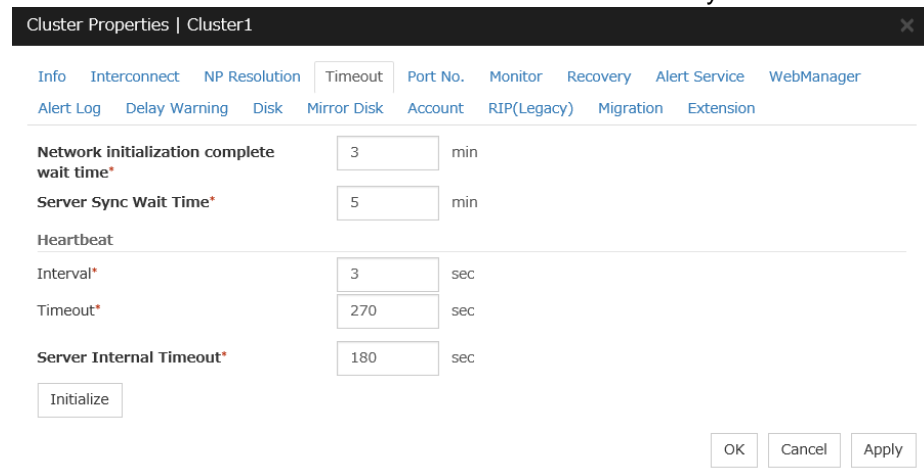
A: **Interval** of the monitor resource being monitored by the multi target monitor resource for NP resolution x (**Retry Count**+1)

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

B: **Interval** of the multi target monitor resource x (**Retry Count**+1)

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

Note: If **Timeout of Heartbeat** is shorter than the time that 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.



Cluster Properties | Cluster1

Info Interconnect NP Resolution Timeout Port No. Monitor Recovery Alert Service WebManager  
Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration Extension

Network initialization complete wait time\* 3 min

Server Sync Wait Time\* 5 min

Heartbeat

Interval\* 3 sec

Timeout\* 270 sec

Server Internal Timeout\* 180 sec

Initialize

OK Cancel Apply

3. Click **OK**.

## 5) Applying the settings and starting the cluster

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

For details, refer to the following:

- *Installation and Configuration Guide*  
→ How to create a cluster

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

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

# Chapter 4 Cluster Creation Procedure (for an HA Cluster Using an Public 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 node-1 is used as an active server.

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

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

Setting item	Setting value
<b>Resource group setting</b>	
Resource group	TestGroup1
Region	Japan East
<b>Virtual network setting</b>	
Name	Vnet1
Address space	10.5.0.0/24
Subnet Name	Vnet1-1
Subnet Address range	10.5.0.0/24
Resource group	TestGroup1
Location	Japan East
<b>Load balancer setting</b>	
Name	TestLoadBalancer
Type	Public
Public IP address: Name	TestLoadBalancerPublicIP
Public IP address: Assignment	Static
Resource group	TestGroup1
Region	Japan East
Backend pool: Name	TestBackendPool
Associated to	Availability set
Target virtual machine	node-1 node-2
Network IP configuration	10.5.0.120 10.5.0.121
Health probe: Name	TestHealthProbe
Health probe: Port	26001
Load balancing rule: Name	TestLoadBalancingRule
Load balancing rule: Port	80 (Port number offering the operation)
Load balancing rule: Backend port	8080 (Port number offering the operation)
<b>Inbound security rule setting</b>	
Name	TestHTTP
Protocol	TCP
Destination Port range	8080 (Port number offering the operation)

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

Setting item	Setting value	
	node-1	node-2
Virtual machine setting		
Disk type	Standard HDD	
User name	testlogin	
Password	PassWord_123	
Resource group	TestGroup1	
Region	Japan East	
Network security group setting		
Name	NetSecGroup-1	
Availability set setting		
Name	AvailabilitySet-1	
Update domains	5	
Fault domains	2	
Diagnostics storage account setting		
Name	Automatically generated (testgroup1diag679)	
Replication	Locally-redundant storage (LRS)	
IP configuration setting		
IP address	10.5.0.120	10.5.0.121
Blob storage setting		
Name	node-1Blob1	node-2Blob1
Source type	None (empty disk)	
Account type	Standard HDD	

- EXPRESSCLUSTER settings (cluster properties)

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

- EXPRESSCLUSTER settings (failover group)

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



- EXPRESSCLUSTER settings (monitor resource)

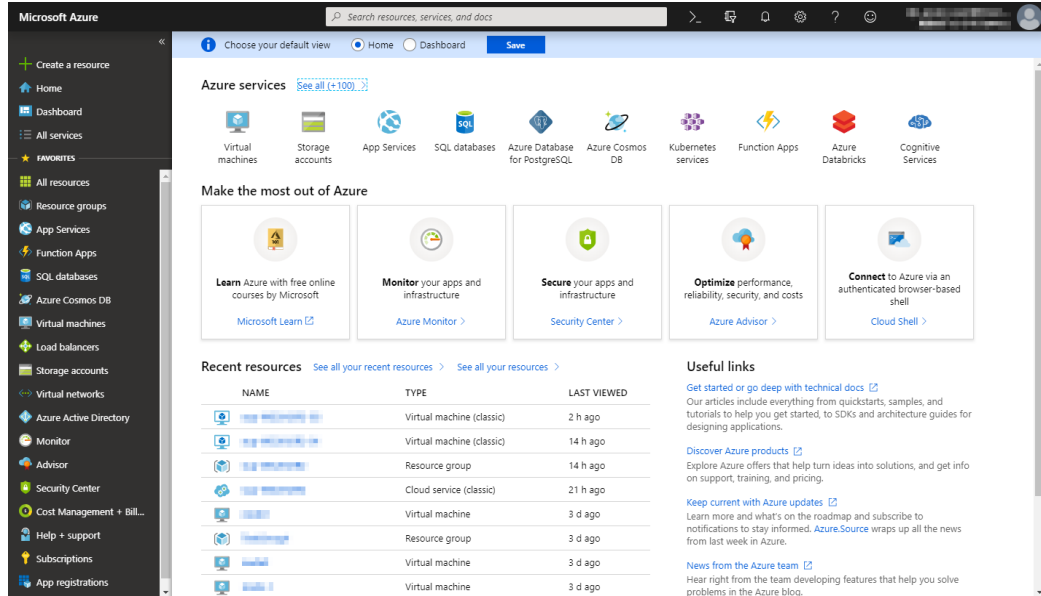
Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	-	-
Azure probe port monitor resource	Name	azureppw1
	Recovery Target	azurepp1
Azure load balance monitor resource	Name	aurelbw1
	Recovery Target	azurepp1
Custom monitor resource	Name	genw1
	Script created with this product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

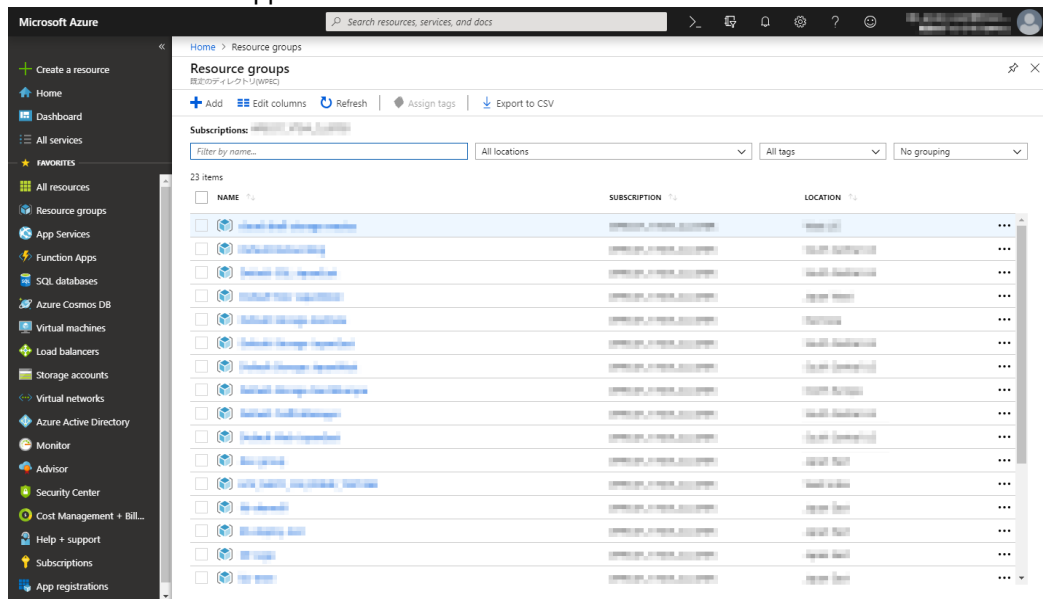
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create a resource group following the steps below.

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.

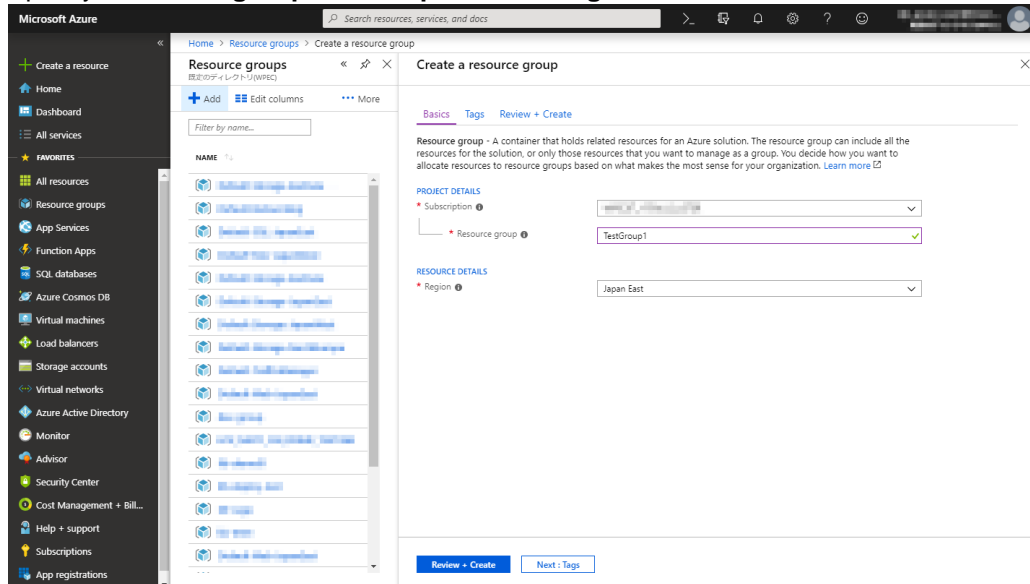


## Cluster Creation Procedure (for an HA Cluster Using an Public Load Balancer)

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



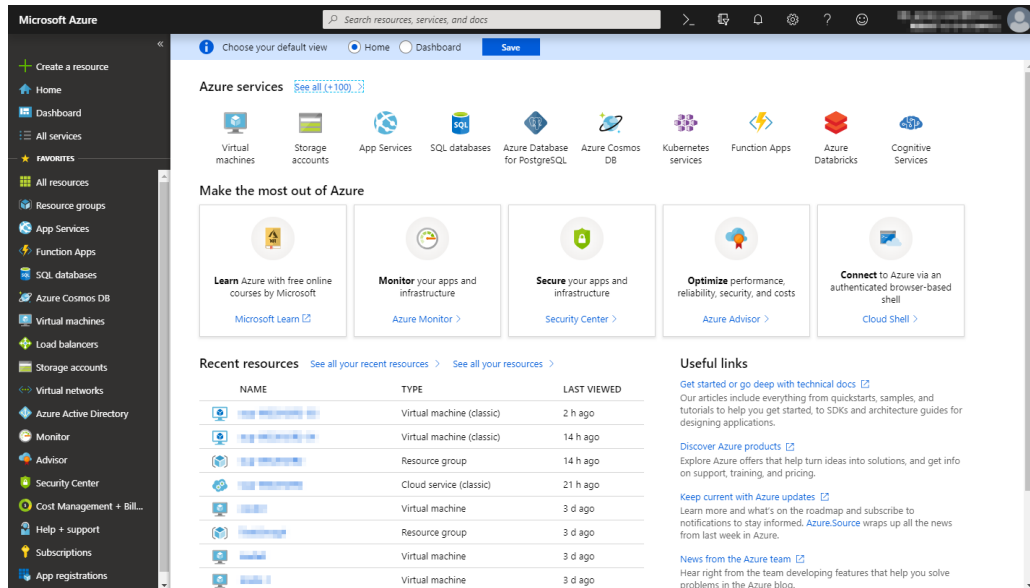
3. Specify **Resource group**, **Subscription**, and **Region**, and click **Review+Create**.



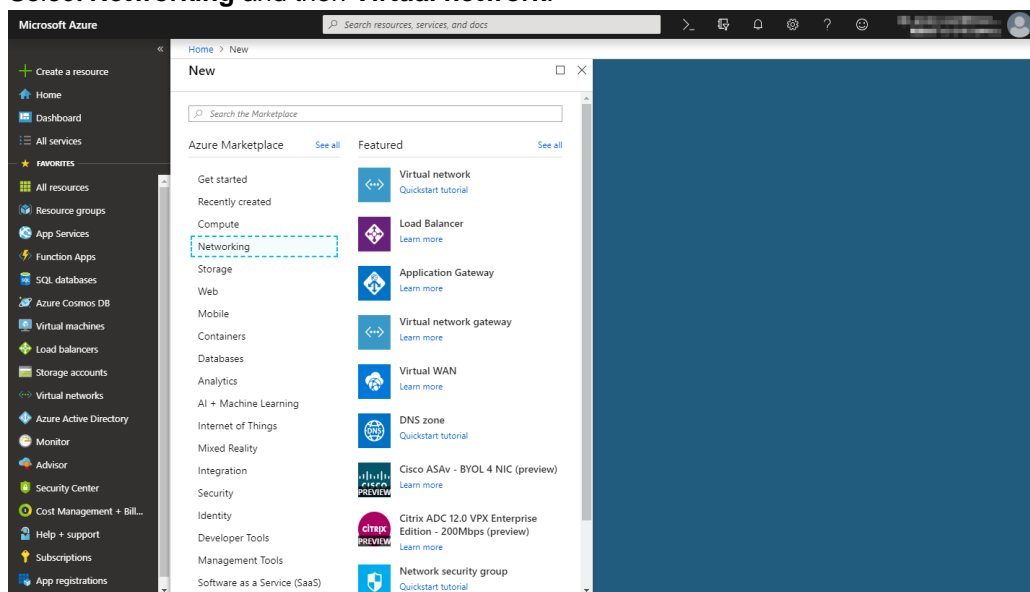
## 2) Creating a virtual network

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

1. Select **+Create a resource** 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**, **Location**, **Name** of Subnet, and **Address range**, and click **Create**.

The screenshot shows the 'Create virtual network' wizard in the Microsoft Azure portal. The left sidebar contains the navigation menu with 'Virtual networks' highlighted. The main pane displays the configuration form for a new virtual network. The form fields are as follows:

- Name:** Vnet1
- Address space:** 10.5.0.0/16 (10.5.0.0 - 10.5.255.255 (65536 addresses))
- Subscription:** [selected]
- Resource group:** TestGroup1
- Location:** Japan East
- Subnet:**
  - Name:** Vnet1-1
  - Address range:** 10.5.0.0/24 (10.5.0.0 - 10.5.0.255 (256 addresses))
- DDoS protection:** Basic (selected), Standard (unselected)
- Service endpoints:** Disabled (selected), Enabled (unselected)
- Firewall:** Disabled (selected), Enabled (unselected)

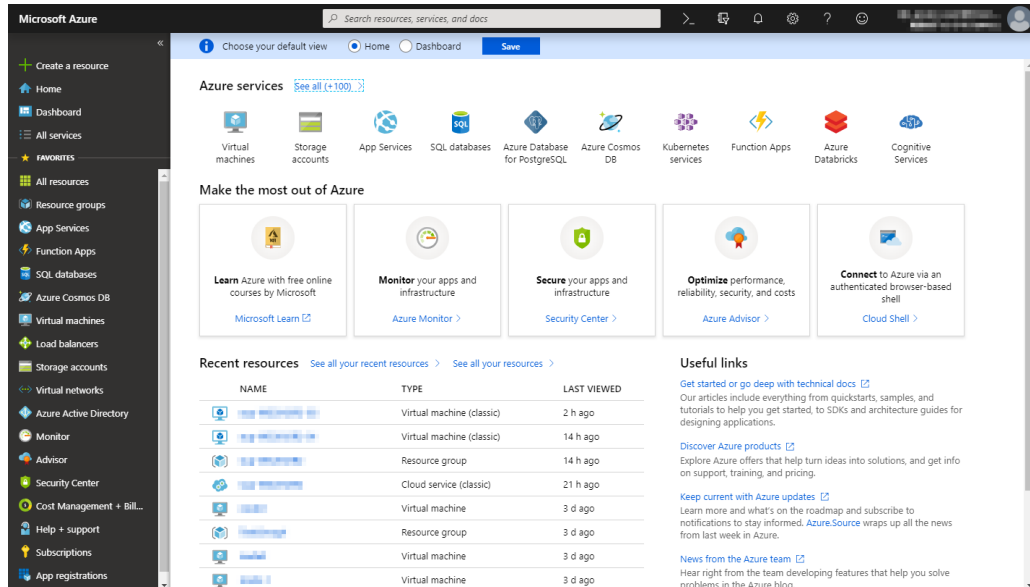
At the bottom of the form, there is a 'Create' button and a link to 'Automation options'.

### 3) Creating a virtual machine

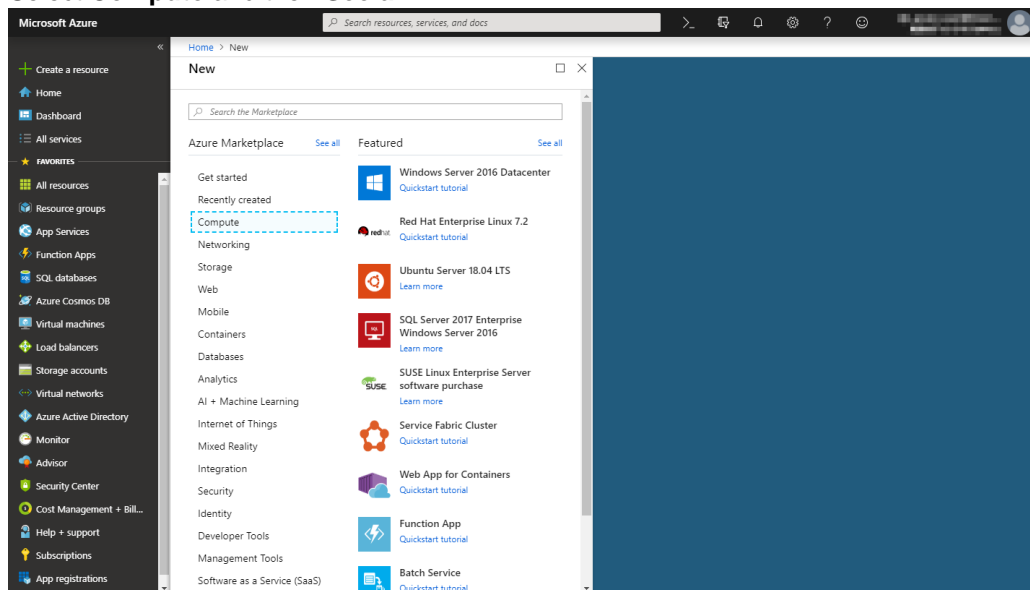
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create virtual machines and disks following the steps below.

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

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



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



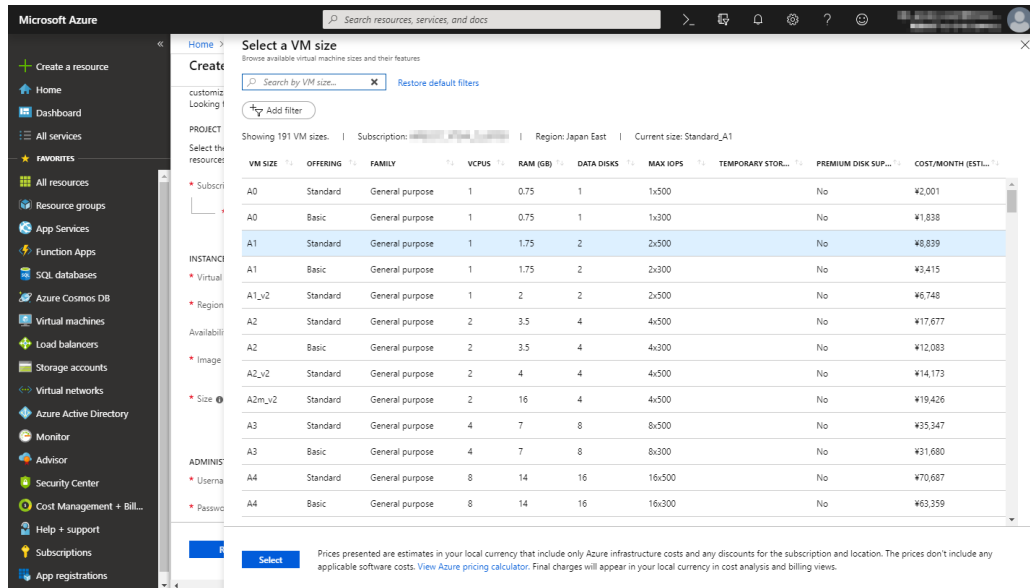
## Cluster Creation Procedure (for an HA Cluster Using an Public Load Balancer)

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

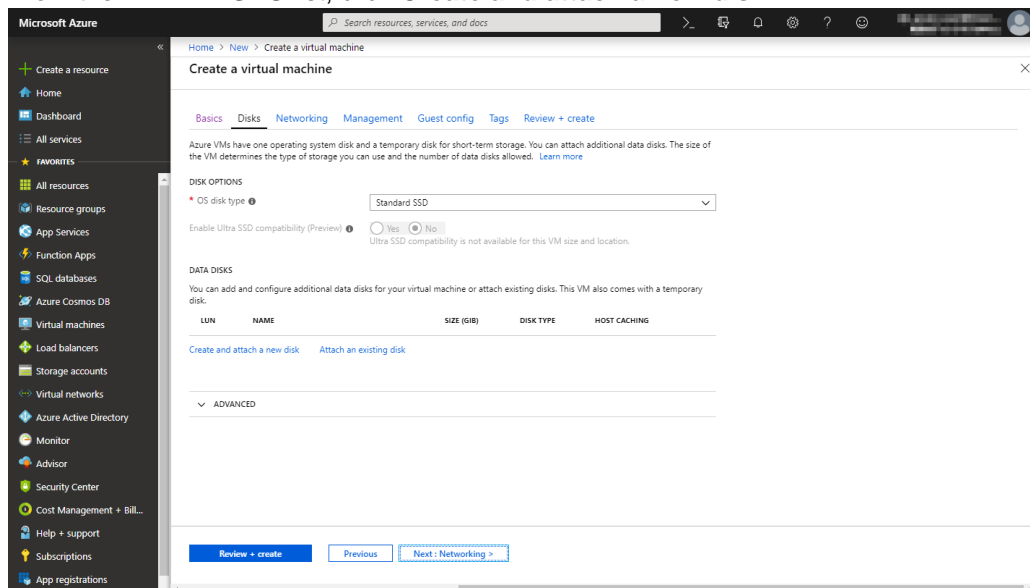
The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal, specifically the 'Basics' tab. The left sidebar contains navigation links for 'Create a resource', 'Home', 'Dashboard', 'All services', and 'FAVORITES'. The main content area is titled 'Create a virtual machine' and includes tabs for 'Basics', 'Disks', 'Networking', 'Management', 'Guest config', 'Tags', and 'Review + create'. Below the tabs, there is a brief description of creating a VM and a link to 'Create VM from Azure Marketplace'. The 'PROJECT DETAILS' section includes fields for 'Subscription' (selected), 'Resource group' (TestGroup1), and a 'Create new' link. The 'INSTANCE DETAILS' section includes fields for 'Virtual machine name' (node-1), 'Region' (Japan East), 'Availability options' (Availability set), 'Availability set' ((new) AvailabilitySet-1), 'Image' (Windows Server 2016 Datacenter), and 'Size' (Standard A1). At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next: Disks >'. The URL at the bottom of the browser window is 'https://portal.azure.com/?l=en-us#f'.

The screenshot shows the 'Create new' blade for an availability set in the Microsoft Azure portal. The left sidebar is the same as the previous screenshot. The main content area is titled 'Create new' and includes a description of creating an availability set. The 'PROJECT DETAILS' section includes fields for 'Subscription' (selected), 'Resource group' (TestGroup1), and a 'Create new' link. The 'INSTANCE DETAILS' section includes fields for 'Virtual machine name' (node-1), 'Region' (Japan East), 'Availability options' (Availability set), 'Availability set' (No existing availability sets in current resource group and location), 'Image' (Windows Server 2016 Datacenter), and 'Size' (Standard A1). At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next: Disks >'. The 'Create new' section on the right includes a 'Name' field (AvailabilitySet-1), a 'Fault domains' slider (set to 2), an 'Update domains' slider (set to 5), and a 'Use managed disks' section with radio buttons for 'No (Classic)' and 'Yes (Aligned)'. An 'OK' button is at the bottom right. The URL at the bottom of the browser window is 'https://portal.azure.com/?l=en-us#f'.

- Click **Change size** to display the **Select a VM size** blade. From the list, choose a size (**A1 - Standard** in this guide) suitable for your virtual machine and click **Select**. Regarding the **Virtual machine name**, node-1 is for node-1, and node-2 is for node-2. Click **Next: Disks** >



- When the **Disks** tab appears, go through the following steps to add a blob to be used for a mirror disk (cluster partition or data partition). From the **DATA DISKS** list, click **Create and attach a new disk**.





7. The **Create a new disk** blade appears. Specify the settings of **Disk type**, **Name**, **Size (GiB)**, and **Source type**. Then click **OK**. Click **Next: Networking >**.

Microsoft Azure

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

### Create a new disk

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

- Disk type: Standard HDD
- Name: node-1blob1
- Size (GiB):
- Source type: None (empty disk)

ESTIMATED PERFORMANCE

IOPS limit: 500

Throughput limit (MB/s): 60

OK

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

Microsoft Azure

Home > New > Create a virtual machine > Create network security group

### Create network security group

Guest config Tags Review + create

By configuring network interface card (NIC) settings, you can control ports, inbound and outbound traffic, and place behind an existing load balancing solution. [Learn more](#)

will be created for you.

new

-1 (10.0.0.0/24)

subnet configuration

new

Basic Advanced

node-1-nsg

new

Off

The selected VM size does not support accelerated networking.

of an existing Azure load balancing solution. [Learn more](#)

No

Next: Management >

OK

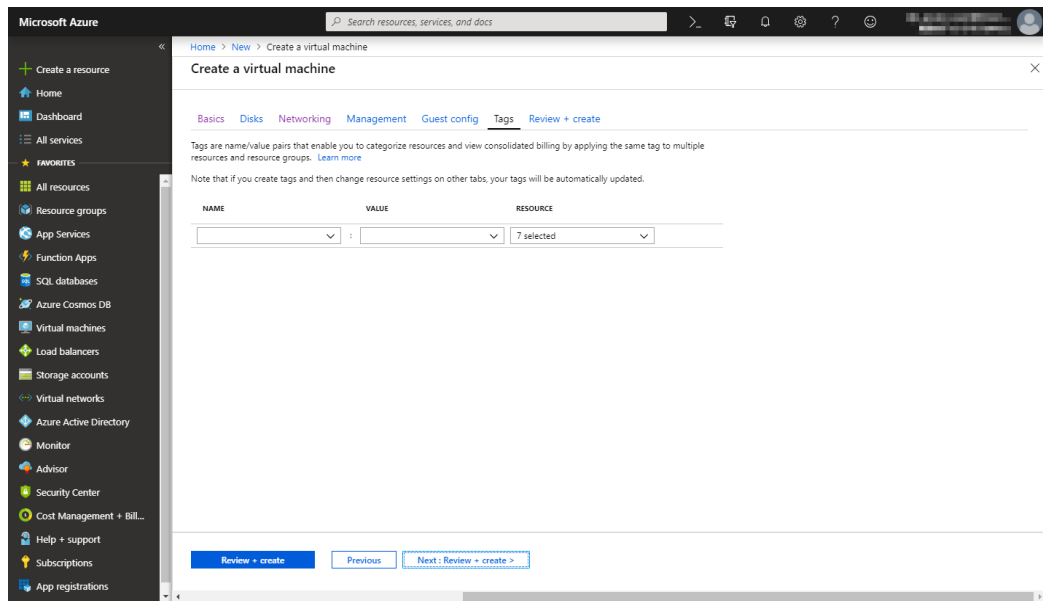
9. The **Management** tab appears.  
Click **Create new** under the **Diagnostics storage account** field to display the **Create storage account** blade.  
Specify the settings of **Name**, **Account kind**, and **Replication**. Then click **OK**.  
In the **Diagnostics storage account** field, the default value is automatically generated and entered.  
Click Next: **Guest config** >.

The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal, specifically the 'Management' tab. The 'Diagnostics storage account' field is set to '(new) testgroup1diag210'. The 'Create storage account' blade is open on the right, showing settings for Name, Account kind, Performance, and Replication. The 'Next: Guest config >' button is visible at the bottom of the main blade.

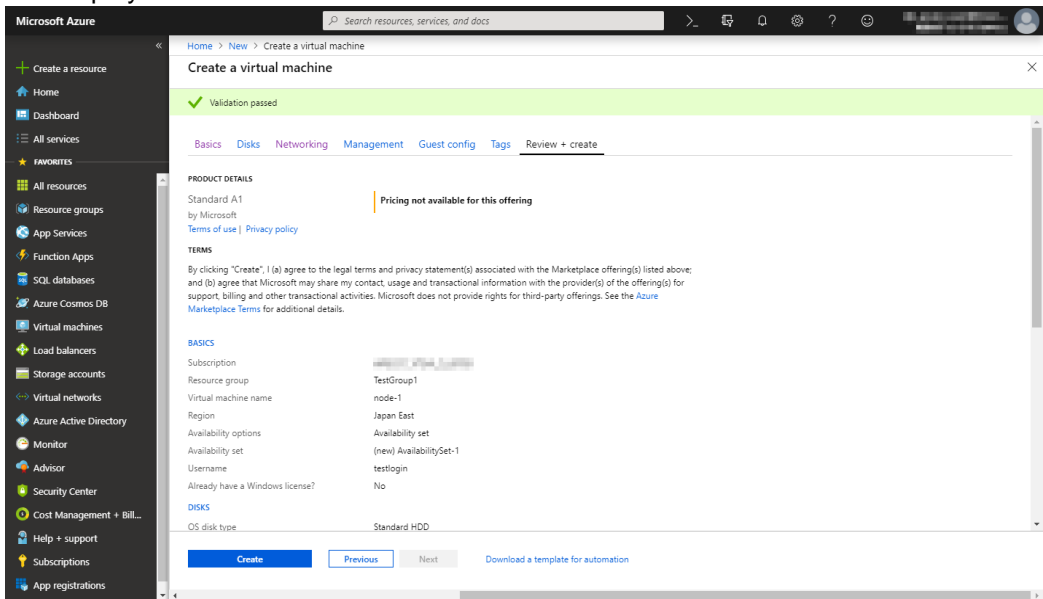
10. Click Next: **Tags** >.

The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal, specifically the 'Tags' tab. The 'Tags' tab is selected, and the 'Next: Tags >' button is visible at the bottom.

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



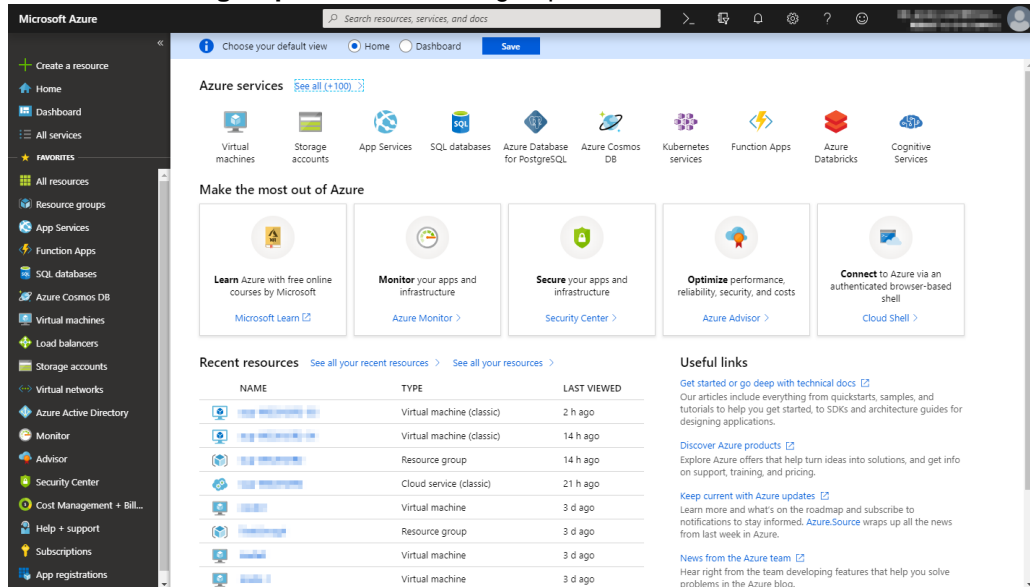
12. The **Review + create** tab appears. Check the contents. If there is no problem, click **Create**. The deployment starts and takes several minutes.



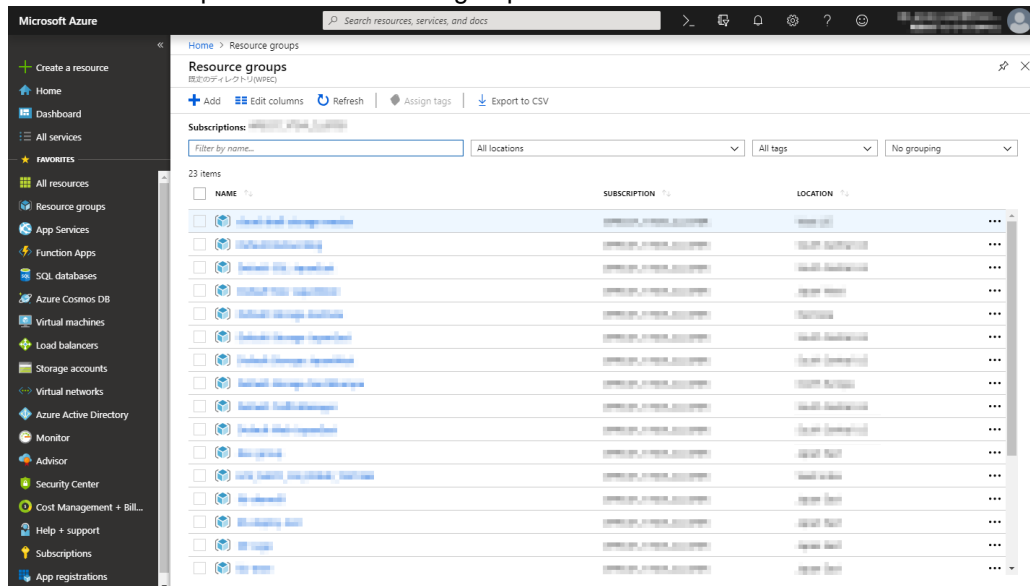
#### 4) Setting a private IP address

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

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

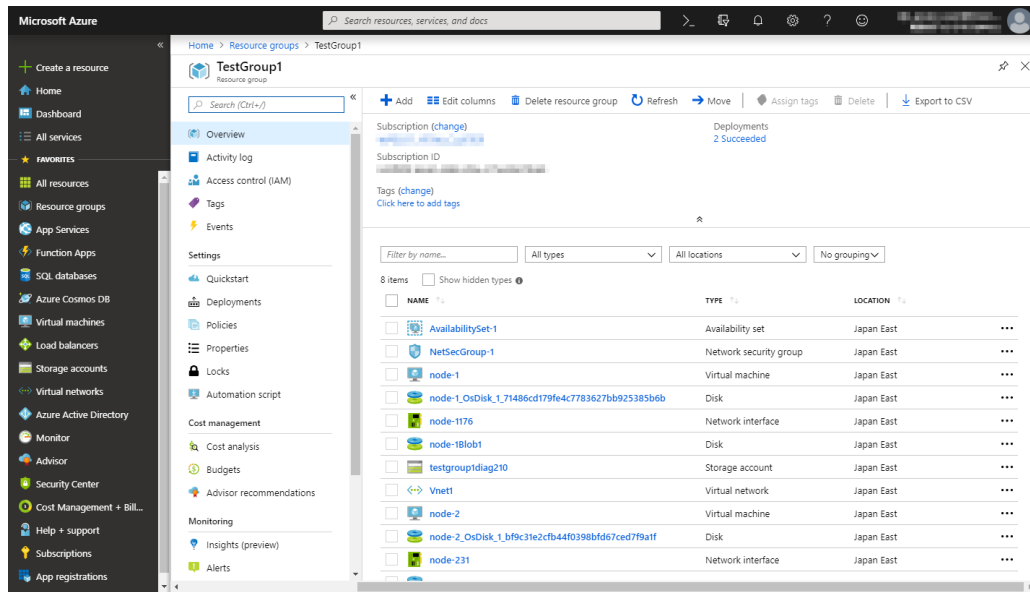


2. Select **TestGroup1** from the resource group list.

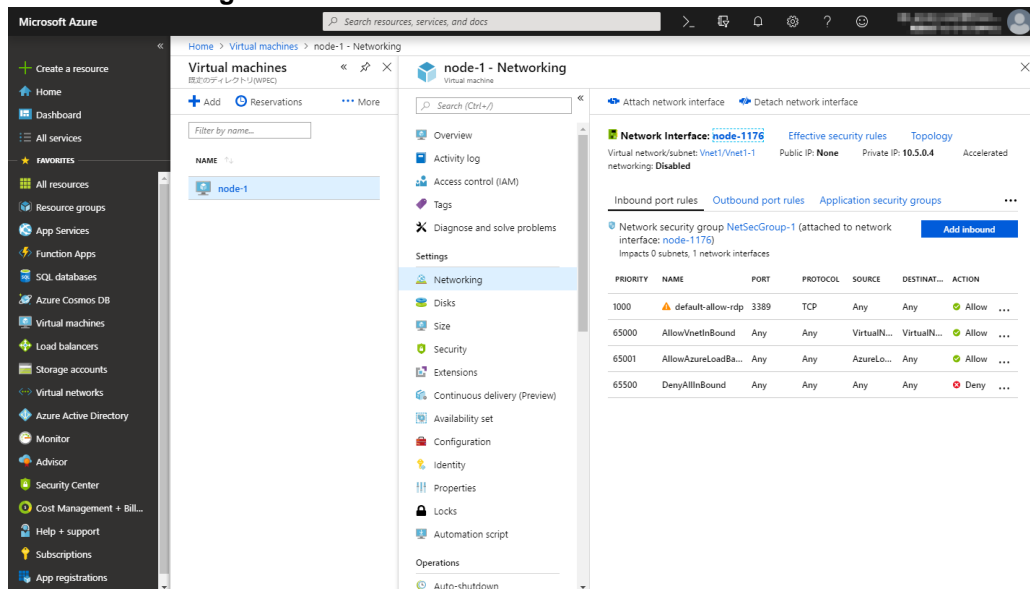


## Cluster Creation Procedure (for an HA Cluster Using an Public Load Balancer)

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

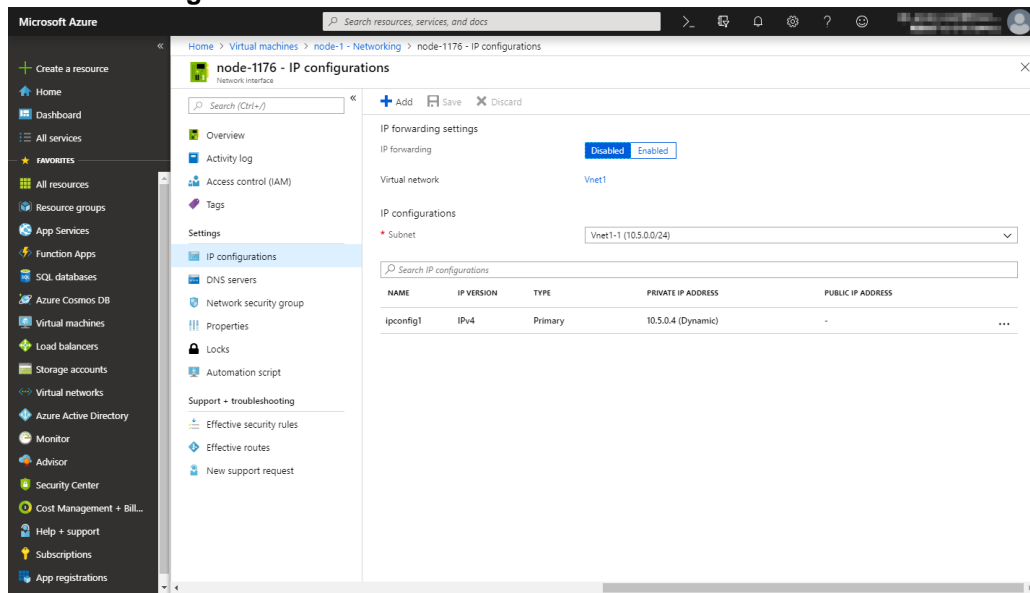


4. Select Networking.



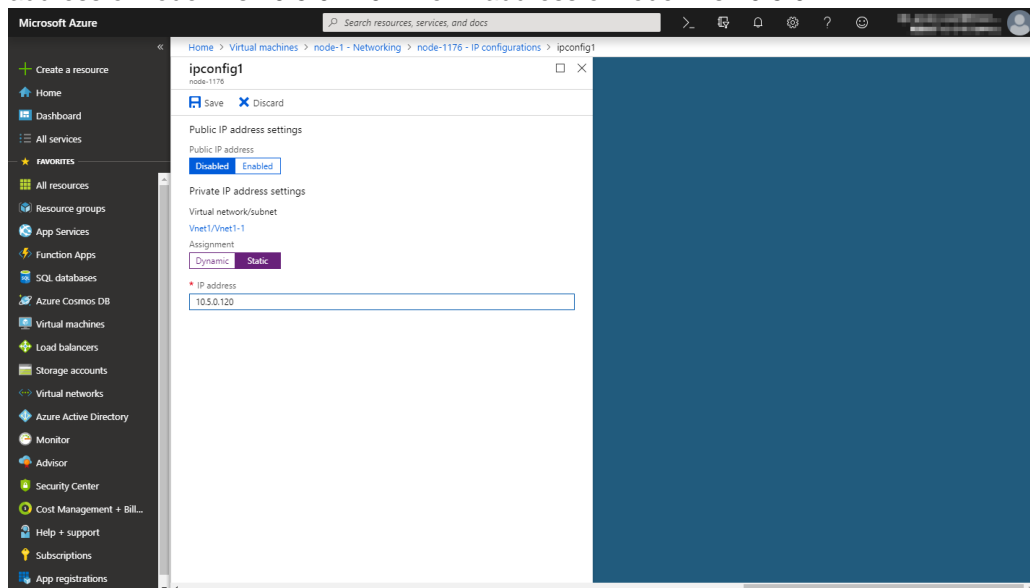
5. Select a network interface displayed in the list. The network interface name is generated automatically.

6. Select **IP configurations**.



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

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

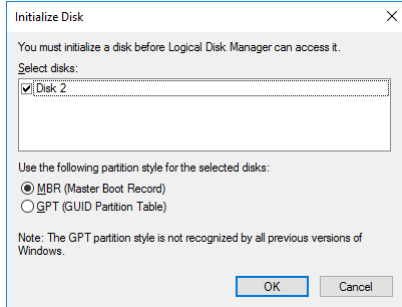


9. The virtual machines restart automatically so that new private IP addresses can be used.

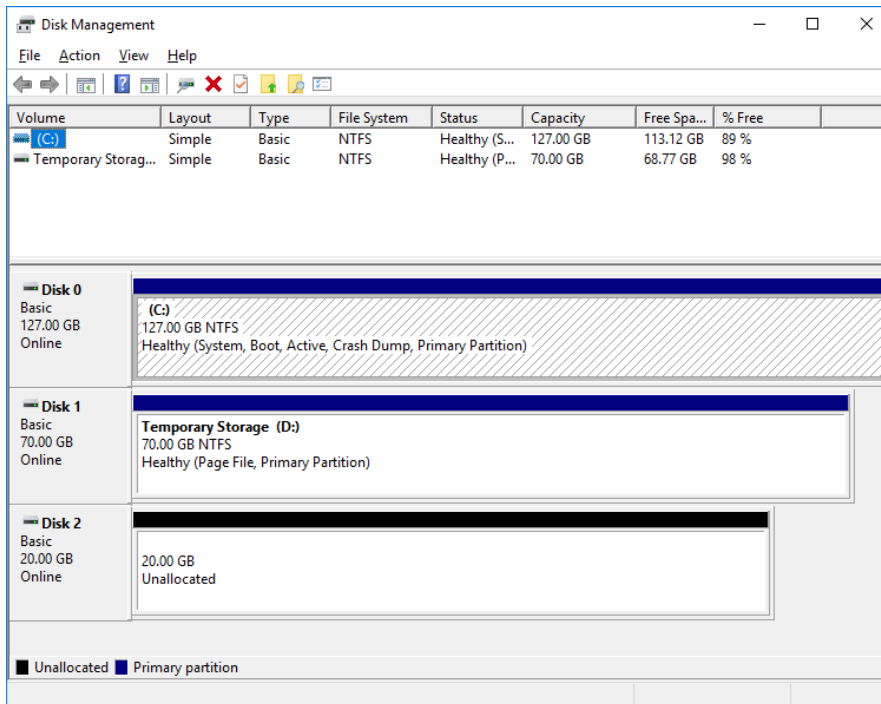
## 5) Configuring virtual machines

Log in to the created node-1 and node-2 and specify the settings following the procedure below. Set a partition for the mirror disk resource. Create a file system in the added Blob storage. For details about a partition for the mirror disk resource, see "Partition settings for mirror disk resource (when using Replicator)" in "Settings after configuring hardware" in Chapter 1, "Determining a system configuration" in the *Installation and Configuration Guide*.

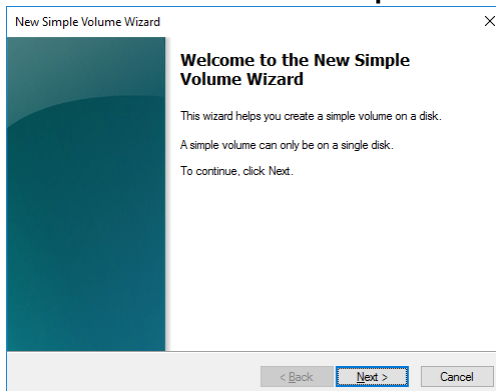
1. Open the **Disk Management** window. The **Initialize Disk** dialog box is displayed.



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



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



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

The screenshot shows the 'Specify Volume Size' step of the 'New Simple Volume Wizard'. The window title is 'New Simple Volume Wizard'. Below the title bar, the section is 'Specify Volume Size' with the instruction 'Choose a volume size that is between the maximum and minimum sizes.' The main area contains three labels: 'Maximum disk space in MB:' with a value of 20477, 'Minimum disk space in MB:' with a value of 8, and 'Simple volume size in MB:' with a text box containing '1024' and a spinner control. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

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

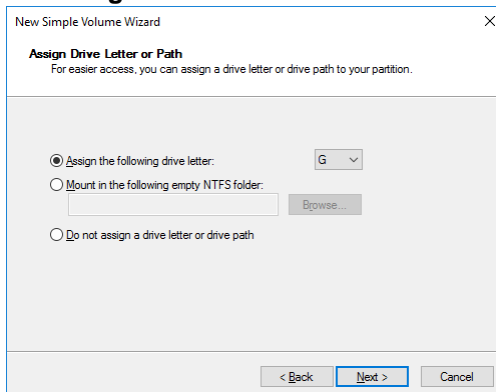
The screenshot shows the 'Assign Drive Letter or Path' step of the 'New Simple Volume Wizard'. The window title is 'New Simple Volume Wizard'. Below the title bar, the section is 'Assign Drive Letter or Path' with the instruction 'For easier access, you can assign a drive letter or drive path to your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

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

The screenshot shows the 'Specify Volume Size' step of the 'New Simple Volume Wizard'. The window title is 'New Simple Volume Wizard'. Below the title bar, the section is 'Specify Volume Size' with the instruction 'Choose a volume size that is between the maximum and minimum sizes.' The main area contains three labels: 'Maximum disk space in MB:' with a value of 19453, 'Minimum disk space in MB:' with a value of 8, and 'Simple volume size in MB:' with a text box containing '19453' and a spinner control. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

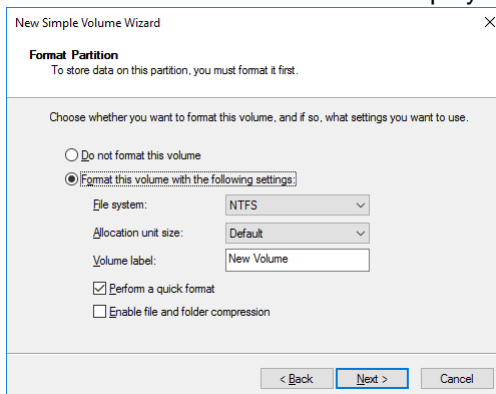


10. The **Assign Drive Letter or Path** window is displayed. Select the G drive for **Assign the following drive letter:** and click **Next**.



The screenshot shows the 'Assign Drive Letter or Path' step of the New Simple Volume Wizard. The title bar reads 'New Simple Volume Wizard'. The main heading is 'Assign Drive Letter or Path' with a subtitle 'For easier access, you can assign a drive letter or drive path to your partition.' There are three radio button options: 'Assign the following drive letter:' (selected), 'Mount in the following empty NTFS folder:', and 'Do not assign a drive letter or drive path'. The first option has a dropdown menu showing 'G'. Below the second option is a text box and a 'Browse...' button. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

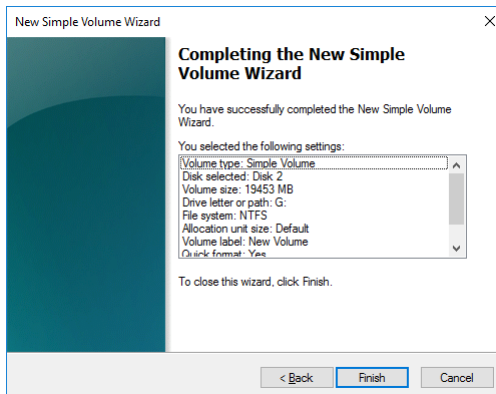
11. The **Format Partition** window is displayed. Confirm that **File system** is **NTFS**.



The screenshot shows the 'Format Partition' step of the New Simple Volume Wizard. The title bar reads 'New Simple Volume Wizard'. The main heading is 'Format Partition' with a subtitle 'To store data on this partition, you must format it first.' Below this is the instruction 'Choose whether you want to format this volume, and if so, what settings you want to use.' There are two radio button options: 'Do not format this volume' and 'Format this volume with the following settings:' (selected). Under the second option, there are settings for 'File system:' (NTFS), 'Allocation unit size:' (Default), and 'Volume label:' (New Volume). There are also checkboxes for 'Perform a quick format' (checked) and 'Enable file and folder compression' (unchecked). At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

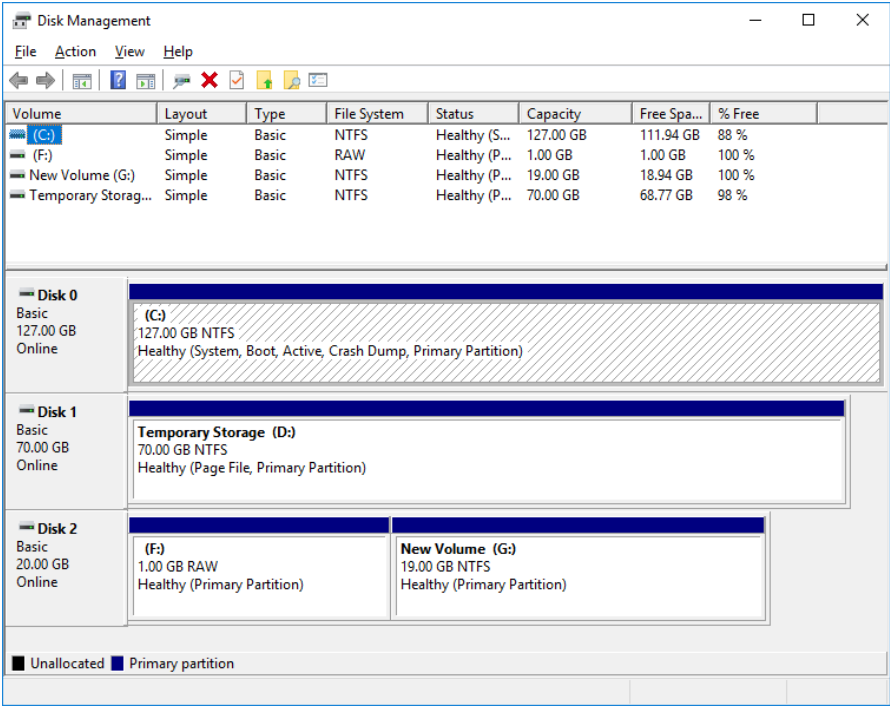
12. Click **Next**.

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



The screenshot shows the 'Completing the New Simple Volume Wizard' step. The title bar reads 'New Simple Volume Wizard'. The main heading is 'Completing the New Simple Volume Wizard'. The text says 'You have successfully completed the New Simple Volume Wizard.' Below this is a list of settings: 'Volume type: Simple Volume', 'Disk selected: Disk 2', 'Volume size: 19453 MB', 'Drive letter or path: G:', 'File system: NTFS', 'Allocation unit size: Default', 'Volume label: New Volume', and 'Quick format: Yes'. At the bottom is the instruction 'To close this wizard, click Finish.' and buttons for '< Back', 'Finish', and 'Cancel'.

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



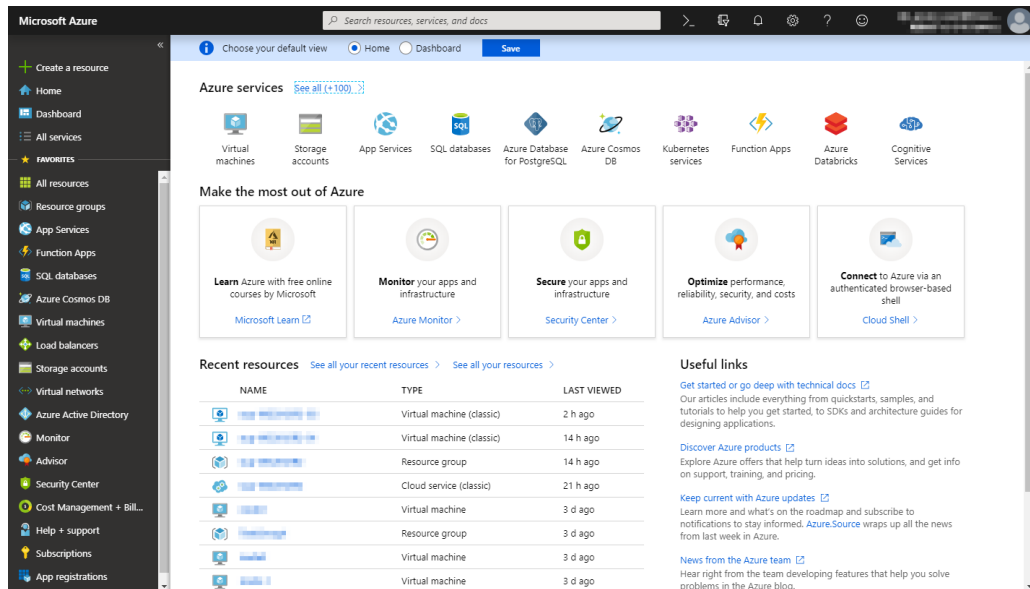
### 6) Configuring a load balancer

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

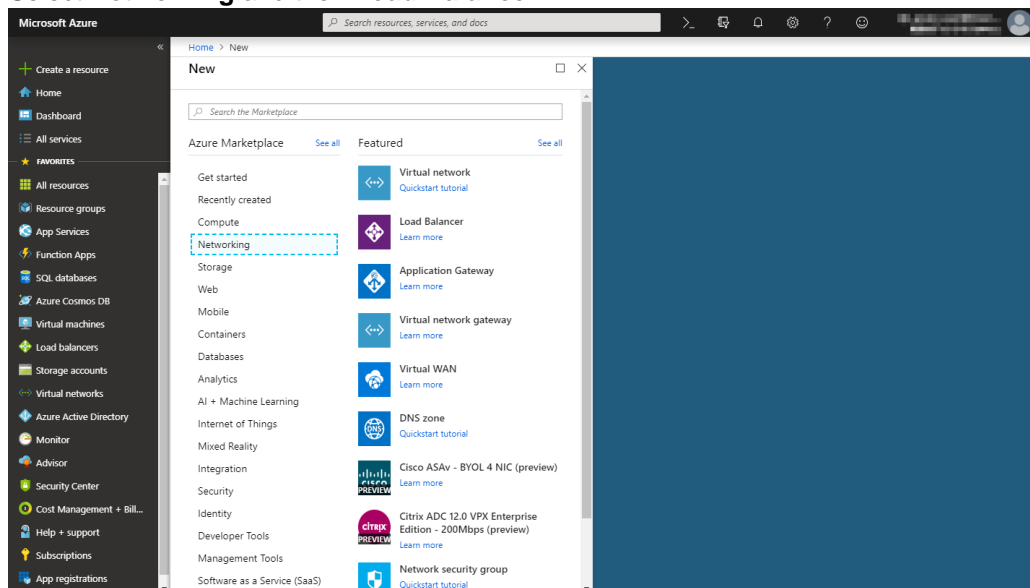
For details, see the following websites:

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

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



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



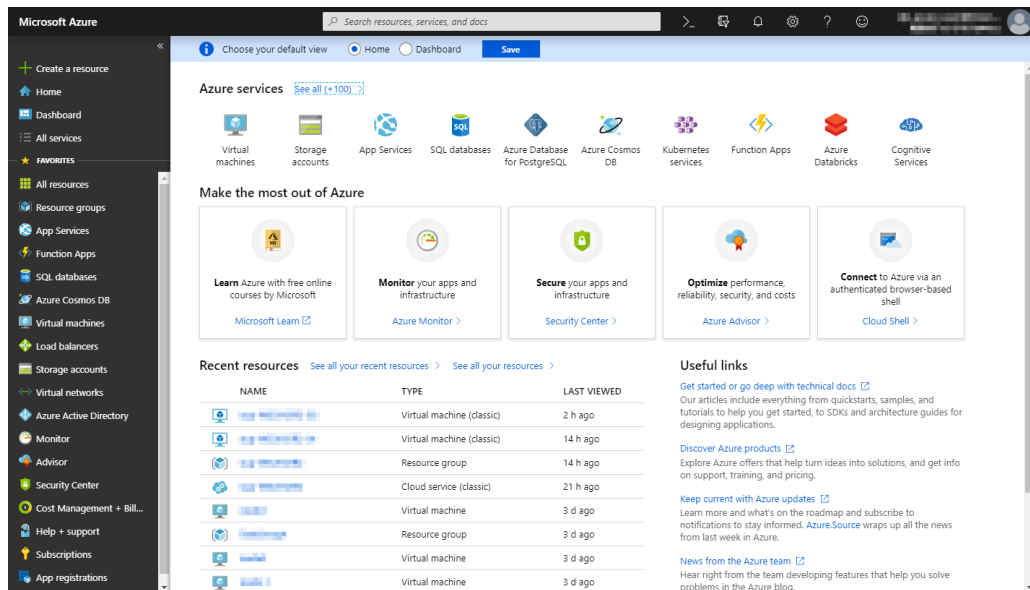
3. The **Create load balancer** blade is displayed. Specify **Name**. Select **Public** for **Type** and **Basic** for **SKU**, respectively.
4. Specify **Create new**, **Name** and **Assignment** for **Public IP address**.

5. Specify **Subscription**, **Resource group**, and **Region**, and click **Review+create**. Deploying the load balancer starts. This processing takes several minutes.

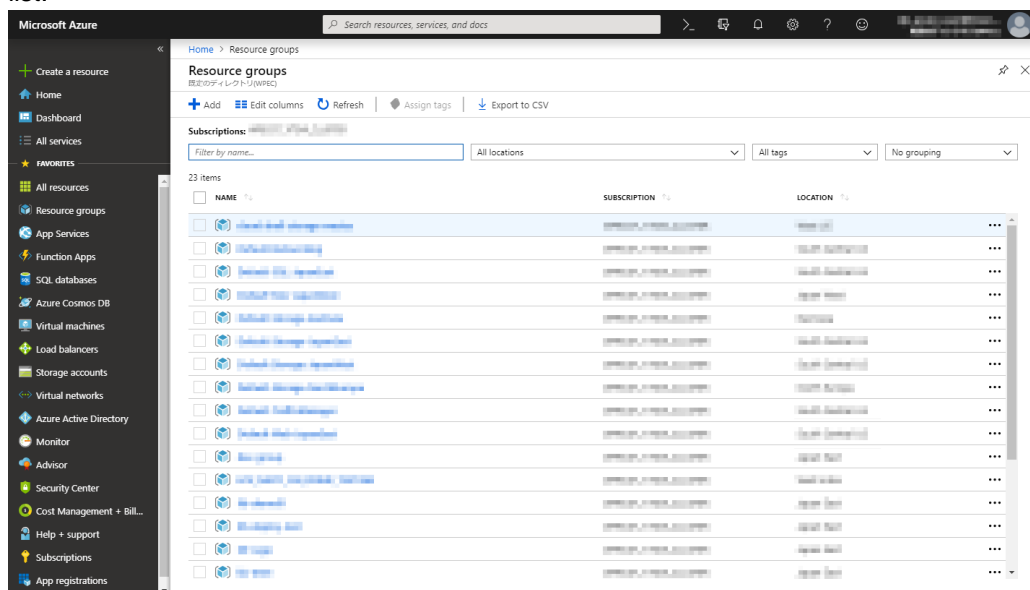
The screenshot shows the 'Create load balancer' wizard in the Microsoft Azure portal. The left sidebar contains navigation links for 'Create a resource', 'Home', 'Dashboard', 'All services', and 'FAVORITES' (All resources, Resource groups, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Bill..., Help + support, Subscriptions, App registrations). The main content area is titled 'Create load balancer' and includes tabs for 'Basics', 'Tags', and 'Review + create'. A descriptive paragraph explains that an Azure load balancer is a layer 4 load balancer that distributes incoming traffic among healthy virtual machine instances. The 'Basics' tab is active and contains the following sections: 'PROJECT DETAILS' with dropdowns for 'Subscription' and 'Resource group' (set to 'TestGroup1'); 'INSTANCE DETAILS' with fields for 'Name' (set to 'TestLoadBalancer'), 'Region' (set to 'Japan East'), 'Type' (radio buttons for 'Internal' and 'Public', with 'Public' selected), and 'SKU' (radio buttons for 'Basic' and 'Standard', with 'Basic' selected); and 'PUBLIC IP ADDRESS' with radio buttons for 'Create new' and 'Use existing' (with 'Create new' selected), a text field for 'Public IP address name' (set to 'TestLoadBalancerPublicIP'), and a label for 'Public IP address SKU' (set to 'Basic'). At the bottom, there are buttons for 'Review + create', 'Previous', 'Next: Tags >', and a link to 'Download a template for automation'.

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

1. Associate a virtual machine registered to the availability set to the load balancer. After the load balancer has been deployed, select **Resource groups** 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 Delete Export to CSV

Subscription (change)  
Subscription ID  
Tags (change)  
Click here to add tags

Deployments  
4 Succeeded

Filter by name... All types All locations No grouping

9 items Show hidden types

NAME	TYPE	LOCATION
node-1	Virtual machine	Japan East
node-1_OsDisk_1_71486cd179fe4c7783627bb925385b6b	Disk	Japan East
node-1176	Network interface	Japan East
node-18lob1	Disk	Japan East
node-2	Virtual machine	Japan East
node-2_OsDisk_1_bf9c31e2cfb44f0398bf6d67ced7f9a1f	Disk	Japan East
node-231	Network interface	Japan East
node-28lob1	Disk	Japan East
testgroupdiag210	Storage account	Japan East
TestLoadBalancer	Load balancer	Japan East
Vnet1	Virtual network	Japan East

4. Select Backend pools.

Microsoft Azure

Home > Resource groups > TestGroup1 > TestLoadBalancer

TestLoadBalancer  
Load balancer

Search (Ctrl+/)

Move Delete Refresh

Resource group (change)  
TestGroup1

Location  
Japan East

Subscription (change)  
Subscription ID

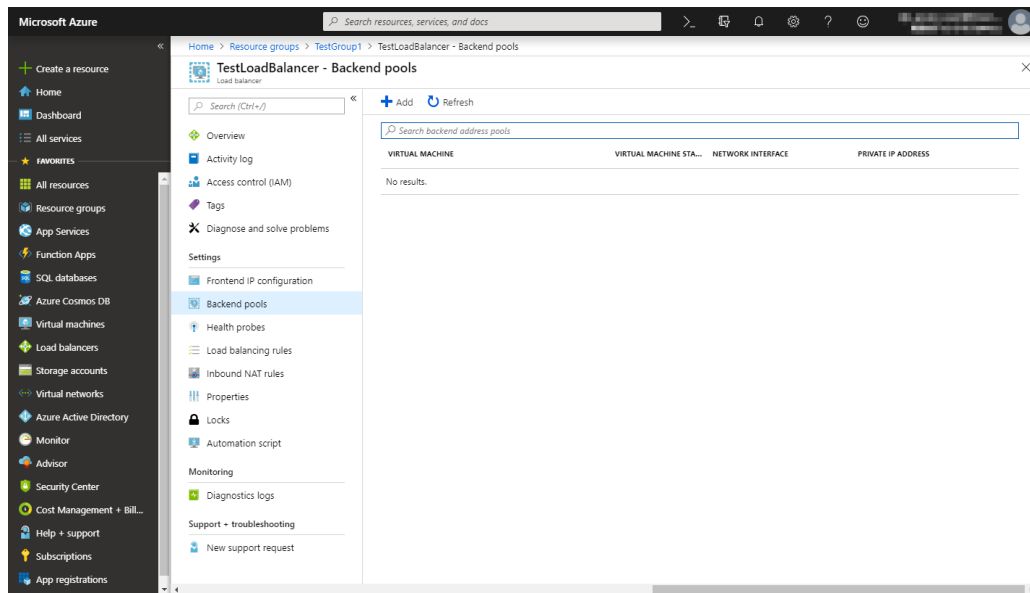
SKU  
Basic

Tags (change)  
Click here to add tags

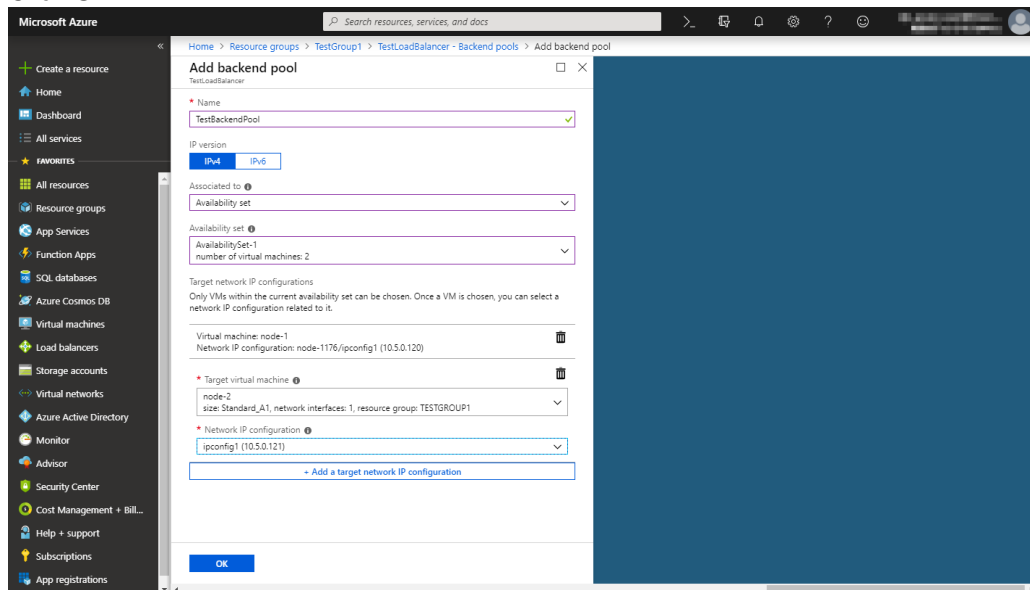
Backend pool  
Health probe  
Load balancing rule  
NAT rules  
0 inbound  
Public IP address  
(TestLoadBalancerPublicIP)

Frontend IP configuration  
Backend pools  
Health probes  
Load balancing rules  
Inbound NAT rules  
Properties  
Locks  
Automation script  
Monitoring  
Diagnostics logs  
Support + troubleshooting  
New support request

5. Click **Add**.

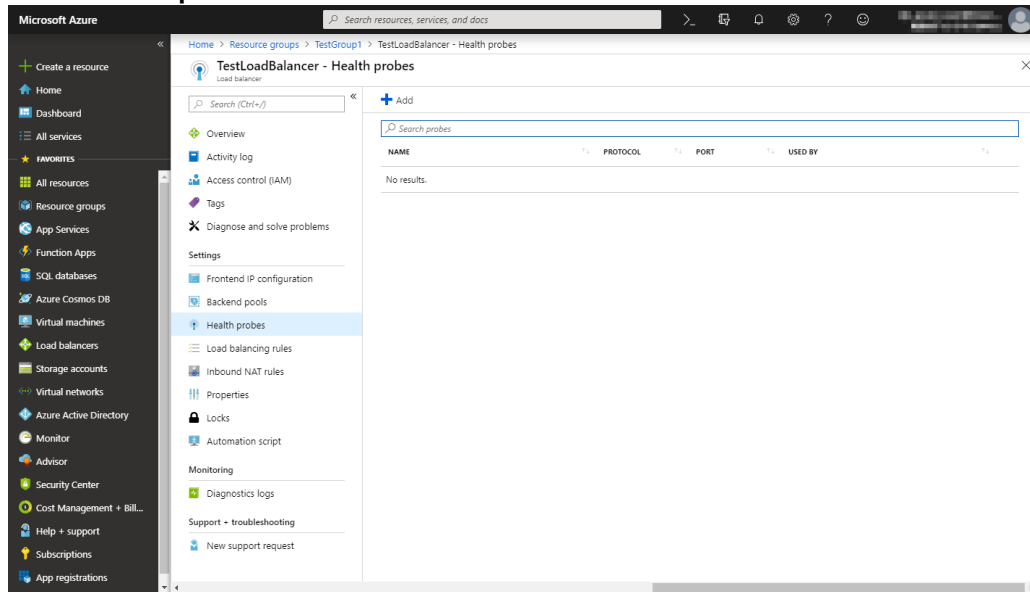


6. The **Add backend pool** blade is displayed. Specify **Name**.
7. For **Associated to**, select **Availability set**.
8. Specify **Availability set**.
9. Click **Add a target network IP configuration**.
10. Specify the target virtual machine for **Target virtual machine** and **Network IP configuration**.
11. Repeat steps 9 and 10 as many times as the number of target virtual machines.
12. Click **OK**.



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

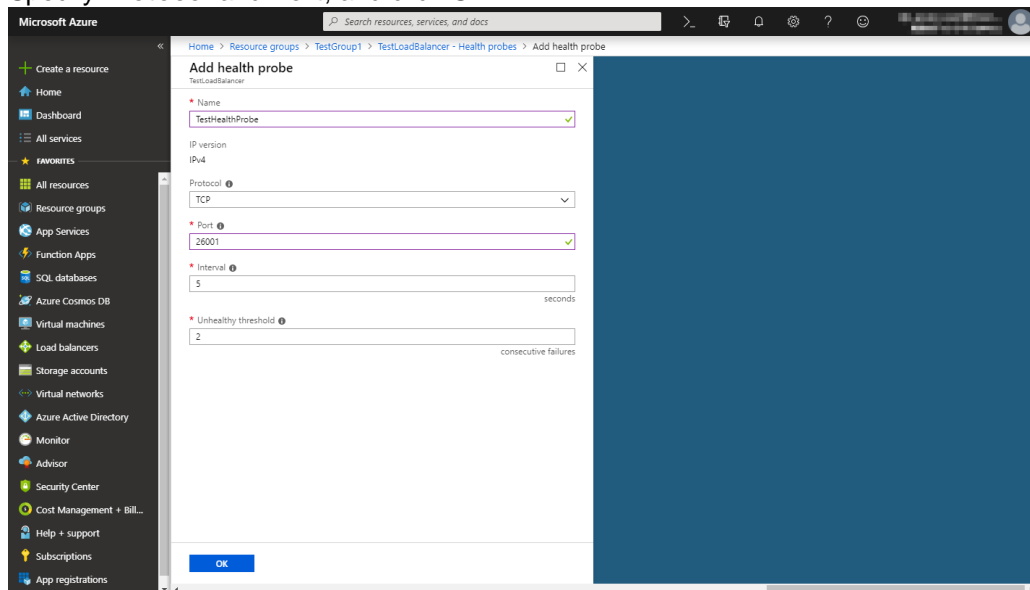
### 1. Select Health probes.



### 2. Click Add.

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

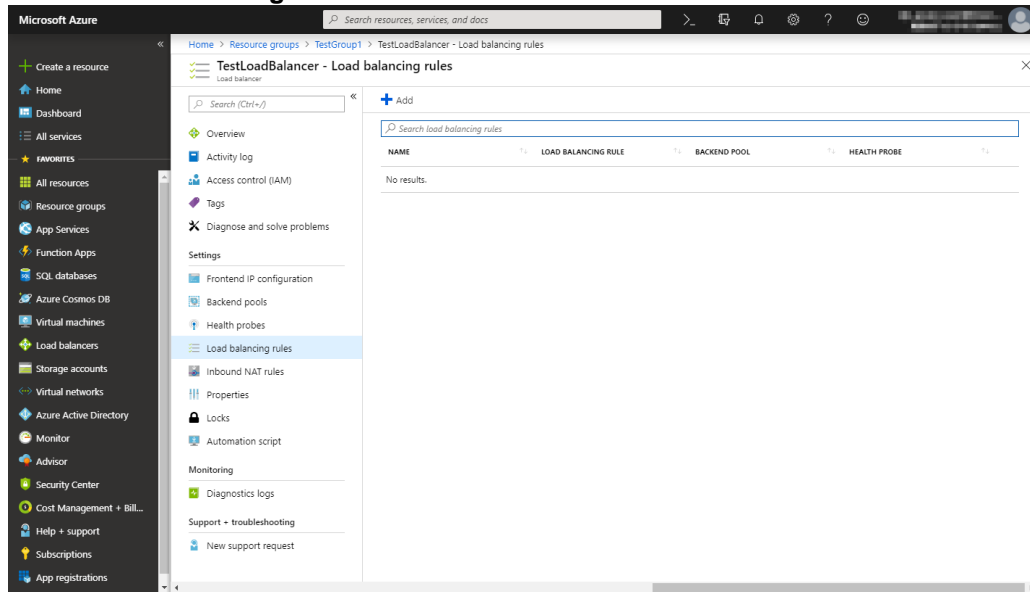
### 4. Specify Protocol and Port, and click OK.





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

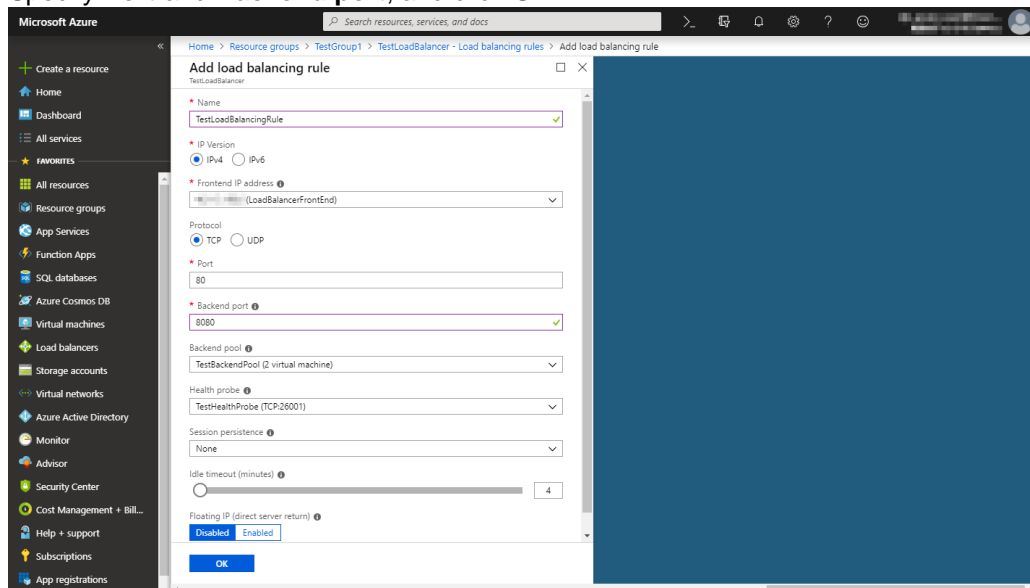
### 1. Select Load balancing rules.



### 2. Click **Add**.

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

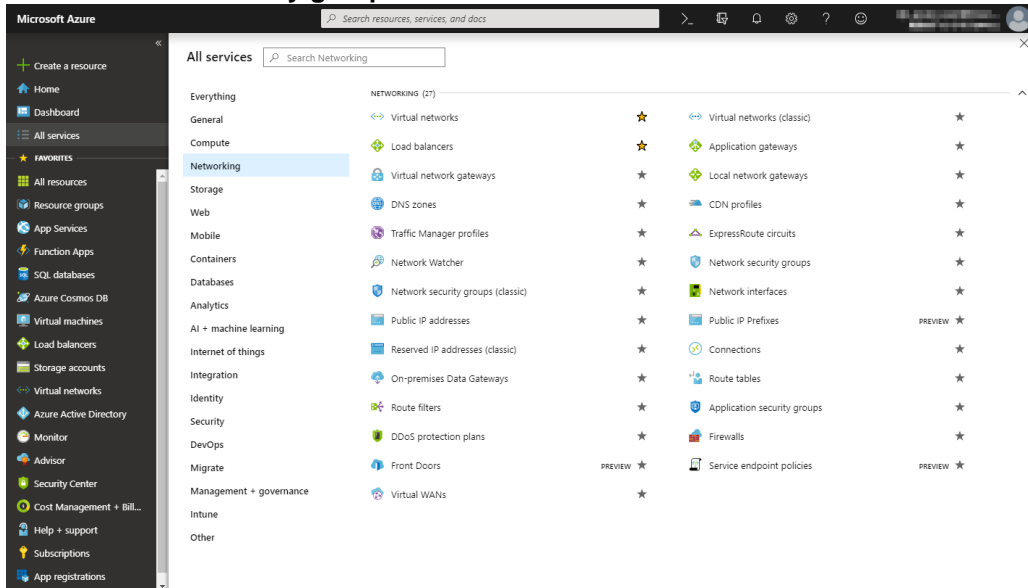
### 4. Specify **Port** and **Backend port**, and click **OK**.



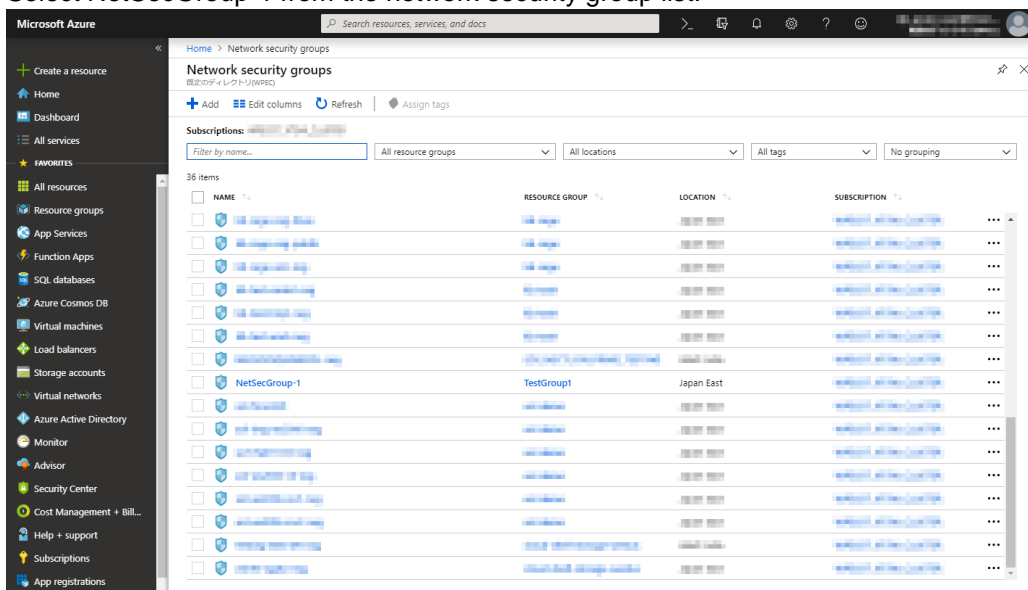
## 10) Setting the inbound security rules

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

1. Select **All services** in the menu on the left side of the window.
2. Select **Network security groups**.

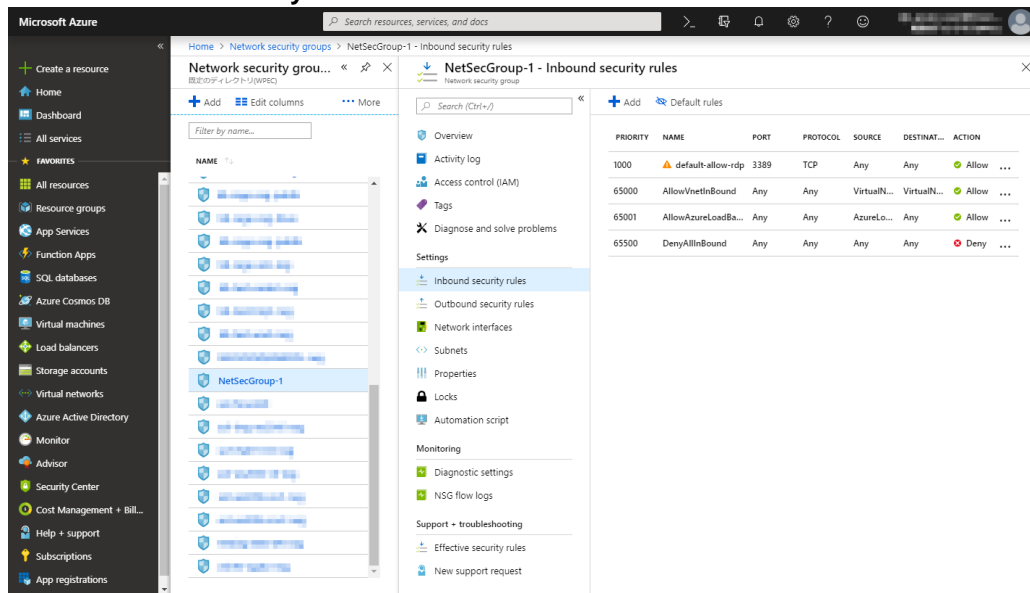


3. Select **NetSecGroup-1** from the network security group list.



4. The summary of **NetSecGroup-1** is displayed.

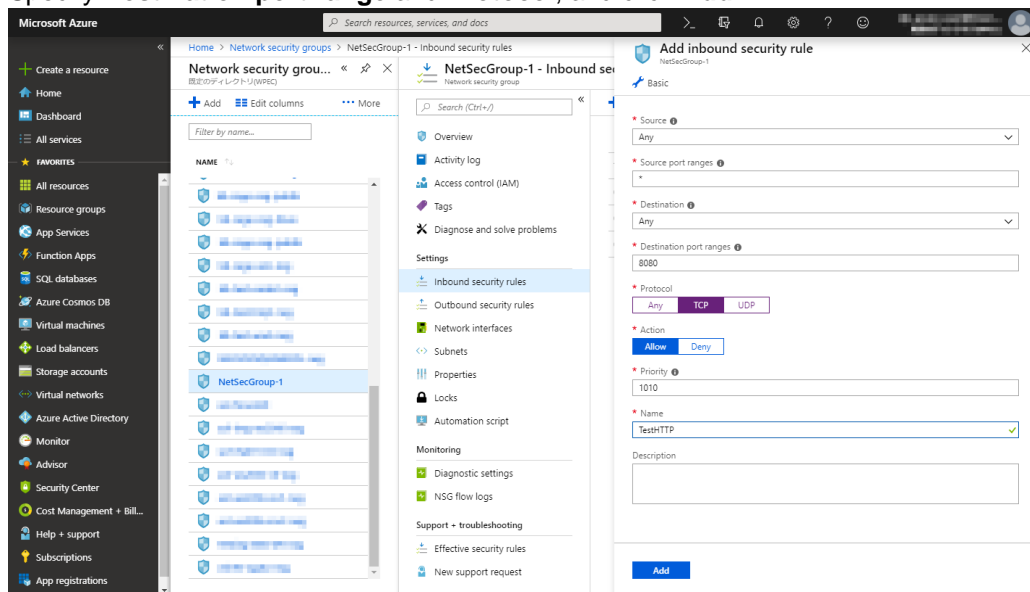
5. Select **Inbound security rules**.



6. Click **Add**.

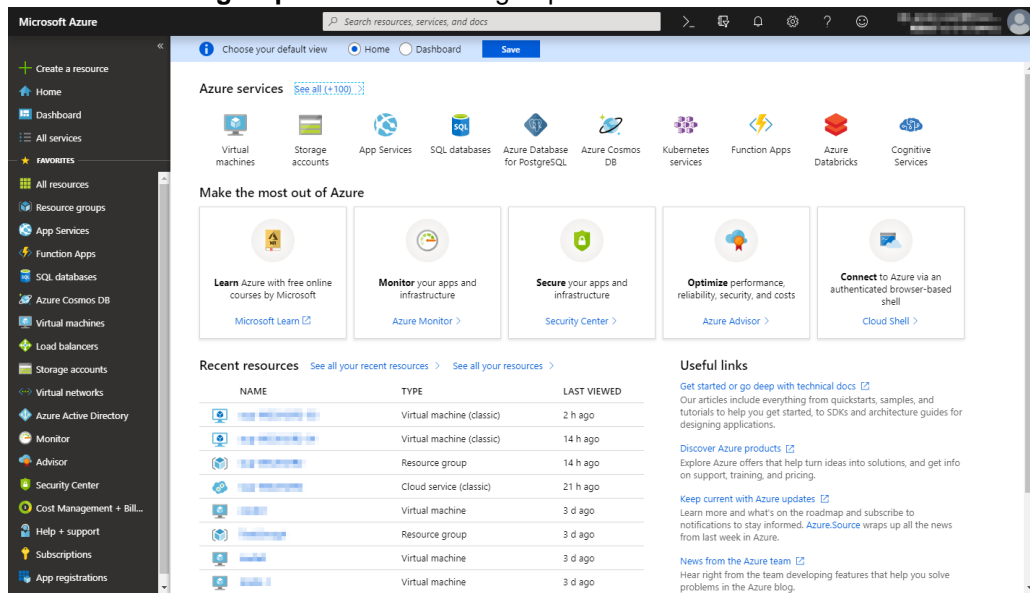
7. The **Add inbound security rule** blade is displayed. Specify **Name**.

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

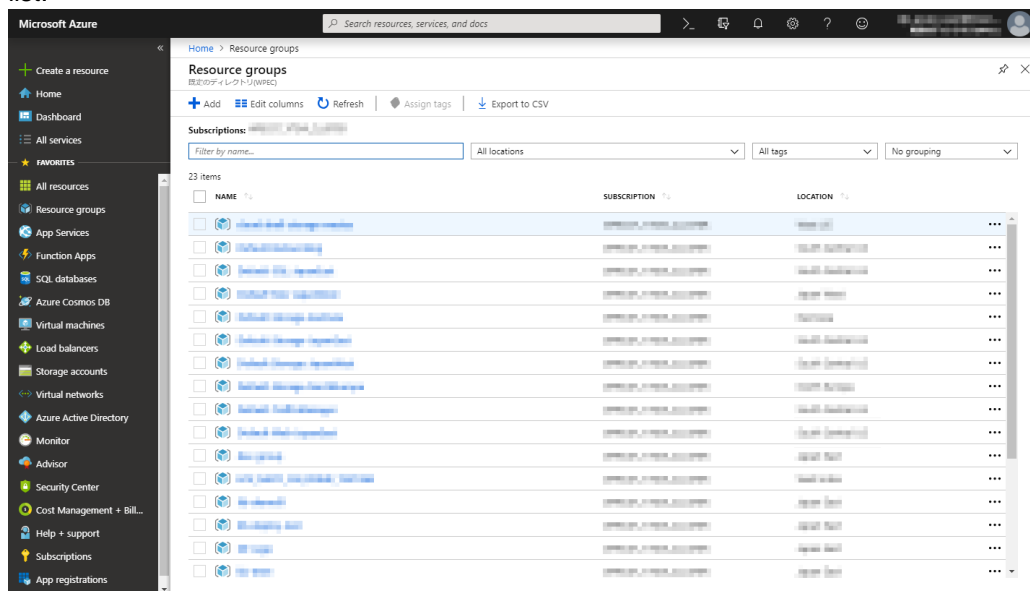


Then, check `<Load_balancer_frontend_IP(public_IP_address)>` specified in the script before recovery action of the multi target monitor resource that is set in "3) Adding a monitor resource." Write down the confirmatory result.

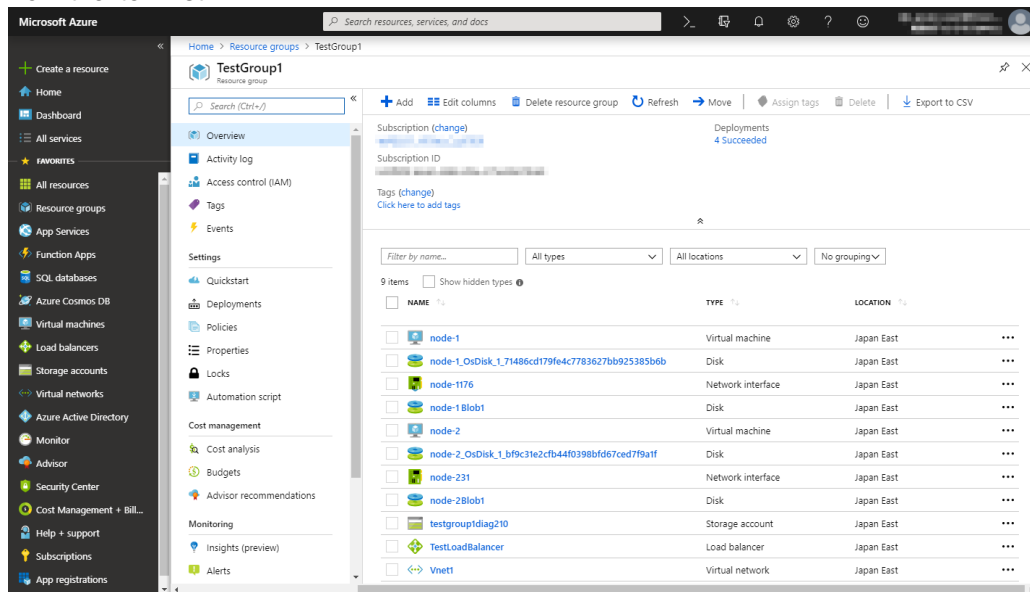
1. Select **Resource groups** or the resource group icon in the menu on the left side of the window.



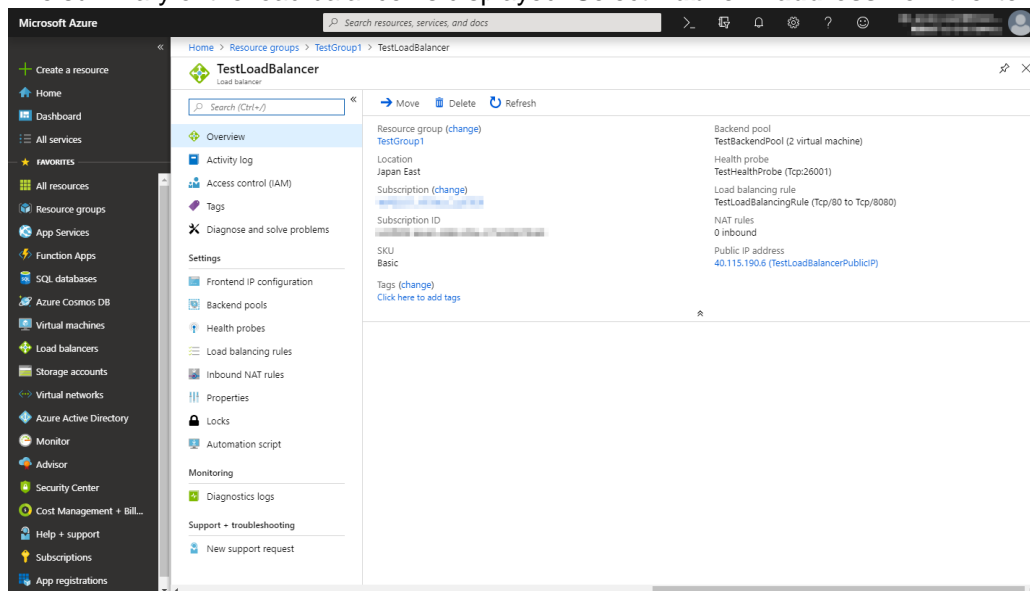
2. Select the resource group to which the created load balancer belongs from the resource group list.



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



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



- 11) **Adjusting the OS startup time, checking the network setting, checking the firewall setting, synchronizing the server time, and disabling the power saving function.**  
For each procedure, see "Settings after configuring hardware" in 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 EXPRESSCLUSER license

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

## 4.3 Configuring the EXPRESSCLUSTER settings

For the Cluster WebUI setup and connection procedures, see Chapter 5, "Creating the cluster configuration data" in the the *Installation and Configuration Guide*.

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

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

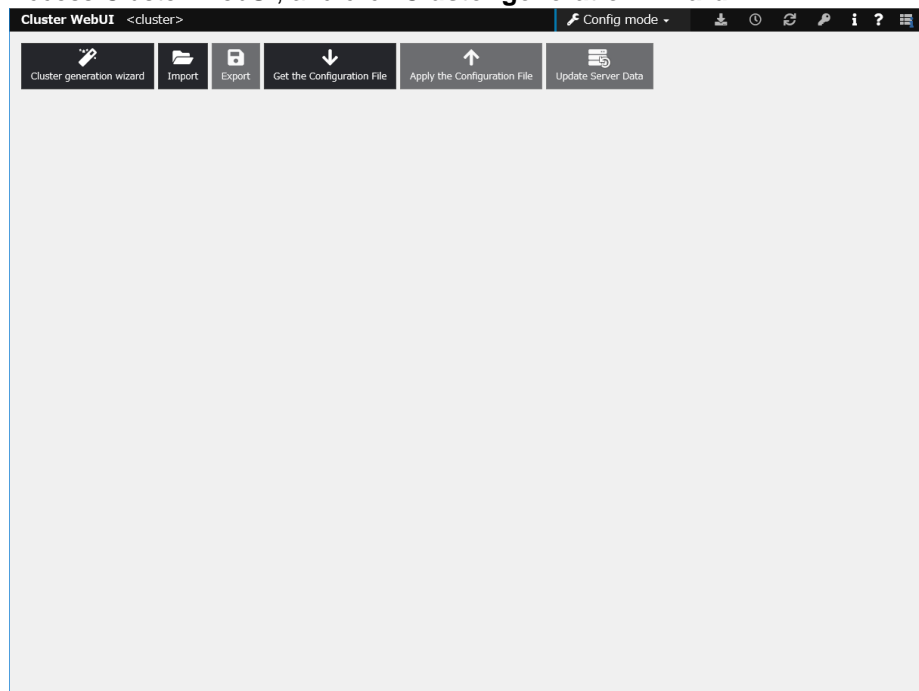
For the settings of other resources and monitor resources, see the *Installation and Configuration Guide* and the *Reference Guide*.

### 1) Creating a cluster

Start the cluster generation wizard to create a cluster.

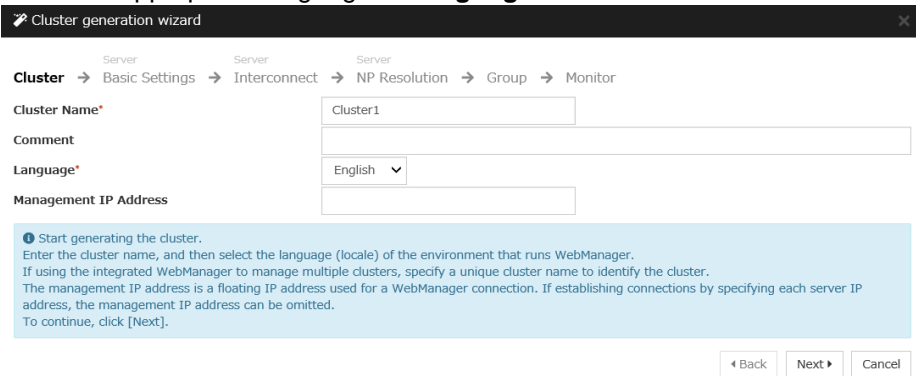
#### ◆ Creating a cluster

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



## Cluster Creation Procedure (for an HA Cluster Using an Public Load Balancer)

- The **Cluster** window on the **Cluster Generation Wizard** is displayed.  
Enter a desired name in **Cluster Name**.  
Select an appropriate language in **Language**. Click **Next**.



Cluster generation wizard

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

Cluster Name\* Cluster1

Comment

Language\* English

Management IP Address

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

Back Next Cancel

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

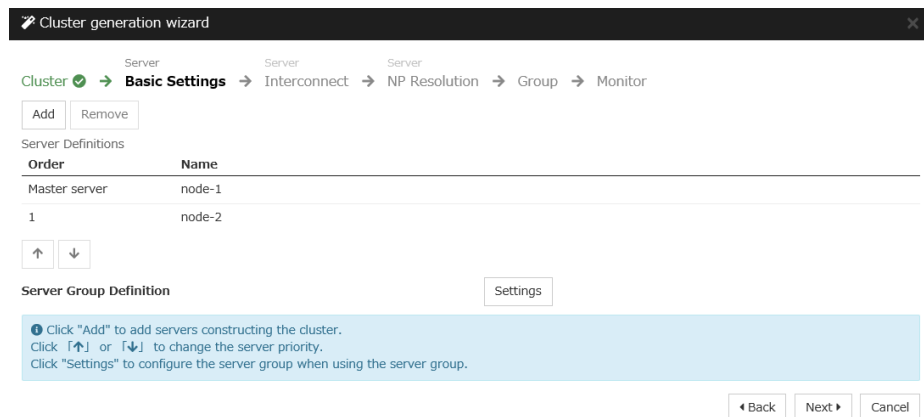


Add server

Server Name or IP Address\* 10.5.0.121

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

OK Cancel



Cluster generation wizard

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

Add Remove

Server Definitions

Order	Name
Master server	node-1
1	node-2

Server Group Definition Settings

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

Back Next Cancel

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

Cluster generation wizard

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

Properties Add Remove

Interconnect List

Priority	Type	MDC	node-1	node-2
1	Kernel Mode	Do Not Use	10.5.0.120	10.5.0.121

↑ ↓

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

◀ Back Next ▶ Cancel

5. The **NP Resolution** window is displayed.  
Note that NP resolution is not configured on this window. The equivalent feature is achieved by adding the IP monitor resource, custom monitor resource, and multi target monitor resource. Configure NP resolution in "3)Adding a monitor resource."  
You need to examine the NP resolution destination and method depending on the location of clients accessing a cluster system and the condition for connecting to an on-premise environment (for example, using a dedicated line). Additionally, you can use network partition resolution resources for NP resolution.  
Click **Next**.

Cluster generation wizard

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

Properties Add Remove

NP Resolution List

Type	Ping Target	node-1	node-2
No NP resolutions			

Tuning

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

◀ Back Next ▶ Cancel



## 2) Adding a group resource

- ◆ Defining a group  
Create a failover group.

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

The screenshot shows the 'Cluster generation wizard' window. The progress bar indicates the following steps: Cluster (checked), Basic Settings (checked), Interconnect (checked), NP Resolution (checked), **Group** (active), and Monitor. Below the progress bar, there are buttons for 'Properties', 'Add', and 'Remove'. A 'Group Resource' button is also visible. The 'Group List' section shows a table with columns 'Name' and 'Type', and it currently displays 'No groups'. A blue information box contains the following text: 'Configure failover group to be a unit of fail over. Click "Add" to add a group. Click "Properties" to configure the properties of the selected group. Click "Group Resource" to add resource to the selected group.' At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

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

The screenshot shows the 'Group Definition' window for a group named 'failover'. The progress bar indicates the following steps: Basic Settings (active), Startup Servers, Group Attributes, and Group Resource. Below the progress bar, there are buttons for 'Properties', 'Add', and 'Remove'. The 'Type' dropdown is set to 'failover'. The 'Name' field is set to 'failover1'. The 'Comment' field is empty. A blue information box contains the following text: 'Select group type. If using virtual machine resources to cluster virtual machines, select "Virtual machine" as the type. In other cases, select "Failover". If using server group, check the "Use Server Group".' At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

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

The screenshot shows the 'Group Definition' window for a group named 'failover'. The progress bar indicates the following steps: Basic Settings (checked), Startup Servers (checked), Group Attributes (checked), and **Group Resource** (active). Below the progress bar, there are buttons for 'Properties', 'Add', and 'Remove'. The 'Group Resource List' section shows a table with columns 'Name' and 'Type', and it currently displays 'No resources'. A blue information box contains the following text: 'Click "Add" to add resources. Click "Properties" to configure the properties of the selected resource.' At the bottom right, there are 'Back', 'Finish', and 'Cancel' buttons.

◆ Mirror disk resource

Create a mirror disk resource.

For details, see "Understanding mirror disk resources" in Chapter 5, "Group resource details" in the *Reference Guide*.

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

Resource Definition of Group | failover1 md ✕

Info → Dependency → Recovery Operation → Details

Type\* Mirror disk resource ▼

Name\* md

Comment

Get license information

Select the type of group resource and enter its name.

◀ Back Next ▶ Cancel

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

Resource Definition of Group | failover1 md ✕

Info ✓ → Dependency ✓ → Recovery Operation ✓ → Details

Mirror Disk No.\* 1 ▼

Data Partition Drive Letter\*

Cluster Partition Drive Letter\*

Cluster Partition Offset Index\* 0 ▼

Mirror Disk Connect Select

Servers that can run the group

Name	Data Partition	Cluster Partition
node-1		
node-2		

← Add

→ Remove

Edit

Add Servers that can run the group

Tuning

◀ Back Finish Cancel

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

**Selection of partition**

Obtain information

Connect

Data Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	71678MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

Cluster Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	71678MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

OK Cancel

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

**Resource Definition of Group | failover1** md x

Info ✓ → Dependency ✓ → Recovery Operation ✓ → Details

Mirror Disk No.\* 1 ▼

Data Partition Drive Letter\* G:

Cluster Partition Drive Letter\* F:

Cluster Partition Offset Index\* 0 ▼

Mirror Disk Connect Select

Servers that can run the group

Name	Data Partition	Cluster Partition
node-1		
node-2		

← Add

→ Remove

Edit

Tuning

◀ Back Finish Cancel

- ◆ **Azure probe port resource**  
When EXPRESSCLUSTER is used on Microsoft Azure, EXPRESSCLUSTER provides a mechanism to wait for alive monitoring from a load balancer on a port specific to a node in which operations are running.

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

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

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

Resource Definition of Group | failover1 azurepp X

Info → Dependency → Recovery Operation → Details

Type\* Azure probe port resource ▼

Name\* azurepp1

Comment

Get license information

Select the type of group resource and enter its name.

Back Next Cancel

3. The **Dependency** window is displayed. Click **Next** without specifying anything.
4. The **Recovery Operation** window is displayed. Click **Next**.
5. For **Probeport**, enter the value specified for **Port** when configuring a load balancer (configuring health probe).

Resource Definition of Group | failover1 azurepp X

Info → Dependency → Recovery Operation → Details

Probeport\* 26001

Tuning

Back Finish Cancel

6. Click **Finish**.

### 3) Adding a monitor resource

◆ Azure probe port monitor resource

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

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

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

◆ Azure load balance monitor resource

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

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

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

◆ Custom monitor resource

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

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

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

The screenshot shows the 'Monitor Resource Definition' window with the title bar 'genw x'. The breadcrumb navigation is 'Info → Monitor(common) → Monitor(special) → Recovery Action'. The 'Type\*' field is a dropdown menu set to 'Custom monitor'. The 'Name\*' field contains the text 'genw1'. There is an empty 'Comment' text area and a 'Get Licence Info' button. A blue information bar at the bottom states: 'Select the type of monitor resource and enter its name.' At the bottom right are three buttons: 'Back', 'Next', and 'Cancel'.

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

The screenshot shows the 'Monitor Resource Definition' window with the 'Monitor(common)' tab selected. The breadcrumb trail is 'Info' (with a green checkmark) → 'Monitor(common)' → 'Monitor(special)' → 'Recovery Action'. The 'Interval\*' is set to 60 sec, 'Timeout\*' is 120 sec, 'Do Not Retry at Timeout Occurrence' is unchecked, 'Do Not Execute Recovery Action at Timeout Occurrence' is unchecked, 'Retry Count\*' is 1 time, and 'Wait Time to Start Monitoring\*' is 3 sec. Under the 'Monitor Timing' section, 'Always' is selected with a radio button, and 'Active' is unselected. There is a 'Target Resource' field with a 'Browse' button. Below that is a 'Choose servers that execute monitoring' section with a 'Server' button. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

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

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

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

The screenshot shows the 'Monitor Resource Definition' window with the 'Monitor(special)' tab selected. The breadcrumb trail is 'Info' (with a green checkmark) → 'Monitor(common)' (with a green checkmark) → 'Monitor(special)' → 'Recovery Action'. Under 'User Application', 'Script created with this product' is selected with a radio button. The 'File' field contains 'genw.bat', with 'Edit', 'View', and 'Replace' buttons to its right. Under 'Monitor Type', 'Synchronous' is selected with a radio button, and 'Asynchronous' is unselected. The 'Normal Return Value\*' is set to 0. There are two unchecked checkboxes: 'Kill the application when exit' and 'Wait for activation monitoring to stop before stopping the cluster'. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

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

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

- Click **Finish** to finish setting.

#### ◆ IP monitor resource

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

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

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

The screenshot shows the 'Monitor Resource Definition' window with the 'IP monitor' type selected. The breadcrumb trail is 'Info → Monitor(common) → Monitor(special) → Recovery Action'. The 'Type' dropdown is set to 'IP monitor'. The 'Name' field contains 'ipw1'. There is a 'Comment' field and a 'Get Licence Info' button. A blue information bar at the bottom states 'Select the type of monitor resource and enter its name.' On the right, there are buttons for 'Back', 'Next', and 'Cancel'.

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

Monitor Resource Definition ipw

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

Interval\*

60

sec

Timeout\*

60

sec

Do Not Retry at Timeout Occurrence

☐

Do Not Execute Recovery Action at Timeout Occurrence

☐

Retry Count\*

1

time

Wait Time to Start Monitoring\*

0

sec

Monitor Timing

☒ Always

☐ Active

Target Resource

Browse

Choose servers that execute monitoring

Server

◀ Back

Next ▶

Cancel

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

Failure Detection Server

☐ All servers

☒ Select

Servers that can run the Group

Name

node-1

Available Servers

Name

node-2

←

Add

→

Remove

OK

Cancel

Apply



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

The screenshot shows the 'Monitor Resource Definition' window with the 'Monitor(special)' tab selected. The breadcrumb trail is 'Info' → 'Monitor(common)' → 'Monitor(special)' → 'Recovery Action'. Below the breadcrumb are 'Edit', 'Add', and 'Remove' buttons. The 'IP Address List' section shows 'IP Address' with the value 'No Ip Address'. A red message states 'Please add a IP Address.' Below this, the 'ping Timeout\*' is set to '5000' msec. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

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

The screenshot shows the 'IP Address Settings' dialog box. It has a single text input field for 'IP Address\*' containing the value '10.5.0.121'. At the bottom right are 'OK' and 'Cancel' buttons.

The screenshot shows the 'Monitor Resource Definition' window with the 'Monitor(special)' tab selected. The breadcrumb trail is 'Info' → 'Monitor(common)' → 'Monitor(special)' → 'Recovery Action'. Below the breadcrumb are 'Edit', 'Add', and 'Remove' buttons. The 'IP Address List' section now shows 'IP Address' with the value '10.5.0.121' highlighted in blue. The 'ping Timeout\*' is still set to '5000' msec. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

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

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

6. Click **Finish** to finish setting.
7. Then, create a monitor resource on the other server. Click **Add** on the **Monitor Resource List** page.
8. Select the monitor resource type (IP monitor) from the **Type** box and enter the monitor resource name (ipw2) in the **Name** box. Click **Next**.
9. The **Monitor (common)** window is displayed.  
Confirm that **Monitor Timing** is **Always**.  
Select one available server for **Choose servers that execute monitoring**. Click **OK** and Click **Next**.
10. The **Monitor (special)** window is displayed.  
On the **Common** tab, select **Add of IP Address** and set an IP address of a server other than the server selected in step 9. Click **Next**.
11. The **Recovery Action** window is displayed.  
Select **Execute only the final action** for **Recovery Action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final action**.
12. Click **Finish** to finish setting.

◆ Multi target monitor resource

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

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

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

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

Monitor Resource Definition mtw ×

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

Type\* Multi target monitor

Name\* mtw1

Comment

Get Licence Info

Select the type of monitor resource and enter its name.

◀ Back Next ▶ Cancel

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

Monitor Resource Definition mtw ×

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

Interval\* 60 sec

Timeout\* 60 sec

Do Not Retry at Timeout Occurrence ☐

Do Not Execute Recovery Action at Timeout Occurrence ☐

Retry Count\* 1 time

Wait Time to Start Monitoring\* 0 sec

Monitor Timing

☒ Always

☐ Active

Target Resource  Browse

Choose servers that execute monitoring Server

◀ Back Next ▶ Cancel

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

Monitor Resource Definition

mbw

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

Monitor Resource List

Monitor Resource	Type
genw1	genw
ipw1	ipw
ipw2	ipw

←

Add

→

Remove

Tuning

Available Monitor Resources

Monitor Resource	Type
userw	userw

◀ Back

Next ▶

Cancel

5. The **Recovery Action** window is displayed.  
Select **Execute only the final action** for **Recovery action**, **LocalServer** for **Recovery Target**, and **No operation** for **Final action**, and select the **Execute Script before Final Action** check box.  
Click **Script Settings** and create a script to be executed when the multi target monitor resource detects an error.

Monitor Resource Definition

mbw

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

Recovery Action

Execute only the final action

Recovery Target \*

LocalServer

Browse

Recovery Script Execution Count

0

time

Execute Script before Reactivation

Maximum Reactivation Count

0

time

Execute Script before Failover

Execute migration before Failover

Failover Target Server

Stable server

Maximum priority server

Maximum Failover Count

0

time

Execute Script before Final Action

☒

Final Action

No operation

Script Settings

◀ Back

Finish

Cancel

6. The script editing dialog box is displayed.  
 Select **Script created with this product** and click **Edit** to edit the script. The following shows the sample of a script to be created.  
 Specify the following by referring to "4.1 Creation example" The ports differ depending on operations.
- **Load balancing rule > Backend port** of the load balancer
  - **Load balancing rule > Port** of the load balancer
- Set the public IP address that you wrote down in "10)Setting the inbound security rules" to the following:
- **Frontend IP** (public IP address) of the load balancer

```

-----
rem *****
rem Check Active Node
rem *****
<EXPRESSCLUSTER_installation_path>\bin\clpazure_port_checker -h 127.0.0.1 -p <
Backend_port_of_the_load_balancer_of_Load_balancing_rule>
IF NOT "%ERRORLEVEL%" == "0" (
    GOTO CLUSTER_SHUTDOWN
)

rem *****
rem Check DNS
rem *****
<EXPRESSCLUSTER_installation_path>\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 "%ERRORLEVEL%" == "0" (
    GOTO EXIT
)

rem *****
rem Cluster Shutdown
rem *****
:CLUSTER_SHUTDOWN
clpdown

rem *****
rem EXIT
rem *****
:EXIT
EXIT 0
-----

```

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

Dialog box titled "Edit Script" showing configuration options for a script.

Options:

- ☐ User Application
- ☒ Script created with this product

File: `preaction.bat`

Buttons: Edit, View, Replace

Timeout\*:  sec

Buttons: OK, Cancel, Apply

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

#### 4) Setting the cluster properties

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

##### ◆ Cluster properties

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

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

Cluster Properties | Cluster1

Info Interconnect NP Resolution Timeout Port No. Monitor Recovery Alert Service WebManager  
Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration Extension

Cluster Name Cluster1

Comment

Language English

OK Cancel Apply

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

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

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

B: **Interval** of the multi target monitor resource x (**Retry Count**+1)

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

Note: If **Timeout of Heartbeat** is shorter than the time that 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.

Cluster Properties | Cluster1

Info Interconnect NP Resolution Timeout Port No. Monitor Recovery Alert Service WebManager  
Alert Log Delay Warning Disk Mirror Disk Account RIP(Legacy) Migration Extension

Network initialization complete wait time\* 3 min

Server Sync Wait Time\* 5 min

Heartbeat

Interval\* 3 sec

Timeout\* 270 sec

Server Internal Timeout\* 180 sec

Initialize

OK Cancel Apply

3. Click **OK**.

## 5) Applying the settings and starting the cluster

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

For details, refer to the following:

- *Installation and Configuration Guide*  
→ How to create a cluster



## 4.4 Verifying the created environment

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

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

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

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

# 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 node-1 is used as an active server.

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

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

Setting item	Setting value
<b>Resource group setting</b>	
Resource group	TestGroup1
Region	Japan East
<b>Virtual network setting</b>	
Name	Vnet1
Address space	10.5.0.0/24
Subnet Name	Vnet1-1
Subnet Address range	10.5.0.0/24
Resource group	TestGroup1
Location	Japan East
<b>Load balancer setting</b>	
Name	TestLoadBalancer
Type	Internal
Virtual network	Vnet1
Subnet	Vnet1-1
IP address assignment	Static
Private IP address	10.5.0.200
Resource group	TestGroup1
Region	Japan East
Backend pool: Name	TestBackendPool
Associated to	Availability set
Target virtual machine	node-1 node-2
Network IP configuration	10.5.0.120 10.5.0.121
Health probe: Name	TestHealthProbe
Health probe: Port	26001
Load balancing rule: Name	TestLoadBalancingRule
Load balancing rule: Port	80 (Port number offering the operation)
Load balancing rule: Backend port	8080 (Port number offering the operation)

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

Setting item	Setting value	
	node-1	node-2
<b>Virtual machine setting</b>		
Disk type	Standard HDD	
User name	testlogin	
Password	PassWord_123	
Resource group	TestGroup1	

Region	Japan East	
Network security group setting		
Name	NetSecGroup-1	
Availability set setting		
Name	AvailabilitySet-1	
Update domains	5	
Fault domains	2	
Diagnostics storage account setting		
Name	Automatically generated (testgroup1diag679)	
Performance	Standard	
Replication	Locally-redundant storage (LRS)	
IP configuration setting		
IP address	10.5.0.120	10.5.0.121
Blob storage setting		
Name	node-1Blob1	node-2Blob1
Source type	None (empty disk)	
Account type	Standard HDD	

- EXPRESSCLUSTER settings (cluster properties)

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

- EXPRESSCLUSTER settings (failover group)

Resource name	Setting item	Setting value
Mirror disk resource	Nama	md
	Details Tab: Data Partition Drive Letter	G:
	Details Tab: Cluster Partition Drive Letter	F:
Azure probe port resource	Name	azurepp1
	Probe port	26001 (Value specified for <b>Port of Health probe</b> )
Script resource (when DSR is used)	Name	script1

- EXPRESSCLUSTER settings (monitor resource)

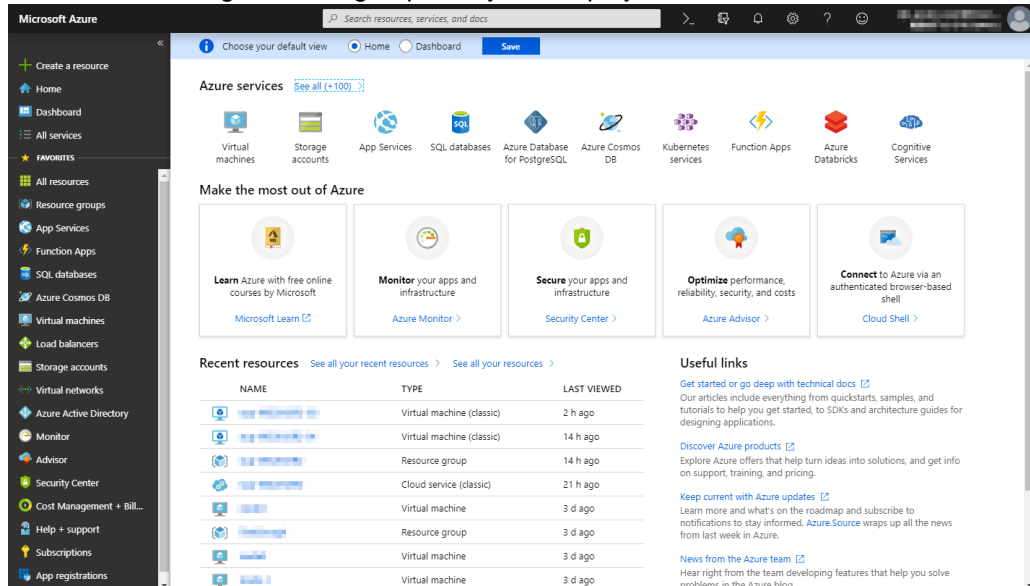
Monitor resource name	Setting item	Setting value
Mirror disk monitor resource	-	-
Azure probe port monitor resource	Name	azureppw1
	Recovery Target	azurepp1
Azure load balance monitor resource	Name	aurelbw1
	Recovery Target	azurepp1

## 5.2 Configuring Microsoft Azure

### 1) Creating a resource group

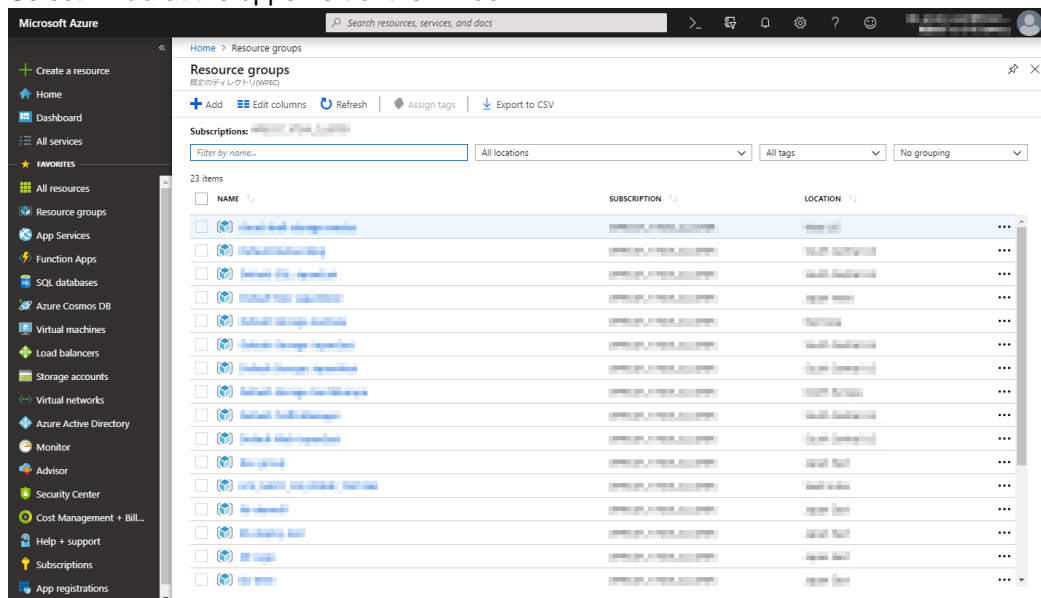
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create a resource group following the steps below.

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.



NAME	TYPE	LAST VIEWED
my-vm1	Virtual machine (classic)	2 h ago
my-vm2	Virtual machine (classic)	14 h ago
my-vm3	Resource group	14 h ago
my-vm4	Cloud service (classic)	21 h ago
my-vm5	Virtual machine	3 d ago
my-vm6	Resource group	3 d ago
my-vm7	Virtual machine	3 d ago
my-vm8	Virtual machine	3 d ago

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



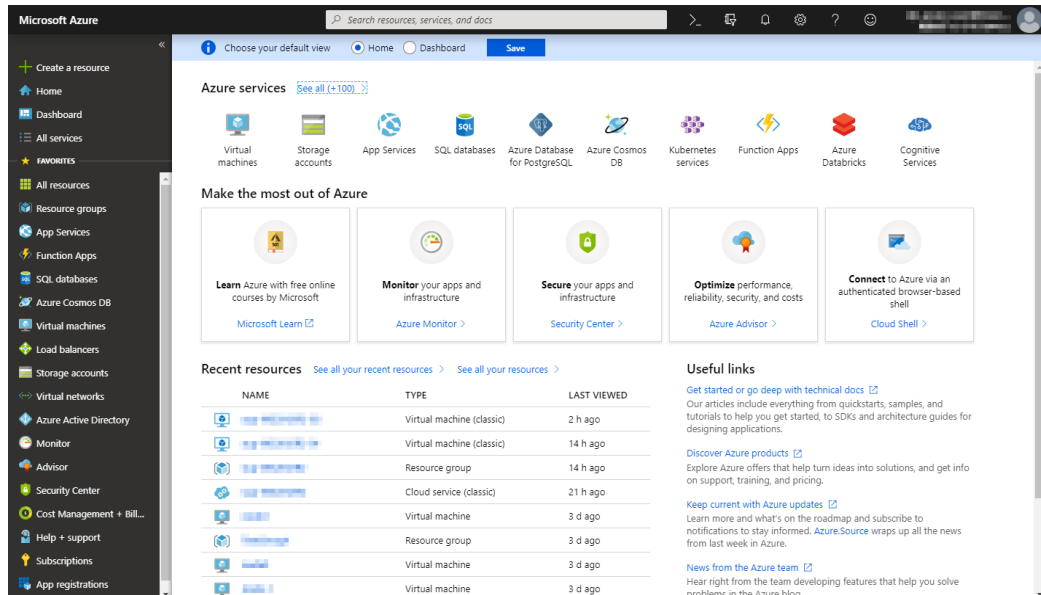
3. Specify **Resource group**, **Subscription**, and **Region**, and click **Review+Create**.

The screenshot shows the Microsoft Azure portal interface. On the left is a navigation sidebar with options like 'Create a resource', 'Home', 'Dashboard', 'All services', and 'FAVORITES'. The 'Resource groups' section is selected. The main content area is titled 'Create a resource group' and includes a description of resource groups. Below this, there are sections for 'PROJECT DETAILS' and 'RESOURCE DETAILS'. In 'PROJECT DETAILS', the 'Subscription' is selected from a dropdown, and 'Resource group' is set to 'TestGroup1'. In 'RESOURCE DETAILS', the 'Region' is set to 'Japan East'. At the bottom, there are two buttons: 'Review + Create' and 'Next: Tags'.

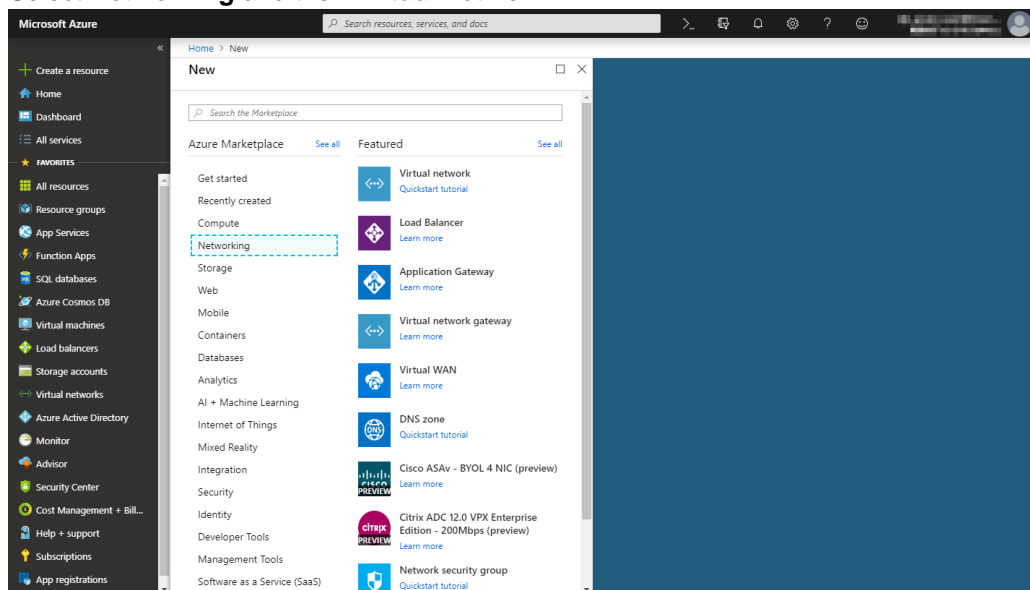
## 2) Creating a virtual network

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**, **Location**, **Name** of Subnet, and **Address range**, and click **Create**.

The screenshot shows the 'Create virtual network' page in the Microsoft Azure portal. The left sidebar contains the navigation menu with 'Virtual networks' highlighted. The main form contains the following fields and values:

- Name:** Vnet1
- Address space:** 10.5.0.0/16 (10.5.0.0 - 10.5.255.255 (65536 addresses))
- Subscription:** [selected]
- Resource group:** TestGroup1
- Location:** Japan East
- Subnet:**
  - Name:** Vnet1-1
  - Address range:** 10.5.0.0/24 (10.5.0.0 - 10.5.0.255 (256 addresses))
- DDoS protection:** Basic (selected)
- Service endpoints:** Disabled
- Firewall:** Disabled

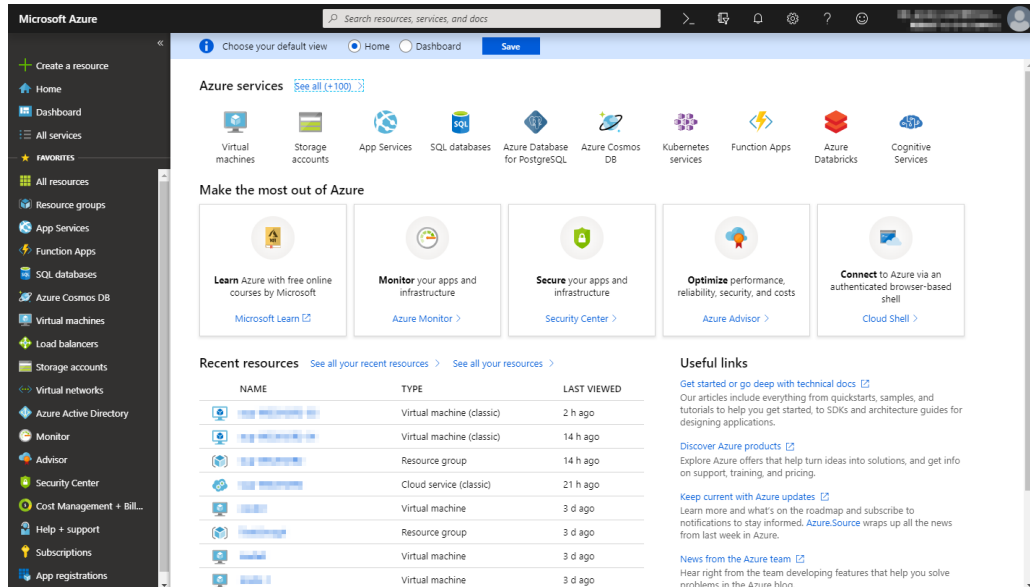
The 'Create' button is located at the bottom of the form, next to the 'Automation options' link.

### 3) Creating a virtual machine

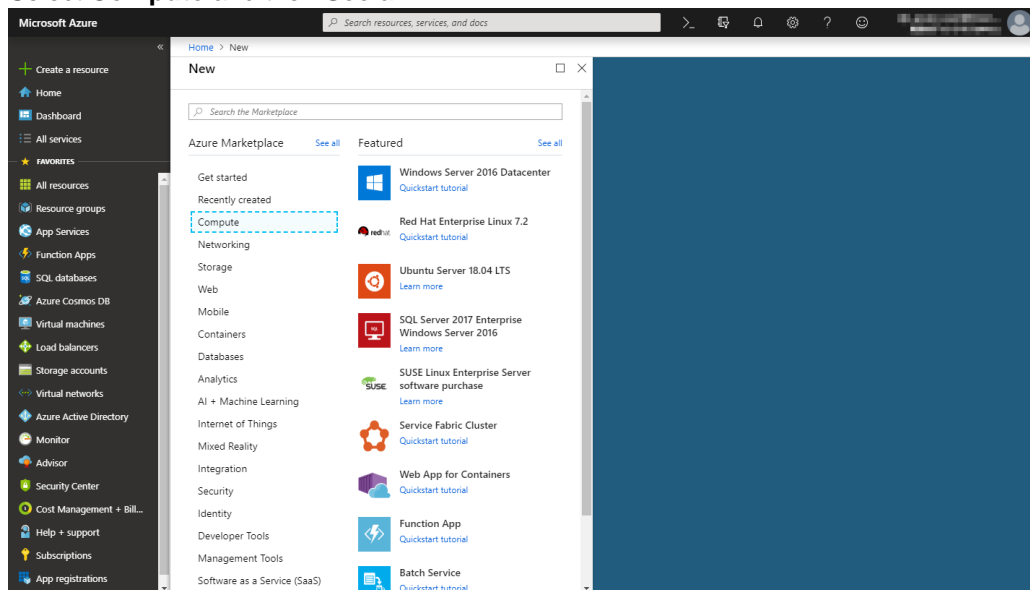
Log in to the Microsoft Azure portal (<https://portal.azure.com/>) and create virtual machines and disks following the steps below.

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

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**.





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

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

The screenshot shows the 'Create a virtual machine' blade in the Microsoft Azure portal, specifically the 'Basics' tab. The left sidebar contains navigation links for various Azure services. The main content area is titled 'Create a virtual machine' and includes instructions for creating a VM. Below the instructions, there are sections for 'PROJECT DETAILS' and 'INSTANCE DETAILS'. In the 'PROJECT DETAILS' section, the 'Subscription' is set to 'my\_subscription' and the 'Resource group' is 'TestGroup1'. In the 'INSTANCE DETAILS' section, the 'Virtual machine name' is 'node-1', the 'Region' is 'Japan East', the 'Availability options' are set to 'Availability set', and the 'Availability set' is '(new) AvailabilitySet-1'. The 'Image' is 'Windows Server 2016 Datacenter' and the 'Size' is 'Standard A1'. At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next: Disks >'. A URL 'https://portal.azure.com/?hl=en-us#f' is visible at the bottom left.

The screenshot shows the 'Create new' blade for an availability set in the Microsoft Azure portal. The left sidebar is the same as the previous screenshot. The main content area is titled 'Create new' and includes instructions for creating an availability set. Below the instructions, there are sections for 'PROJECT DETAILS' and 'INSTANCE DETAILS'. In the 'PROJECT DETAILS' section, the 'Subscription' is set to 'my\_subscription' and the 'Resource group' is 'TestGroup1'. In the 'INSTANCE DETAILS' section, the 'Virtual machine name' is 'node-1', the 'Region' is 'Japan East', the 'Availability options' are set to 'Availability set', and the 'Availability set' is 'No existing availability sets in current resource group and location'. The 'Image' is 'Windows Server 2016 Datacenter' and the 'Size' is 'Standard A1'. At the bottom, there are buttons for 'Review + create', 'Previous', and 'Next: Disks >'. On the right side, there are settings for 'Name' (set to 'AvailabilitySet-1'), 'Fault domains' (set to 2), and 'Update domains' (set to 5). There is also a section for 'Use managed disks' with radio buttons for 'No (Classic)' and 'Yes (Aligned)'. An 'OK' button is at the bottom right.

- Click **Change size** to display the **Select a VM size** blade. From the list, choose a size (**A1 - Standard** in this guide) suitable for your virtual machine and click **Select**. Regarding the **Virtual machine name**, node-1 is for node-1, and node-2 is for node-2. Click **Next: Disks** >

VM SIZE	OFFERING	FAMILY	VCPUS	RAM (GB)	DATA DISKS	MAX IOPS	TEMPORARY STORAGE	PREMIUM DISK SUPP.	COST/MONTH (EST.)
A0	Standard	General purpose	1	0.75	1	1x500	No	No	\$2,001
A0	Basic	General purpose	1	0.75	1	1x300	No	No	\$1,838
A1	Standard	General purpose	1	1.75	2	2x500	No	No	\$8,839
A1	Basic	General purpose	1	1.75	2	2x300	No	No	\$3,415
A1_v2	Standard	General purpose	1	2	2	2x500	No	No	\$6,748
A2	Standard	General purpose	2	3.5	4	4x500	No	No	\$17,677
A2	Basic	General purpose	2	3.5	4	4x300	No	No	\$12,083
A2_v2	Standard	General purpose	2	4	4	4x500	No	No	\$14,173
A2m_v2	Standard	General purpose	2	16	4	4x500	No	No	\$19,426
A3	Standard	General purpose	4	7	8	8x500	No	No	\$35,347
A3	Basic	General purpose	4	7	8	8x300	No	No	\$31,680
A4	Standard	General purpose	8	14	16	16x500	No	No	\$70,687
A4	Basic	General purpose	8	14	16	16x300	No	No	\$63,359

- When the **Disks** tab appears, go through the following steps to add a blob to be used for a mirror disk (cluster partition or data partition). From the **DATA DISKS** list, click **Create and attach a new disk**.

**DISK OPTIONS**

OS disk type: Standard SSD

Enable Ultra SSD compatibility (Preview): ☐ Yes ☒ No

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

**DATA DISKS**

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

LUN	NAME	SIZE (GiB)	DISK TYPE	HOST CACHING
Create and attach a new disk    Attach an existing disk				

ADVANCED

Review + create    Previous    Next: Networking >

7. The **Create a new disk** blade appears. Specify the settings of **Disk type**, **Name**, **Size (GiB)**, and **Source type**. Then click **OK**. Click **Next: Networking >**

Microsoft Azure

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

### Create a new disk

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

- Disk type: Standard HDD
- Name: node-1blob1
- Size (GiB):
- Source type: None (empty disk)

ESTIMATED PERFORMANCE

IOPS limit: 500

Throughput limit (MB/s): 60

OK

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

Microsoft Azure

Home > New > Create a virtual machine > Create network security group

### Create network security group

Guest config Tags Review + create

By configuring network interface card (NIC) settings, you can control ports, inbound traffic, and place behind an existing load balancing solution. [Learn more](#)

will be created for you.

new

-1 (10.0.0.0/24)

subnet configuration

new

Basic Advanced

node-1-nsg

new

Off

The selected VM size does not support accelerated networking.

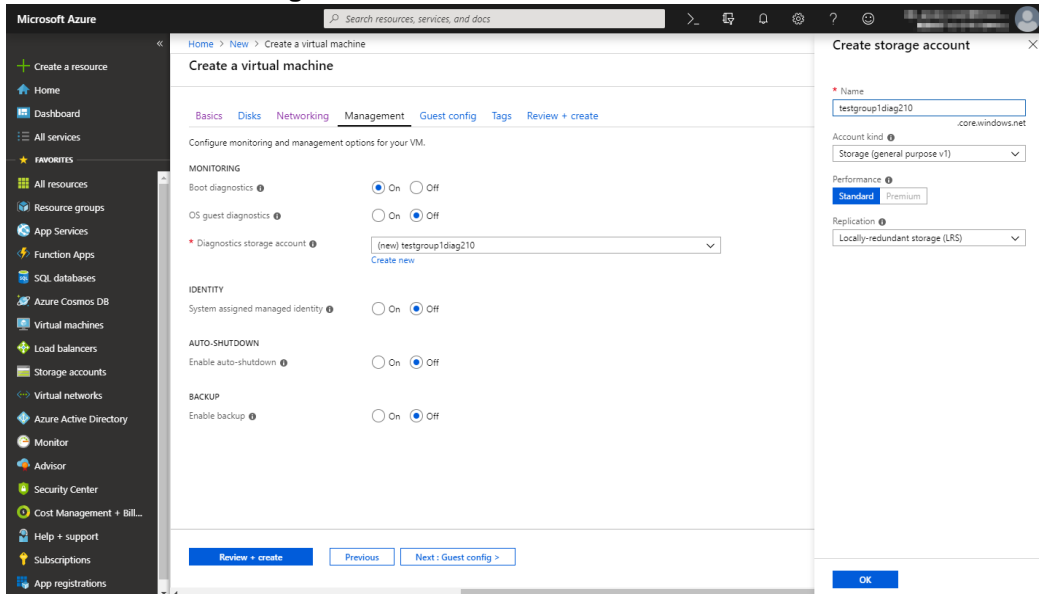
of an existing Azure load balancing solution. [Learn more](#)

No

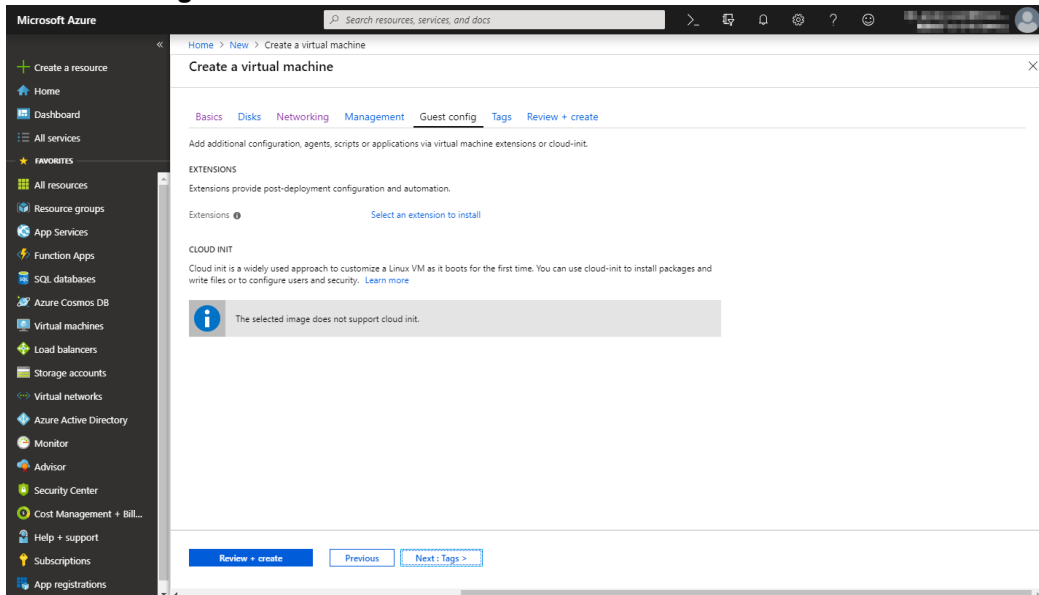
Next: Management >

OK

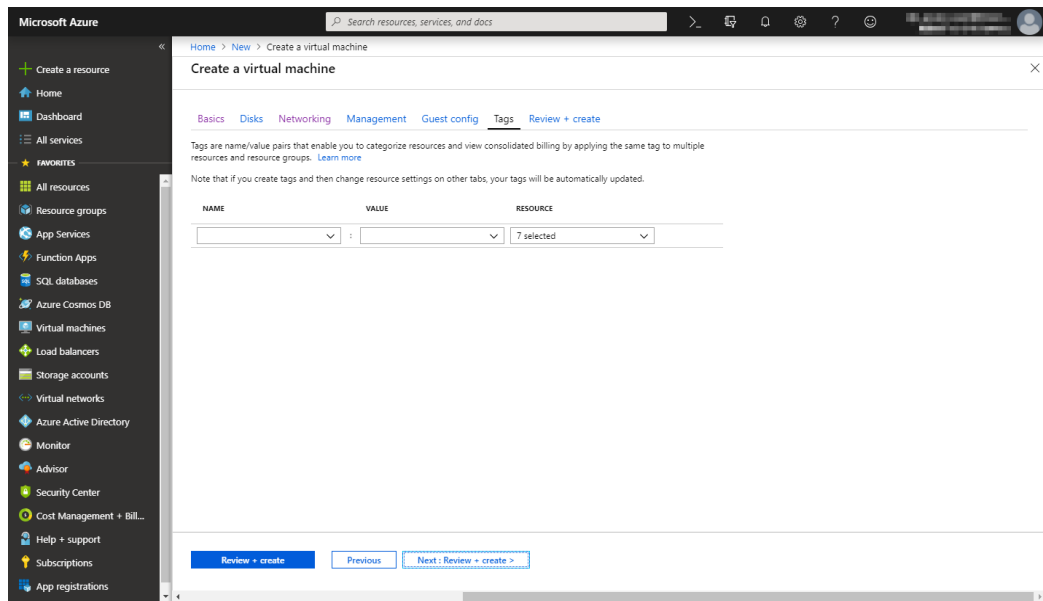
9. The **Management** tab appears.  
Click **Create new** under the **Diagnostics storage account** field to display the **Create storage account** blade.  
Specify the settings of **Name**, **Account kind**, and **Replication**. Then click **OK**.  
In the **Diagnostics storage account** field, the default value is automatically generated and entered.  
Click Next: **Guest config** >.



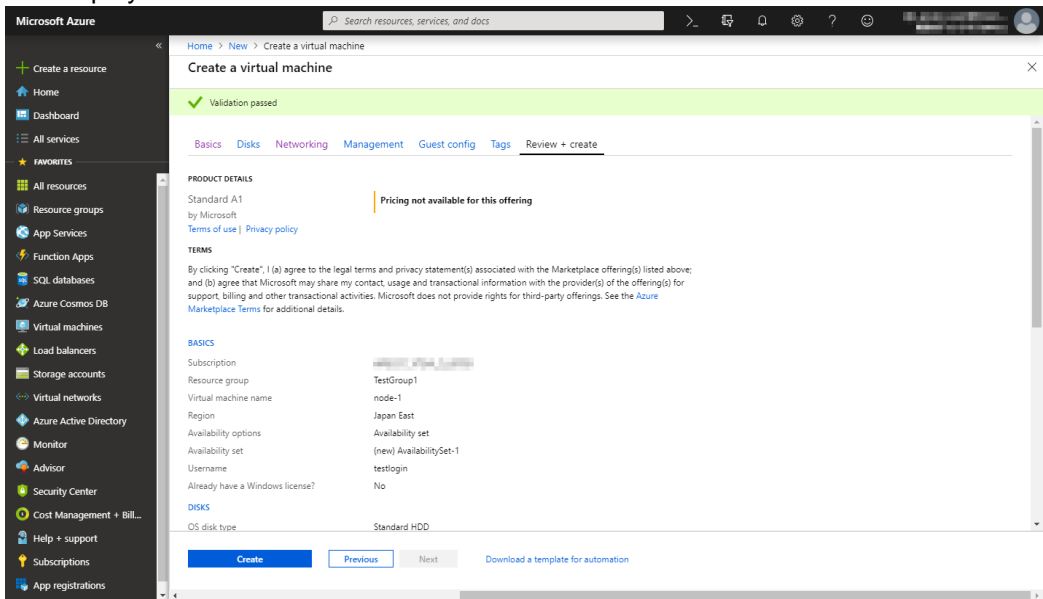
10. Click Next: **Tags** >.



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



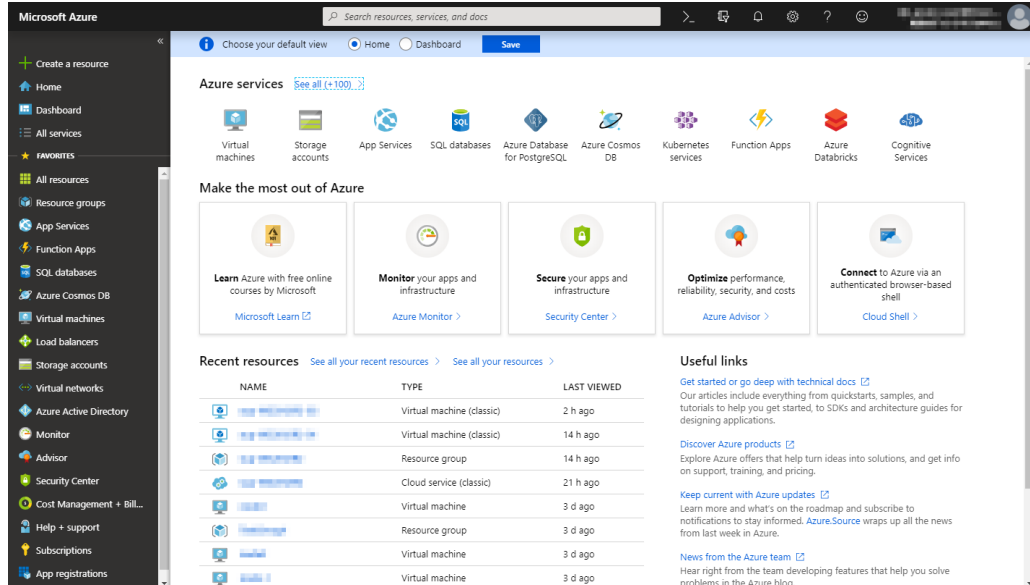
12. The **Review + create** tab appears. Check the contents. If there is no problem, click **Create**. The deployment starts and takes several minutes.



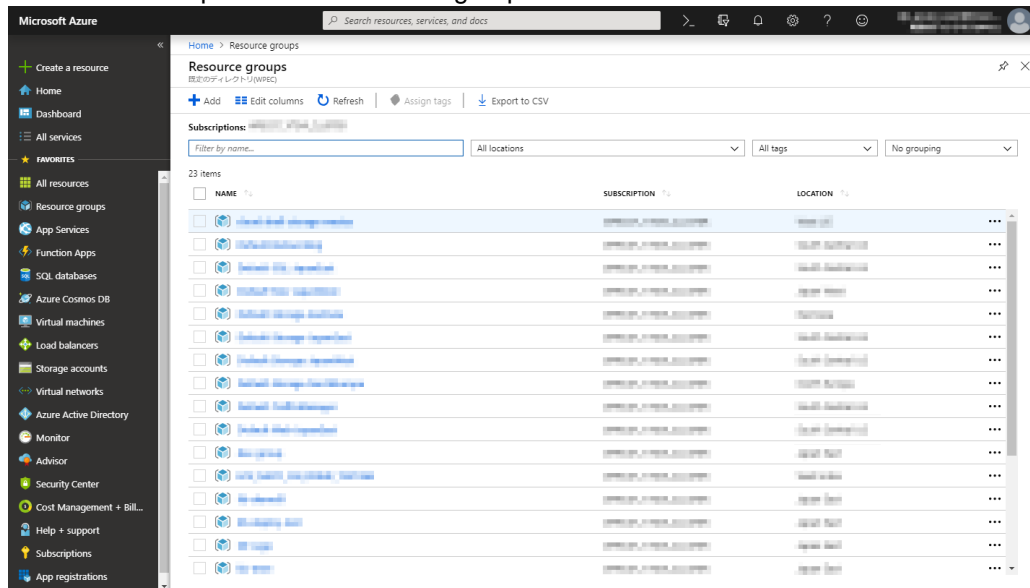
#### 4) Setting a private IP address

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

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

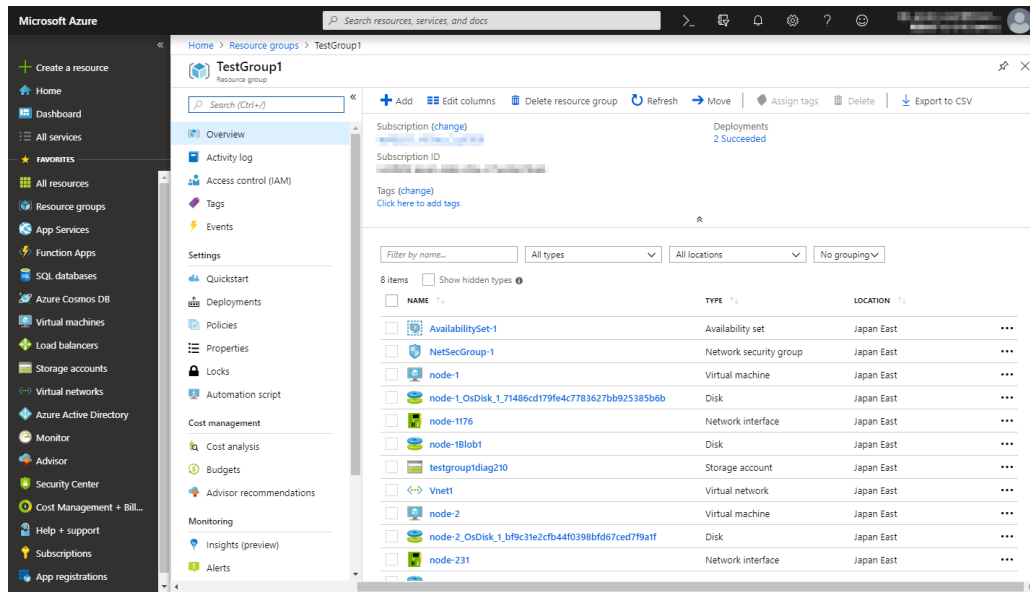


2. Select **TestGroup1** from the resource group list.

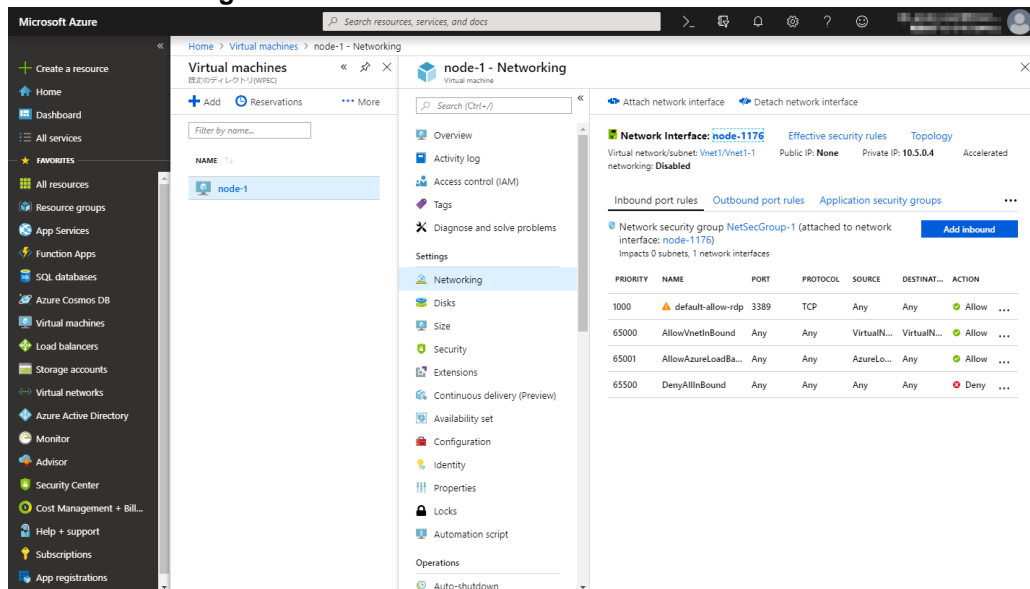


## Cluster Creation Procedure (for an HA Cluster Using an Internal Load Balancer)

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

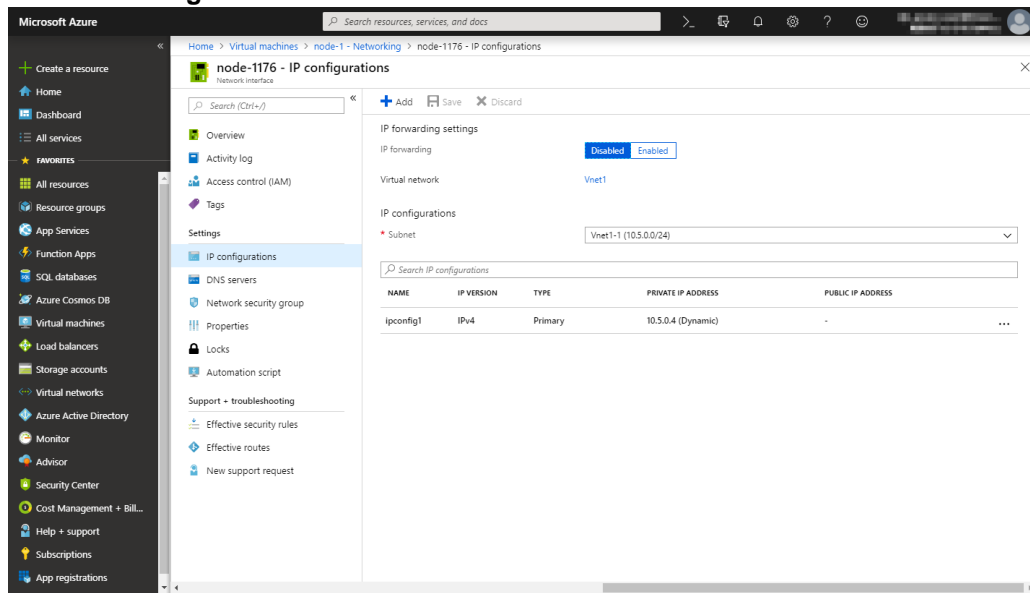


4. Select Networking.



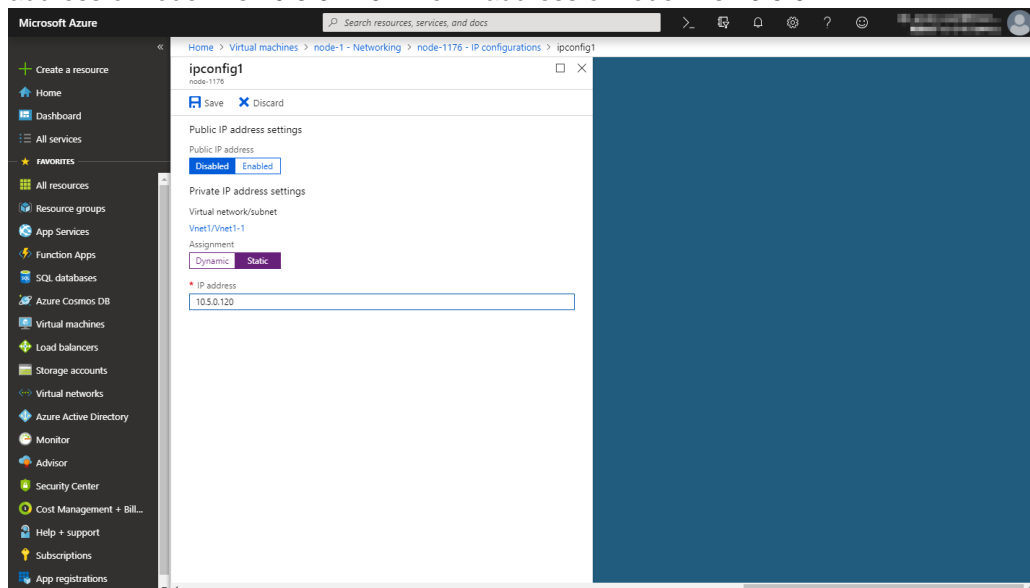
5. Select a network interface displayed in the list. The network interface name is generated automatically.

6. Select **IP configurations**.



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

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



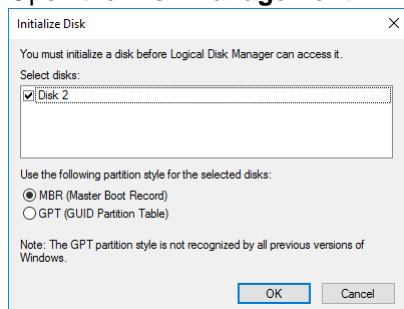
9. The virtual machines restart automatically so that new private IP addresses can be used.



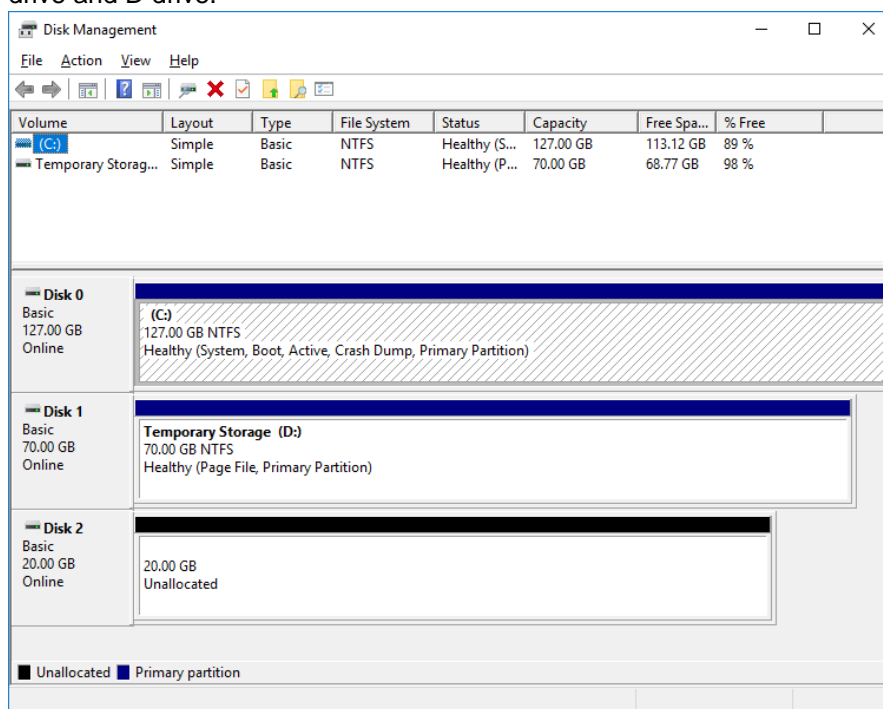
## 5) Configuring virtual machines

Log in to the created node-1 and node-2 and specify the settings following the procedure below. Set a partition for the mirror disk resource. Create a file system in the added Blob storage. For details about a partition for the mirror disk resource, see "Partition settings for mirror disk resource (when using Replicator)" in "Settings after configuring hardware" in Chapter 1, "Determining a system configuration" in the *Installation and Configuration Guide*.

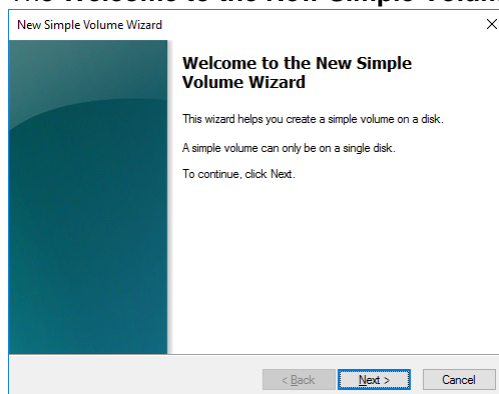
1. Open the **Disk Management** window. The **Initialize Disk** dialog box is displayed.



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



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



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

The screenshot shows the 'Specify Volume Size' window of the 'New Simple Volume Wizard'. The window title is 'New Simple Volume Wizard' with a close button (X). Below the title bar, the section is 'Specify Volume Size' with the instruction 'Choose a volume size that is between the maximum and minimum sizes.' The main area contains three labels: 'Maximum disk space in MB:' with the value '20477', 'Minimum disk space in MB:' with the value '8', and 'Simple volume size in MB:' with a text box containing '1024' and a spinner control. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

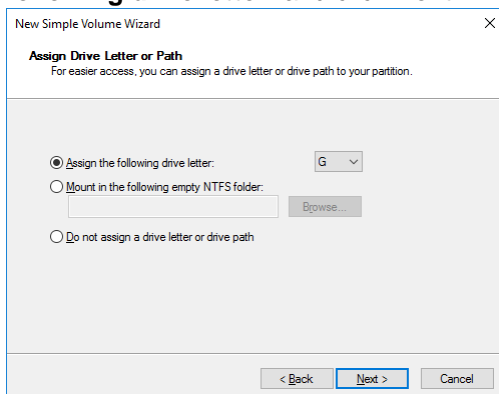
6. The **Assign Drive Letter or Path** window is displayed. Select the F drive for **Assign the following drive letter:**. Use the disk as a raw partition without formatting.

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

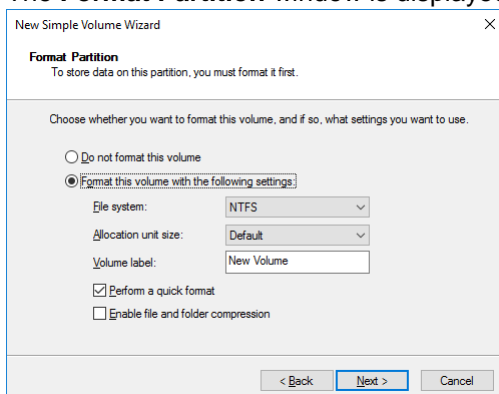
7. Next, create a data partition. Right-click "Disk 2" and select **New Simple Volume**.  
8. The **Welcome to the New Simple Volume Wizard** is displayed. Click **Next**.  
9. The **Specify Volume Size** window is displayed. Click **Next**.

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

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

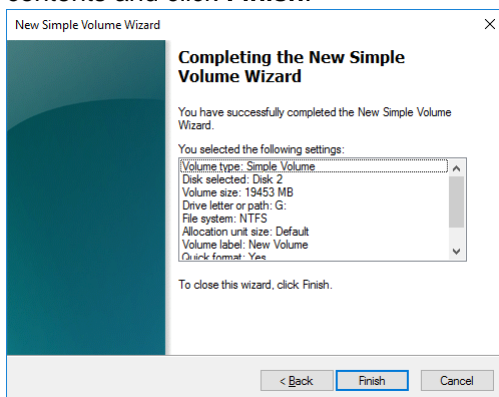


11. The **Format Partition** window is displayed. Confirm that **File System** is **NTFS**.

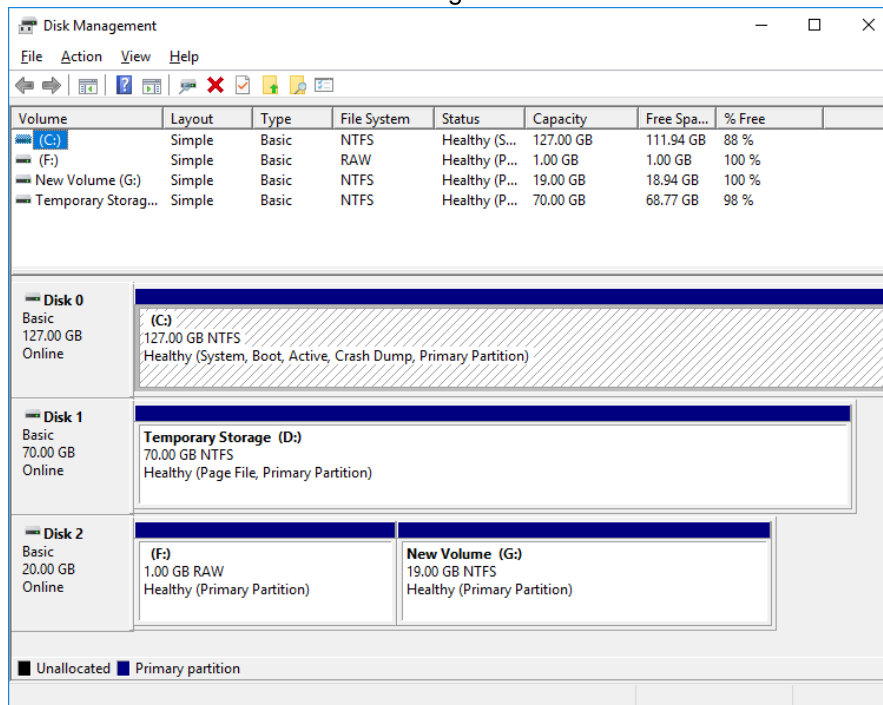


12. Click **Next**.

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



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



Next, for using DSR, add a loopback adapter in each node configuring a cluster. Refer to the following when creating a DSR configuration.  
<https://jpn.nec.com/clusterpro/blog/20181031.html> (Japanese only)

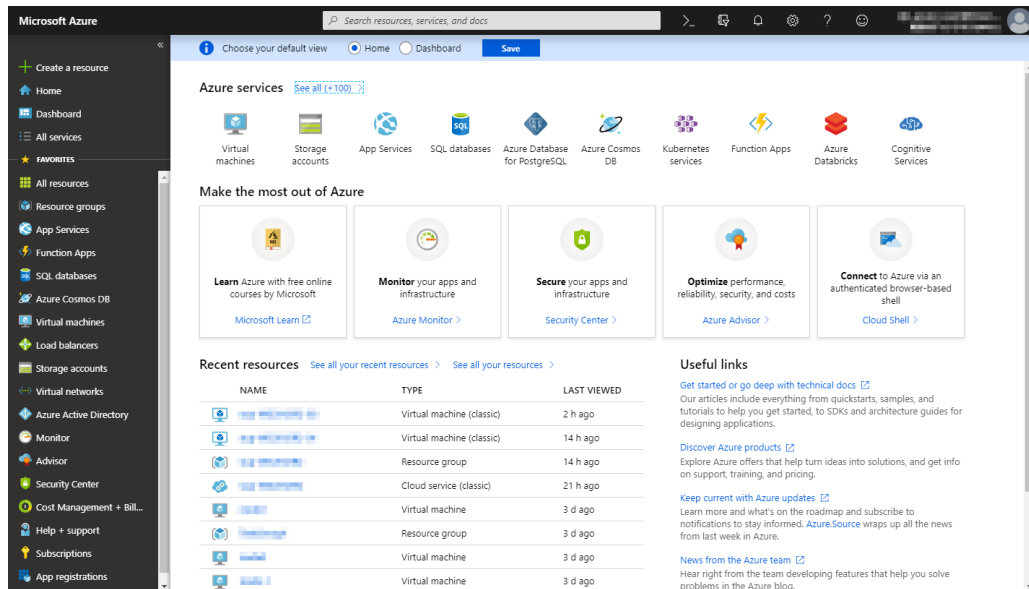
## 6) Configuring a load balancer

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

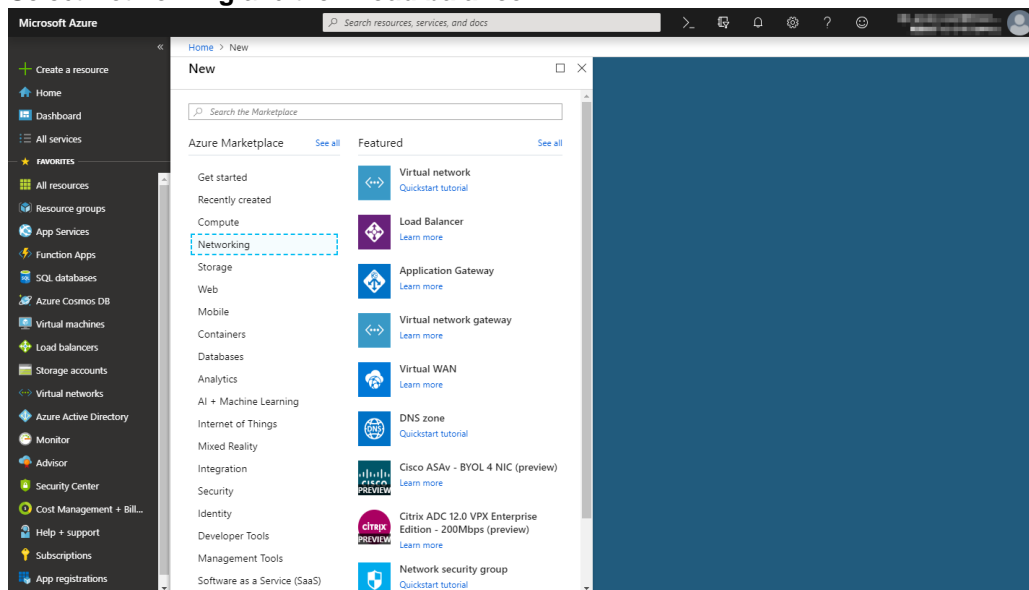
For details, see the following websites:

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

1. Select **+Create a resource** 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**. Select **Internal** for **Type** and **Basic** for **SKU**, respectively.
4. For **Virtual network** and **Subnet**, select the virtual network and subnet created in "2)Creating a virtual network"

5. Specify **IP address assignment**, **Private IP address**, **Subscription**, **Resource group**, and **Region**, and click **Review+create**. Deploying the load balancer starts. This processing takes several minutes.

The screenshot shows the 'Create load balancer' wizard in the Microsoft Azure portal. The left sidebar contains navigation links for various Azure services. The main content area is titled 'Create load balancer' and includes a brief description of the service. The configuration is organized into three sections: 'PROJECT DETAILS', 'INSTANCE DETAILS', and 'CONFIGURE VIRTUAL NETWORK'. The 'PROJECT DETAILS' section includes fields for 'Subscription' and 'Resource group' (set to 'TestGroup1'). The 'INSTANCE DETAILS' section includes fields for 'Name' (set to 'TestLoadBalancer'), 'Region' (set to 'Japan East'), 'Type' (set to 'Internal'), and 'SKU' (set to 'Basic'). The 'CONFIGURE VIRTUAL NETWORK' section includes fields for 'Virtual network' (set to 'Vnet1'), 'Subnet' (set to 'Vnet1-1 (10.5.0.0/24)'), 'IP address assignment' (set to 'Static'), and 'Private IP address' (set to '10.5.0.200'). At the bottom, there are buttons for 'Review + create', 'Previous', 'Next: Tags >', and a link to 'Download a template for automation'.

Microsoft Azure

Home > New > Create load balancer

### Create load balancer

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

**PROJECT DETAILS**

- \* Subscription: [Dropdown]
- \* Resource group: TestGroup1 [Create new](#)

**INSTANCE DETAILS**

- \* Name: TestLoadBalancer ✓
- \* Region: Japan East
- \* Type: ☒ Internal ☐ Public
- \* SKU: ☒ Basic ☐ Standard

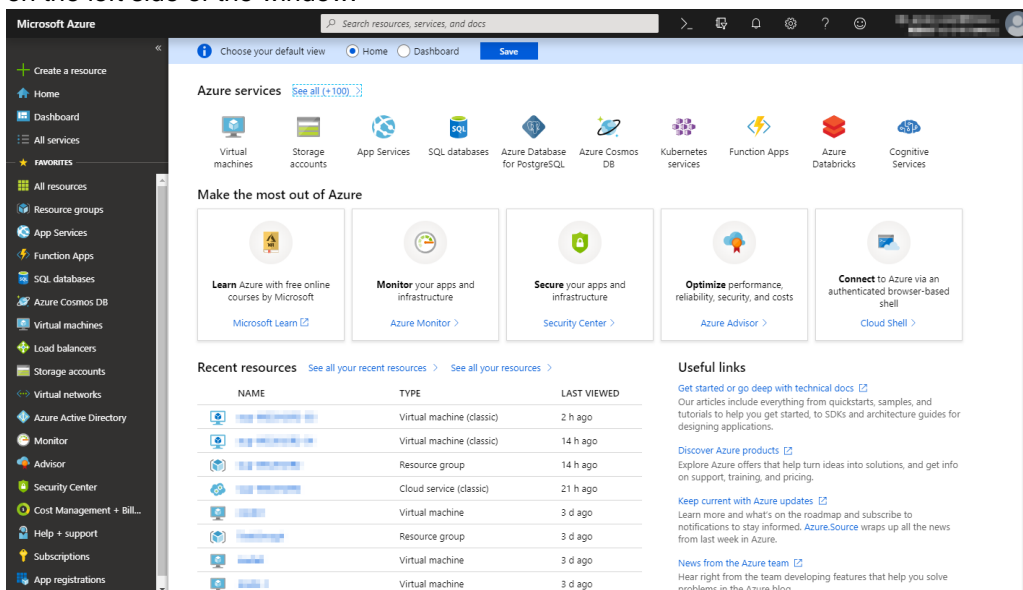
**CONFIGURE VIRTUAL NETWORK**

- \* Virtual network: Vnet1
- \* Subnet: Vnet1-1 (10.5.0.0/24) [Manage subnet configuration](#)
- \* IP address assignment: ☒ Static ☐ Dynamic
- \* Private IP address: 10.5.0.200 ✓

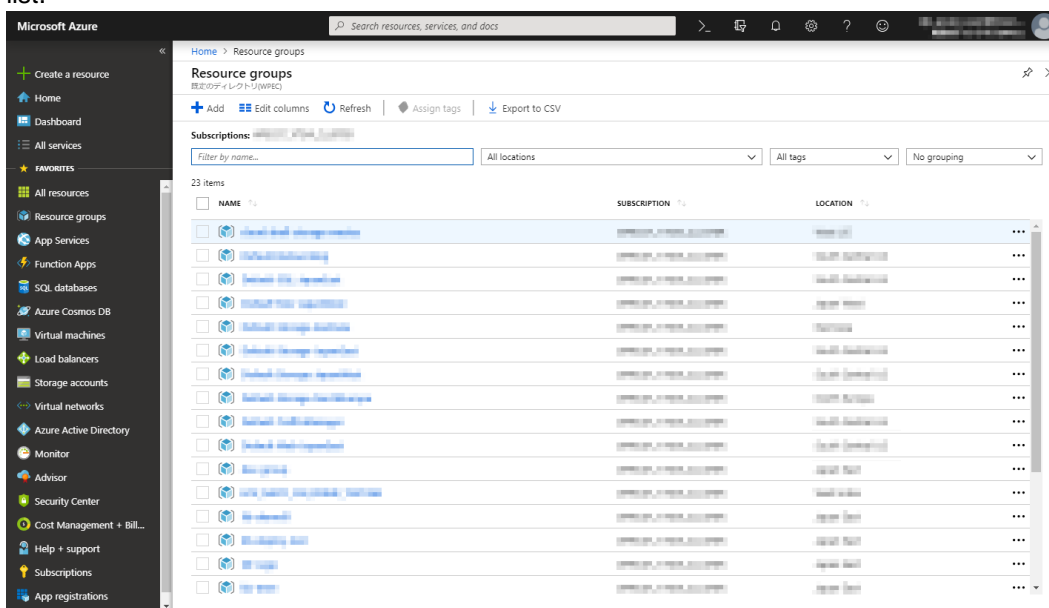
[Review + create](#) [Previous](#) [Next: Tags >](#) [Download a template for automation](#)

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

1. Associate a virtual machine registered to the availability set to the load balancer. After the load balancer has been deployed, select **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 Delete Export to CSV

Subscription (change)  
Subscription ID  
Tags (change)  
Click here to add tags

Deployments  
4 Succeeded

Filter by name... All types All locations No grouping

9 items Show hidden types

NAME	TYPE	LOCATION
node-1	Virtual machine	Japan East
node-1_OsDisk_1_7f486cd179fe4c7783627bb925385b6b	Disk	Japan East
node-1176	Network interface	Japan East
node-18lob1	Disk	Japan East
node-2	Virtual machine	Japan East
node-2_OsDisk_1_bf9c31e2cfb44f0398bf6d67ced7f9a1f	Disk	Japan East
node-231	Network interface	Japan East
node-28lob1	Disk	Japan East
testgroupdiag210	Storage account	Japan East
TestLoadBalancer	Load balancer	Japan East
Vnet1	Virtual network	Japan East

4. Select Backend pools.

Microsoft Azure

Home > Resource groups > TestGroup1 > TestLoadBalancer

TestLoadBalancer  
Load balancer

Search (Ctrl+/)

Move Delete Refresh

Resource group (change)  
TestGroup1

Location  
Japan East

Subscription (change)

Subscription ID

SKU  
Basic

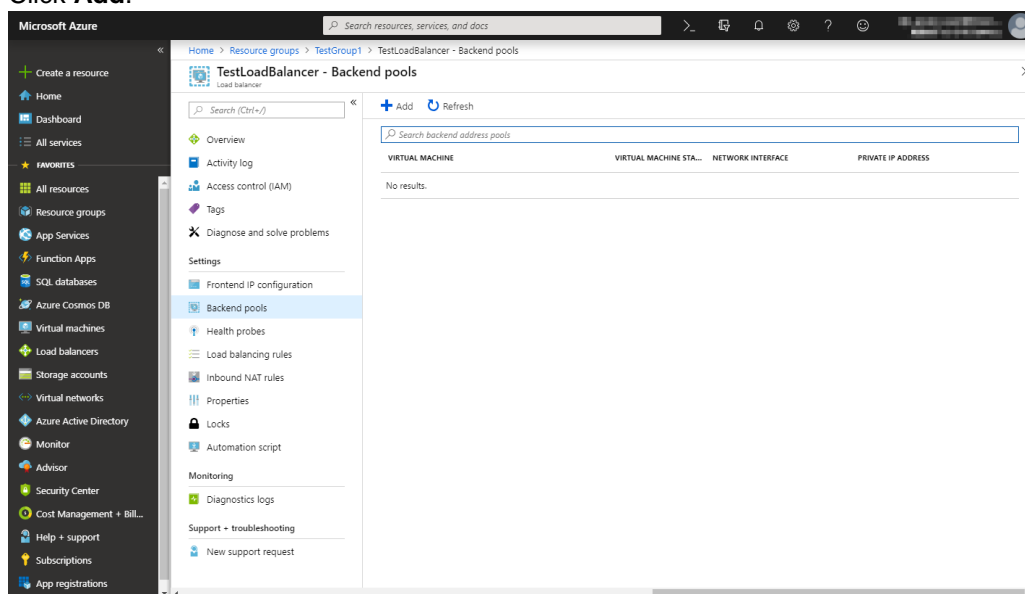
Tags (change)  
Click here to add tags

Backend pool  
Health probe  
Load balancing rule  
NAT rules  
0 inbound  
Private IP address  
10.5.0.200

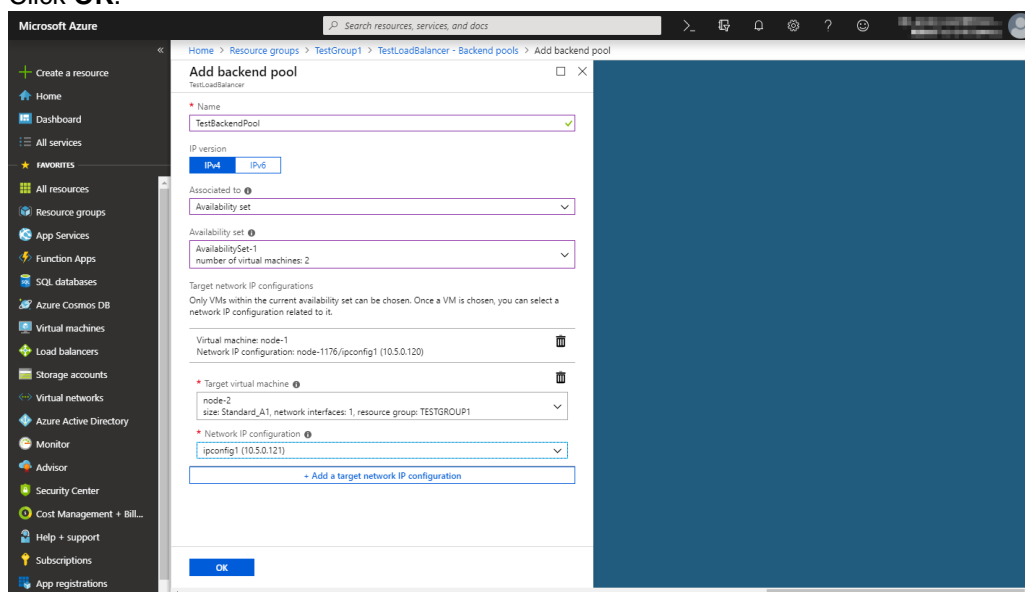
Frontend IP configuration  
Backend pools  
Health probes  
Load balancing rules  
Inbound NAT rules  
Properties  
Locks  
Automation script  
Monitoring  
Diagnostics logs  
Support + troubleshooting  
New support request



## 5. Click **Add**.

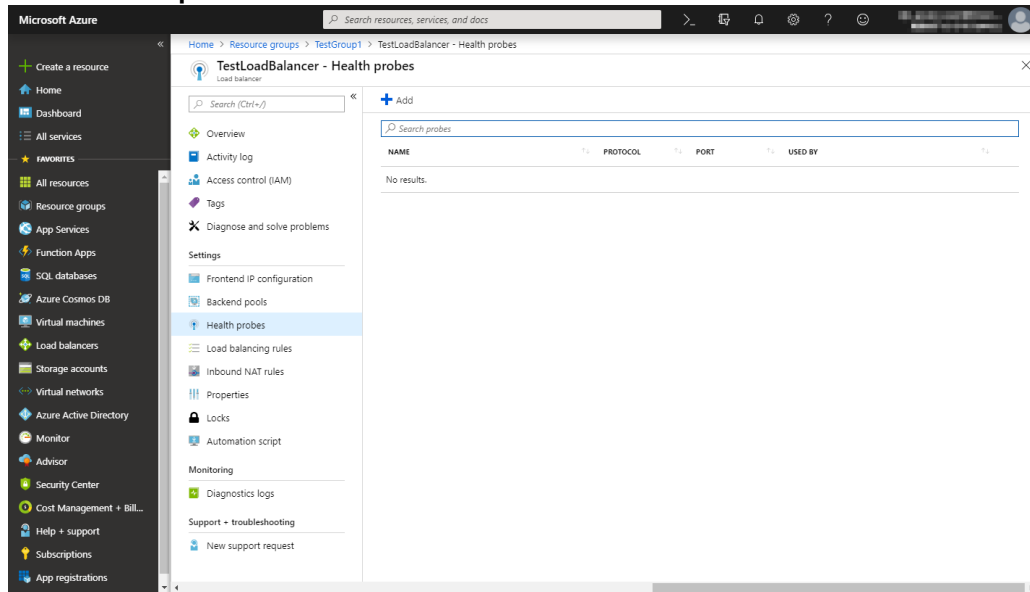


6. The **Add backend pool** blade is displayed. Specify **Name**.
7. For **Associated to**, select **Availability set**.
8. Specify **Availability set**.
9. Click **Add a target network IP configuration**.
10. Specify the target virtual machine for **Target virtual machine** and **Network IP configuration**.
11. Repeat steps 9 and 10 as many times as the number of target virtual machines.
12. Click **OK**.



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

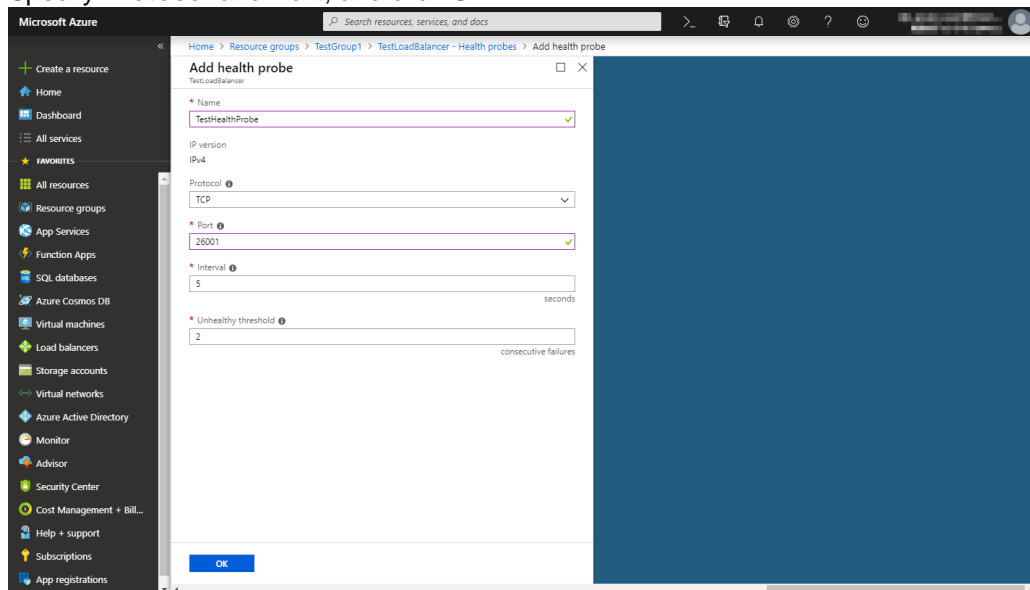
### 1. Select Health probes.



### 2. Click Add.

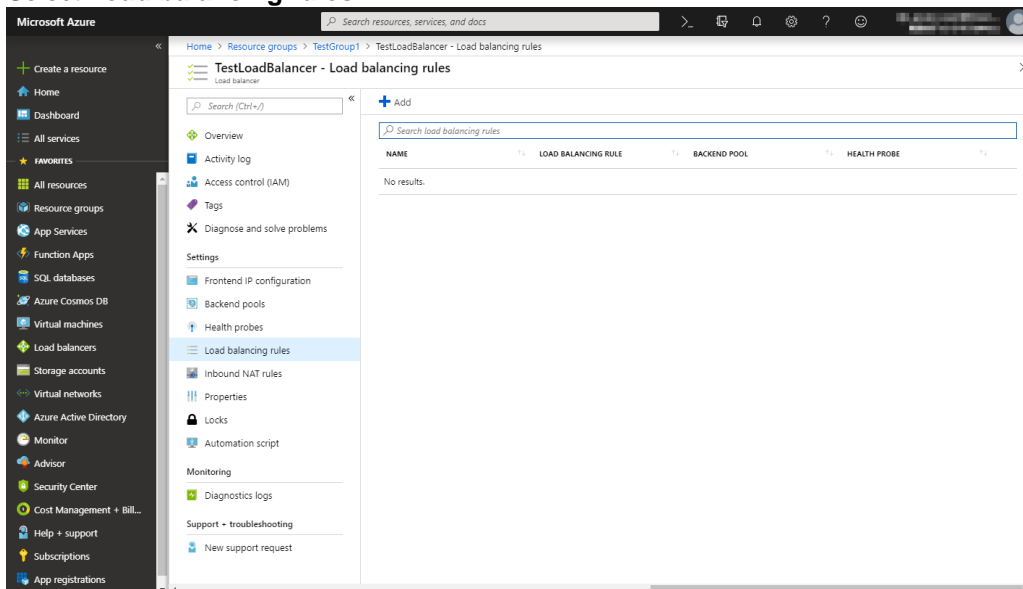
### 3. The Add health probe blade is displayed. Specify Name.

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



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

### 1. Select Load balancing rules.

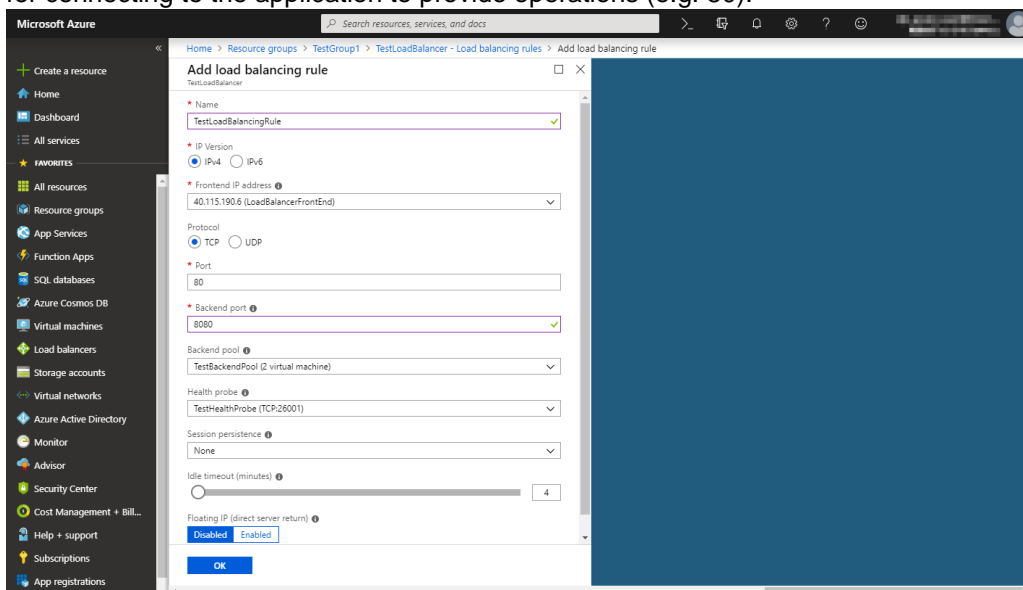


### 2. Click Add.

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

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

For using DSR, set the same port number to **Port** and **Backend port** and set **Floating IP (Direct Server Return)** to Enabled, and then select **OK**. In that case, specify the port number for connecting to the application to provide operations (e.g. 80).



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

For each procedure, see "Settings after configuring hardware" in Chapter 1, "Determining a system configuration" in the *Installation and Configuration Guide*.

**11) Installing EXPRESSCLUSTER**

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

After installation is complete, restart the OS.

**12) Registering the EXPRESSCLUSTER license**

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

## 5.3 Configuring the EXPRESSCLUSTER settings

For the Cluster WebUI 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)

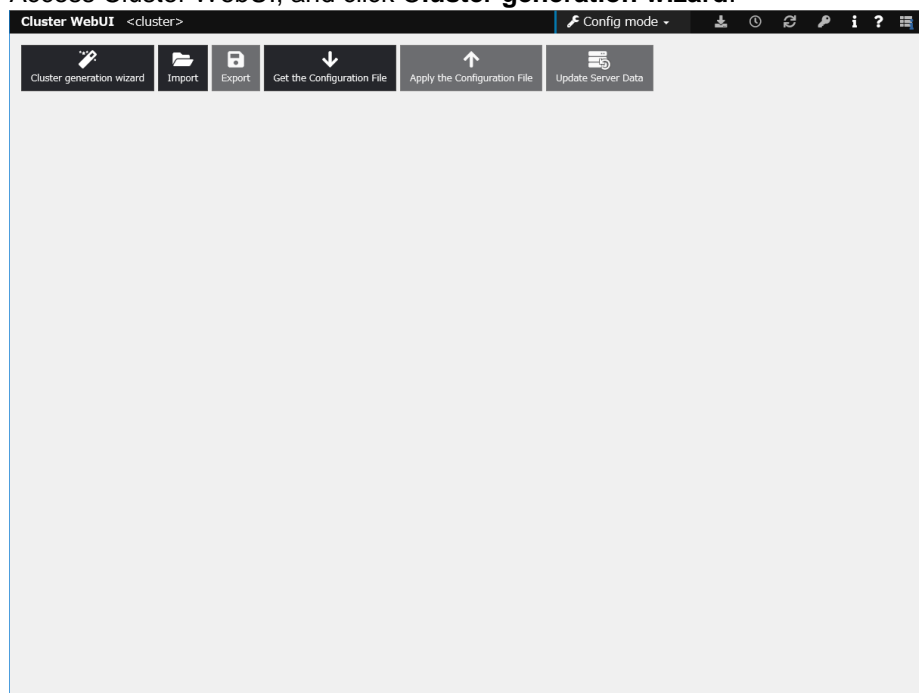
For the settings of other resources and monitor resources, see the *Installation and Configuration Guide* and the *Reference Guide*.

### 1) Creating a cluster

Start the cluster generation wizard to create a cluster.

#### ◆ Creating a cluster

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



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

Cluster generation wizard

Cluster

Basic Settings

Interconnect

NP Resolution

Group

Monitor

Cluster Name\*

Cluster1

Comment

Language\*

English

Management IP Address

Start generating the cluster.

Enter the cluster name, and then select the language (locale) of the environment that runs WebManager.

If using the integrated WebManager to manage multiple clusters, specify a unique cluster name to identify the cluster.

The management IP address is a floating IP address used for a WebManager connection. If establishing connections by specifying each server IP address, the management IP address can be omitted.

To continue, click [Next].

Back

Next

Cancel

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

Add server

Server Name or IP Address\*

10.5.0.121

Enter an IP address or a server name.

When entering a server name, name resolution is necessary.

Both IPv4 and IPv6 for IP address can be used.

When entering an IP address, the server name is automatically acquired.

OK

Cancel

Cluster generation wizard

Cluster

Basic Settings

Interconnect

NP Resolution

Group

Monitor

Add

Remove

Server Definitions

Order	Name
Master server	node-1
1	node-2

Up

Down

Server Group Definition

Settings

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.

Back

Next

Cancel

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

Cluster generation wizard

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

Properties Add Remove

Interconnect List

Priority	Type	MDC	node-1	node-2
1	Kernel Mode	Do Not Use	10.5.0.120	10.5.0.121

↑ ↓

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

Back Next Cancel

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

Cluster generation wizard

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

Properties Add Remove

NP Resolution List

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

Tuning

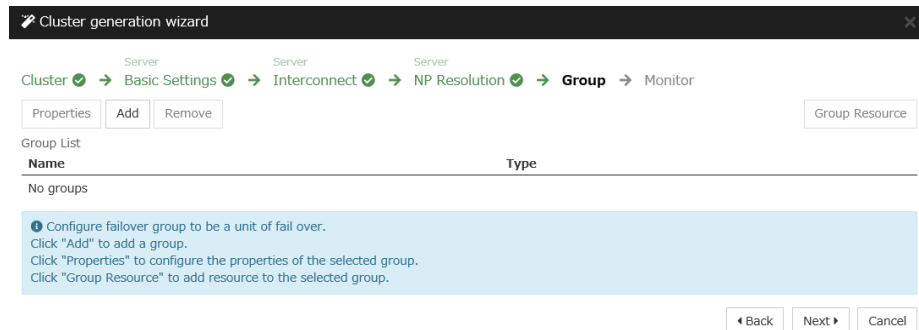
Configure network partition (NP) resolution function.  
Click "Add" to add NP resolution resource and select the type.  
For "COM" setting, click each server column cell to configure COM port.  
For "DISK" setting, click each server column cell to configure driver letter of the partition for disk heartbeat.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

Back Next Cancel

## 2) Adding a group resource

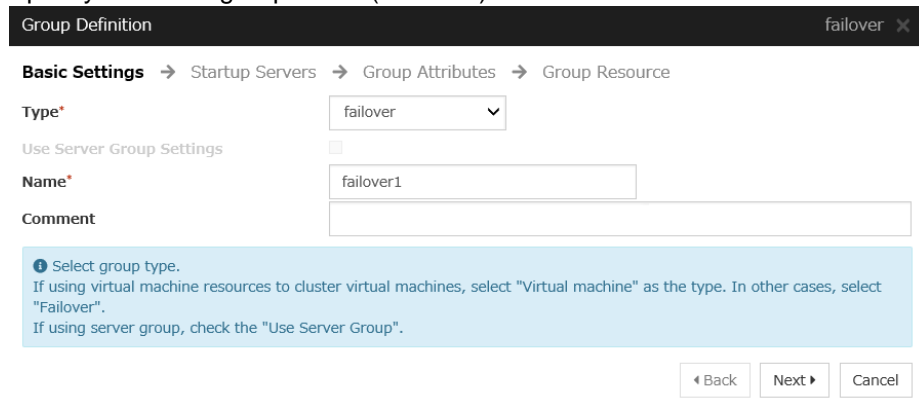
- ◆ Defining a group  
Create a failover group.

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



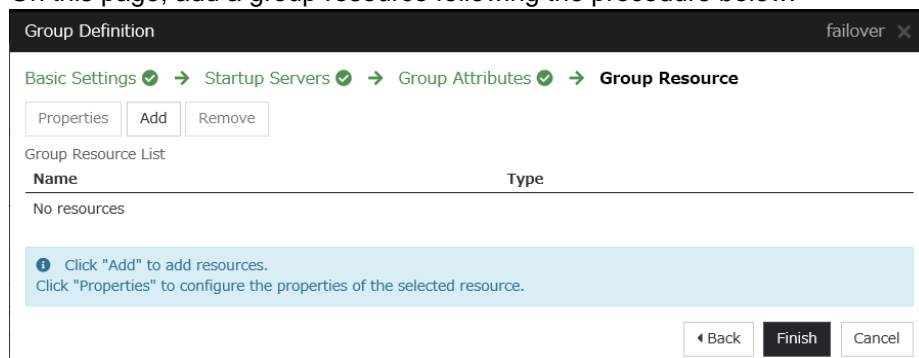
The screenshot shows the 'Cluster generation wizard' window. The progress bar indicates the following steps: Cluster (checked), Basic Settings (checked), Interconnect (checked), NP Resolution (checked), **Group** (active), and Monitor. Below the progress bar are buttons for 'Properties', 'Add', and 'Remove'. A 'Group Resource' button is also visible. The 'Group List' table is empty, showing 'No groups'. A blue information box contains instructions: 'Configure failover group to be a unit of fail over. Click "Add" to add a group. Click "Properties" to configure the properties of the selected group. Click "Group Resource" to add resource to the selected group.' Navigation buttons at the bottom are 'Back', 'Next', and 'Cancel'.

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



The screenshot shows the 'Group Definition' window for a group named 'failover'. The progress bar shows: Basic Settings (active), Startup Servers, Group Attributes, and Group Resource. The 'Type' dropdown is set to 'failover'. The 'Use Server Group Settings' checkbox is unchecked. The 'Name' field contains 'failover1'. The 'Comment' field is empty. A blue information box contains instructions: 'Select group type. If using virtual machine resources to cluster virtual machines, select "Virtual machine" as the type. In other cases, select "Failover". If using server group, check the "Use Server Group".' Navigation buttons at the bottom are 'Back', 'Next', and 'Cancel'.

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



The screenshot shows the 'Group Definition' window for a group named 'failover', specifically the 'Group Resource' page. The progress bar shows: Basic Settings (checked), Startup Servers (checked), Group Attributes (checked), and **Group Resource** (active). Below the progress bar are buttons for 'Properties', 'Add', and 'Remove'. The 'Group Resource List' table is empty, showing 'No resources'. A blue information box contains instructions: 'Click "Add" to add resources. Click "Properties" to configure the properties of the selected resource.' Navigation buttons at the bottom are 'Back', 'Finish', and 'Cancel'.



◆ Mirror disk resource

Create a mirror disk resource.

For details, see "Understanding mirror disk resources" in Chapter 5, "Group resource details" in the *Reference Guide*.

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

Resource Definition of Group | failover1 md X

Info → Dependency → Recovery Operation → Details

Type\* Mirror disk resource ▼

Name\* md

Comment

Get license information

Select the type of group resource and enter its name.

◀ Back Next ▶ Cancel

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

Resource Definition of Group | failover1 md X

Info ✓ → Dependency ✓ → Recovery Operation ✓ → Details

Mirror Disk No.\* 1 ▼

Data Partition Drive Letter\*

Cluster Partition Drive Letter\*

Cluster Partition Offset Index\* 0 ▼

Mirror Disk Connect Select

Servers that can run the group

Name	Data Partition	Cluster Partition
node-1		
node-2		

◀ Add ▶

→ Remove

Edit

Add Servers that can run the group

Tuning

◀ Back Finish Cancel

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

Selection of partition

Obtain information

Connect

Data Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	71678MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

Cluster Partition

Volume	Disk No.	Partition No.	Size	GUID
	0	1	500MB	
D:¥	1	1	71678MB	
F:¥	2	1	1024MB	
C:¥	0	2	129546MB	
G:¥	2	2	19453MB	

OK

Cancel

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

Resource Definition of Group | failover1

md x

Info ✓ → Dependency ✓ → Recovery Operation ✓ → Details

Mirror Disk No.\*

1 ▼

Data Partition Drive Letter\*

G:

Cluster Partition Drive Letter\*

F:

Cluster Partition Offset Index\*

0 ▼

Mirror Disk Connect

Select

Servers that can run the group

Name	Data Partition	Cluster Partition
node-1		
node-2		

← Add

→ Remove

Edit

Tuning

◀ Back

Finish

Cancel

- ◆ **Azure probe port resource**  
When EXPRESSCLUSTER is used on Microsoft Azure, EXPRESSCLUSTER provides a mechanism to wait for alive monitoring from a load balancer on a port specific to a node in which operations are running.

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

- Click **Add** on the **Group Resource List** page.

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

- The **Dependency** window is displayed. Click **Next** without specifying anything.
- The **Recovery Operation** window is displayed. Click **Next**.
- For **Probeport**, enter the value specified for **Port** when configuring a load balancer (configuring health probe).

- Click **Finish**.

◆ Script resource (when DSR is used)

The addition of a script resource provides a mechanism to add/delete the frontend IP address to the loopback adapter along with the switching of the load balancer.

For details on script resources, refer to "Understanding script resources" in the *Reference Guide*.

- Click **Add** on the **Group Resource List** page.
- The **Resource Definition of Group | failover1** window is displayed. Select the type of the group resource (script resource) in the **Type** box and enter the group name (script1) in the **Name** box.
- Click **Next**.
- The **Dependency** window is displayed. Click **Next** without specifying anything.
- The **Recovery Operation** window is displayed. Click **Next**.
- Select start.bat and stop.bat, and then click **Edit**. For details on configuring scripts, refer to the following EXPRESSCLUSTER official blog (<https://jpn.nec.com/clusterpro/blog/20181031.html>) (Japanese only). The scripts described on the blog are just samples. Customize the scripts according to your environment.
- Click **Finish**.

### 3) Adding a monitor resource

- ◆ Azure probe port monitor resource

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

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

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

- ◆ Azure load balance monitor resource

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

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

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

#### 4) Applying the settings and starting the cluster

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

For details, refer to the following:

- *Installation and Configuration Guide*  
→ How to create a cluster

## 5.4 Verifying the created environment

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

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

1. Start the failover group (failover1) on the active node (node-1). In the Status tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node-1 is **Normal**.  
Additionally, for using DSR, perform a packet capture to confirm that communications are made between the IP address of the client and the frontend IP address of the load balancer.
2. Change **Operation Mode** to **Verification Mode** from the Cluster WebUI pull-down menu.
3. In the Status tab on the Cluster WebUI, click the **Enable dummy failure** icon of azureppw1 of Monitors.
4. After the Azure probe port resource (azurepp1) activated three times, the failover group (failover1) becomes abnormal and fails over to node-2. In the Status tab on the Cluster WebUI, confirm that **Group Status** of failover1 of node-2 is **Normal**.  
Also, confirm that access to the frontend IP and port of the Azure load balancer is normal after the failover.  
Additionally, for using DSR, perform a packet capture to confirm that communications are made between the IP address of the client and the frontend IP address of the load balancer.

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

## Chapter 6      Error Messages

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

- Chapter 9, “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"
- "Notes on Azure DNS monitor resources"

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

Please refer the following for details about memory preserving maintenance.

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

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

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

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

Please refer the following about the above:

*EXPRESSCLUSTER X Getting Started Guide*

- "Adjusting OS startup time" in Chapter 5, "Notes and Restrictions"

*EXPRESSCLUSTER X Reference Guide*

- "Timeout tab"



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

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

Please refer the following for details about memory preserving maintenance.

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

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

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

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

Please refer the following about the above:

*EXPRESSCLUSTER X Getting Started Guide*

- "Adjusting OS startup time" in Chapter 5, "Notes and Restrictions"

*EXPRESSCLUSTER X Reference Guide*

- "Timeout tab"