Quest® QoreStor™

Azure Deployment Guide

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OFANY KIND

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser’s personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal .

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

🟥 **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death**

! **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ℹ **IMPORTANT**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

QoreStor Azure Deployment Guide
Updated – August 10, 2021
Version – 7.0.1

Contents

1

Azure QoreStor

This document outlines the QoreStor Object Direct Images available in the Microsoft Azure Marketplace, as well as the steps to deploy an image into a subscription.

The images use blob storage for containing data and Azure Managed Disks for storing metadata.

The VM images are available at:

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/quest.qorestor_7_0_1

2

QoreStor tiers

There are three tiers available based on the following storage and performance requirements: Tier 1, Tier 2, and Tier 3.

NOTE: Azure includes both Compute and Storage costs in their monthly billing cycles.

QoreStor™ Tier 1

The following are the recommended virtual machine (VM) Instances that have been been validated for Tier 1. Tier1 Edition image can scale to a maximum capacity of 40TB.

Table 1: Recommended VM Instances for Tier 1

Series	Size	vCPU	Memory: GiB	Metadata disk usage	Max uncached disk throughput: IOPS / MBps	Max NICs / Expected network bandwidth (Mbps)
Esv3	Standard_E4s_v3	4	32	1 TB	6000/93/46	2 / 2,000

QoreStor™ Tier 2

The following are the recommended VM Instances that have been been validated for Tier 2. Tier2 Edition image can scale to a maximum capacity of 150 TB.

Table 2: Recommended VM instances for Tier 2

Series	Size	vCPU	Memory: GiB	Metadata disk usage	Max uncached disk throughput: IOPS / MBps	Max NICs / Expected network bandwidth (Mbps)
DSv3	Standard_D8s_v3	8	32	4TB	12000/187/93	4 / 4,000

QoreStor™ Tier 3

The following are the recommended VM Instances that have been been validated for Tier 3. Tier3 Edition image can scale to a maximum capacity of 360 TB.

Table 3: Recommended VM instances for Tier 3

Series	Size	vCPU	Memory: GiB	Metadata disk usage	Max uncached disk throughput: IOPS / MBps	Max NICs / Expected network bandwidth (Mbps)
DSv3	Standard_D32_v3	32	128	10 TB	48000/750/375	8/16000

2

Deployment

The steps below describe the process to deploy a QoreStor virtual machine (VM) from the Azure Marketplace. For clarity, the procedure is subdivided into the sections below:

- Prerequisite
- Deploying the image
- Creating the virtual machine
- Accessing and configuring the virtual machine
- Port usage

Prerequisite

The following procedures assume that you have a Microsoft Azure storage account and that you are familiar with Azure Marketplace and the Azure user interface. We recommend configuring private endpoint for the Azure storage account to be used for blob storage for object direct deployments. For optimal performance, the storage account and the Qorestor instance reside in the same region.

For details on configuring a storage account with a private endpoint, see https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal#create-storage-account-with-a-private-endpoint.

Deploying the image

In Azure Marketplace, complete the following steps.

To deploy the image

1 Click https://azuremarketplace.microsoft.com/en-us/marketplace/apps/quest.qorestor-701?tab=Overview.

2 On the product page, click on **Get it Now.**

3 From the drop-down menu under Software plan, select the desired tier, and then click **Continue**.

The virtual machine you selected opens in the Azure portal.

4 Click **Create.**

Creating the virtual machine

In the Azure user interface, complete the following steps.

To create the virtual machine

1 On the **Basics** tab, enter the details described in the following table.

Table 1: Basics details

Option	Description
Subscription	Select your Azure storage account from the drop-down list.
Resource group	Select a resource group from the drop-down. If you do not have a resource group or want to use a different group, click **Create new**. For procedure instructions, consult Microsoft Azure documentation
Virtual machine name	Enter a name for the virtual machine that you want to create.
Region	Select your Azure region from the drop-down list.
Availability options	Select **No infrastructure redundancy required**.
Image	Select the QoreStor tier you want to use to create the virtual machine.
Azure Spot instance	Quest does not recommend selecting this option.
Size	Select the **Recommended by image publisher** option.
Authentication type	Select **Password**, and then enter the following information: • Create a username. • Create a password. • Re-enter the password For information about password requirements and limitations, see Azure documentation.

2 Click **Next**.

3 On the **Disks** tab, keep the following default options:

- **OS Disk Type — Premium SSD**
- **Encryption Type — Encryption-at-rest with a platform-managed key**

4 Click **Next: Networking**.

5 On the Networking tab, configure the settings to match your network configuration, or leave the default options.

> **NOTE:** The QoreStor image supports accelerated networking. A pre-configured network security group is provided.

Table 2: Networking details

Option	Description
Virtual network	Select a network from the drop-down. If you do not have a network established, or you want to use a different network than what appears in the drop-down list, click **Create new**. For more information about creating a network, see Microsoft Azure documentation.
Subnet	Select a subnet from the drop-down list. Optionally, to configure your subnet options, click **Manage subnet configuration**. For more information about managing subnet configurations, see Microsoft Azure documentation.
Public IP	Optionally, select a public IP for your virtual machine. If you do not have a public IP, or you want to use a different IP than what appears in the drop-down list, click **Create new**. For more information about creating an IP, see Microsoft Azure documentation.
NIC network security group	Select **Advanced**.
Configure network security group	Select a network security group from the drop-down list. If you do not have an existing Network Security Group, or you want to use dedicated Network Security Group than what appears in the drop-down list, click **Create new**. For more information about creating a Network Security group, see Microsoft Azure documentation.
Accelerated networking	Quest recommends selecting this option.
Place this virtual machine behind an existing load balancing solution?	Quest does not recommend selecting this option.

6 Click **Next: Management**.

7 On the Management tab, ensure that all options are disabled or not selected.

> **NOTE:** The default for the **Boot diagnostics** option is Disable, but this setting is not required.

> **CAUTION: Operating system updates are not automatic and must be performed by the administrator.**

8 Click **Next: Advanced**.

9 On the Advanced tab, select **Enable user data**.

10 Under User data, enter the following commands:

```
cloud-container: <user named container>
connection-string: <connection string to the customer storage account>
```

> **NOTE:** You can find the connection string for your Azure Storage account in the Azure UI under Access Keys.

CAUTION: Container names must start or end with a letter or number, and can container only letters, numbers, and the dash (-) character. Every dash (-) character must be immediately preceded and followed by a letter or number; consecutive dashes are not permitted in container names. All letters in a container name must be lowercase. Container names must be from 3 through 63 characters long.

11. Click **Next: Tags**.
12. On the Tags tab, add any required tags.
13. Click **Review + Create**.
14. On the Review + create tab, verify that your selections are correct, and then enter the following information:

Table 3: Contact details

Option	Description
Name	Enter the name of the point of contact for the Azure account.
Preferred e-mail address	Enter the email address for the point of contact.
Preferred phone number	Enter the phone number for the point of contact.

15. Click **Create**.
16. After the deployment is complete, click **Go to resource**.

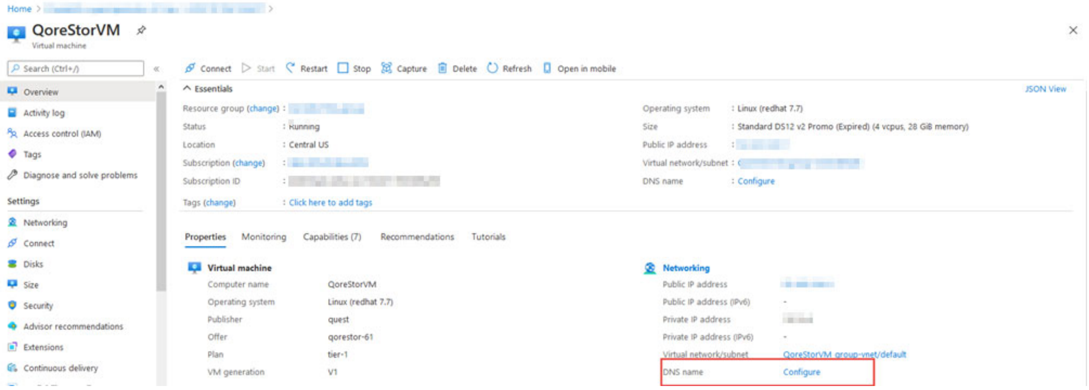
Accessing and configuring the virtual machine

NOTE: If you recently created the virtual machine, it is recommended that you wait 3 or 4 minutes before you begin this procedure.

To access and configure the virtual machine

1. By default, the instance does not have the DNS name configured. To configure the DNS name, find the **DNS name** field in the **Networking** section, and then click **Configure**.

Figure 1: QoreStorVM page in Azure



Resource group (change) : [redacted]
Status : Running
Location : Central US
Subscription (change) : [redacted]
Subscription ID : [redacted]
Tags (change) : Click here to add tags

Operating system : Linux (redhat 7.7)
Size : Standard DS12 v2 Promo (Expired) (4 vcpus, 28 GiB memory)
Public IP address : [redacted]
Virtual network/subnet : [redacted]
DNS name : Configure

Virtual machine

Computer name	QoreStorVM
Operating system	Linux (redhat 7.7)
Publisher	quest
Offer	qorestor-61
Plan	tier-1
VM generation	V1

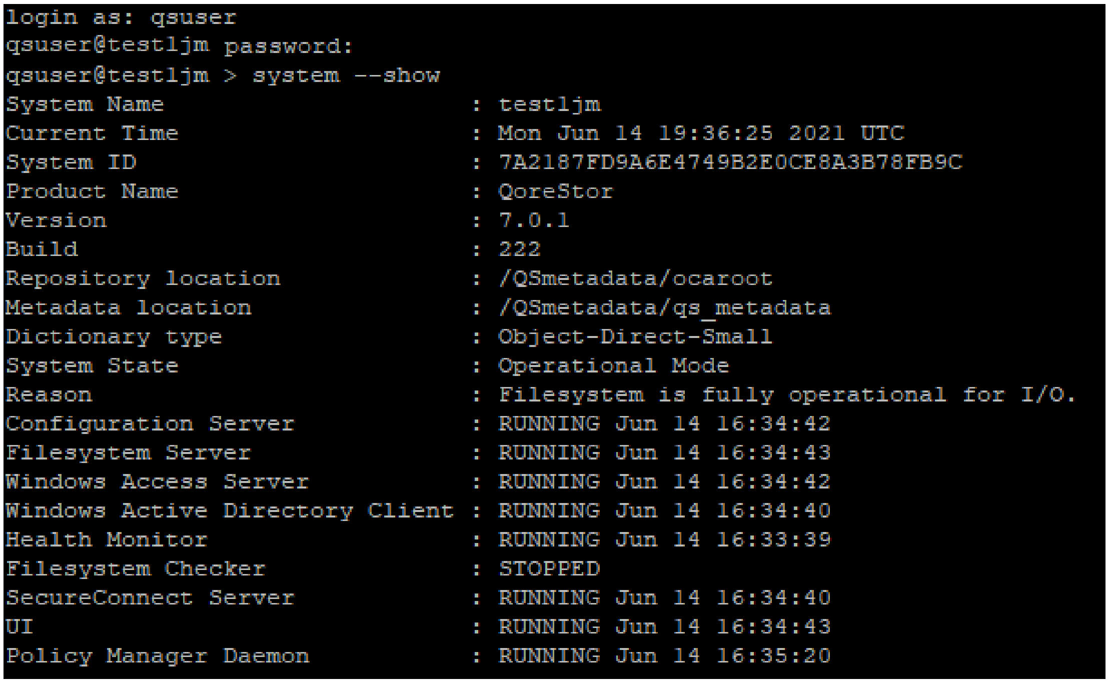
Networking

Public IP address	[redacted]
Public IP address (IPv6)	-
Private IP address	[redacted]
Private IP address (IPv6)	-
Virtual network/subnet	QoreStorVM_group-vnet/default
DNS name	Configure

2. By default, Azure provides the **<region>.cloudapp.azure.com** domain. Edit the options for the name based on your Public IP configuration, and then click **Save**.
3. Open a SSH session to the Public IP or DNS name.
4. In the SSH session, provide the credentials from the Deploying the image section of this guide.

5 After you log in, verify the filesystem is operational for I/O using the `system -show` command.

Figure 2: Filesystem list confirming operations



```
login as: qsuser
qsuser@testljm password:
qsuser@testljm > system --show
System Name                       : testljm
Current Time                      : Mon Jun 14 19:36:25 2021 UTC
System ID                         : 7A2187FD9A6E4749B2E0CE8A3B78FB9C
Product Name                      : QoreStor
Version                           : 7.0.1
Build                             : 222
Repository location               : /QSmetadata/ocaroot
Metadata location                 : /QSmetadata/qs_metadata
Dictionary type                   : Object-Direct-Small
System State                      : Operational Mode
Reason                            : Filesystem is fully operational for I/O.
Configuration Server              : RUNNING Jun 14 16:34:42
Filesystem Server                 : RUNNING Jun 14 16:34:43
Windows Access Server             : RUNNING Jun 14 16:34:42
Windows Active Directory Client   : RUNNING Jun 14 16:34:40
Health Monitor                    : RUNNING Jun 14 16:33:39
Filesystem Checker                : STOPPED
SecureConnect Server              : RUNNING Jun 14 16:34:40
UI                                : RUNNING Jun 14 16:34:43
Policy Manager Daemon             : RUNNING Jun 14 16:35:20
```

IMPORTANT: If the system appears in manual intervention mode for the reason, “Configuration Service failed to start due to object direct is not configured or Object Storage is offline. Object Direct marker detected,” then likely incorrect information was entered into the **user data** field during the Deploying the image procedure in this guide.

6 If the system is in Manual Intervention mode, use the following command to update the Azure Blob Storage account connection string:

```
object_direct --update_sentinel --cloud_container <containername> --
cloud_provider AZURE
```

NOTE: The system prompts you for the connection string in secret.

7 To access the QoreStor UI, use the public IP assigned in the section “Creating Virtual Machine”. The URL for accessing QoreStor UI would be **https://<public_ip_of_virutal_machine>:5233**.

Port usage

QoreStor uses certain ports for the services mentioned in the following table. The table also mentions the recommended network group settings (NSG) in Azure for each of the ports. Please refer to the next section for instructions on how to change the default/recommended NSG settings.

Table 4: Port functions and settings

Component / Function	Ports used	Protocol	Details	Default Network Security Group setting in Azure
SSH	22	TCP	SSH uses port 22. We recommend keeping this port open to enable secure connections within and from outside the QS	22: ENABLE
UI	80	HTTP	80 is HTTP port and newer QoreStor releases no longer use it. Quest does not recommend exposing this port to a public network.	80: DISABLE
	5233	TCP	QS uses 5233 for HTTPS connections (and not 443). Since this connection is secure, the port remains open in default NSG settings for all incoming traffic.	5233: ENABLE
Object (S3)	9000	TCP	Object Tier uses port 9000 for namespace as well as data transfer. QoreStor uses Minio front-end for object client interface. Currently, QoreStor does not support Secure Connect with Minio, but QoreStor uses port 9000 for both HTTP and HTTPS protocols. By default, NSG disables port 9000. However, if customer wants to use Object Tier, the port needs to be enabled in NSG.	9000: DISABLE
RDA-NDMP	12000-12127	ANY	These ports are used for RDA based NDMP. By default, they are disabled in NSG. Each NDMP needs 2 ports (internal port used by NDMP and OST servers + filer port to transfer data). In general, only 5 are used at any time. So, if customers intend to use NDMP over RDA, 5*2=10 ports are typically enough. Customers need to enable the ports using a range specification in NSG settings. We recommend 12000-12009.	12000-12127: DISABLE
Secure Connect	9443	ANY	Port used by secure connect. Secure connect is enabled by default and we recommend keeping this port open in NSG settings.	9443: ENABLE

Configuring Azure Network Security Group settings

The settings for enabling or disabling the Network Security Group (NSG) settings are available in Azure using the following instructions.

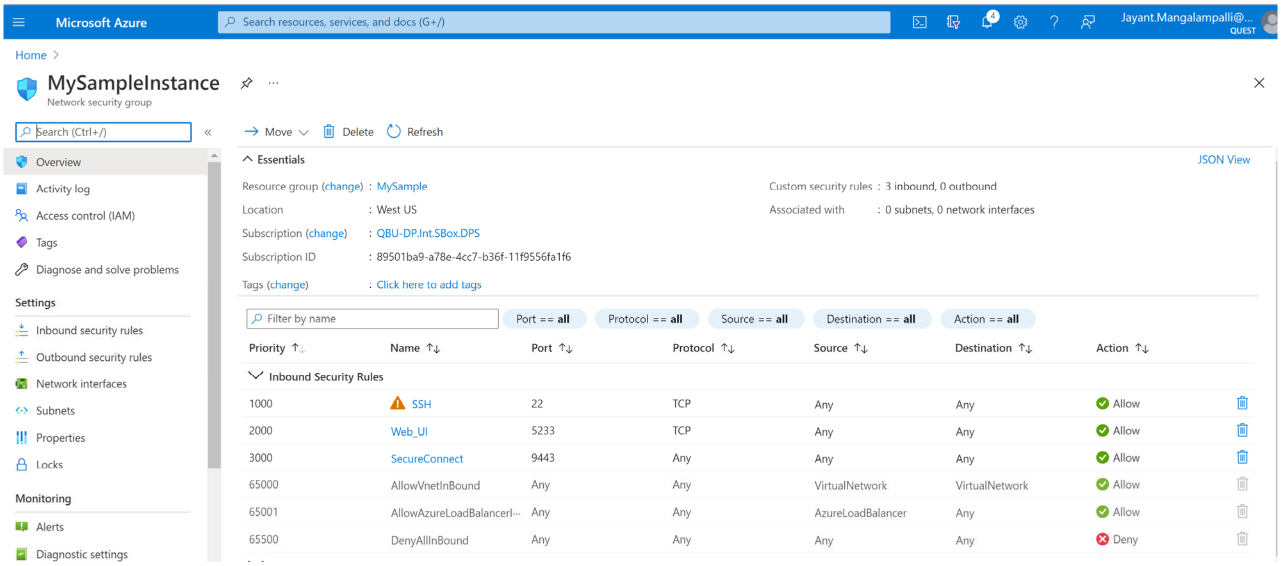
To configure Azure Network Security Group settings

1. In Azure console, find “Services” and click on “Network security groups”.
2. Click the NSG name you want to modify. This is the same NSG that is deployed with the Azure Marketplace image of QoreStor.

> **NOTE:** Any modification to this NSG will change the default settlings recommended by QoreStor.

3. After you click the NSG name, a settings page like the one in the following image shows where you can modify the network settings.

Figure 3: Overview of network settings in Azure



MySampleInstance

Network security group

Resource group (change) : MySample

Location : West US

Subscription (change) : QBU-DP.Int.SBox.DPS

Subscription ID : 89501ba9-a78e-4cc7-b36f-11f9556fa1f6

Tags (change) : Click here to add tags

Custom security rules : 3 inbound, 0 outbound

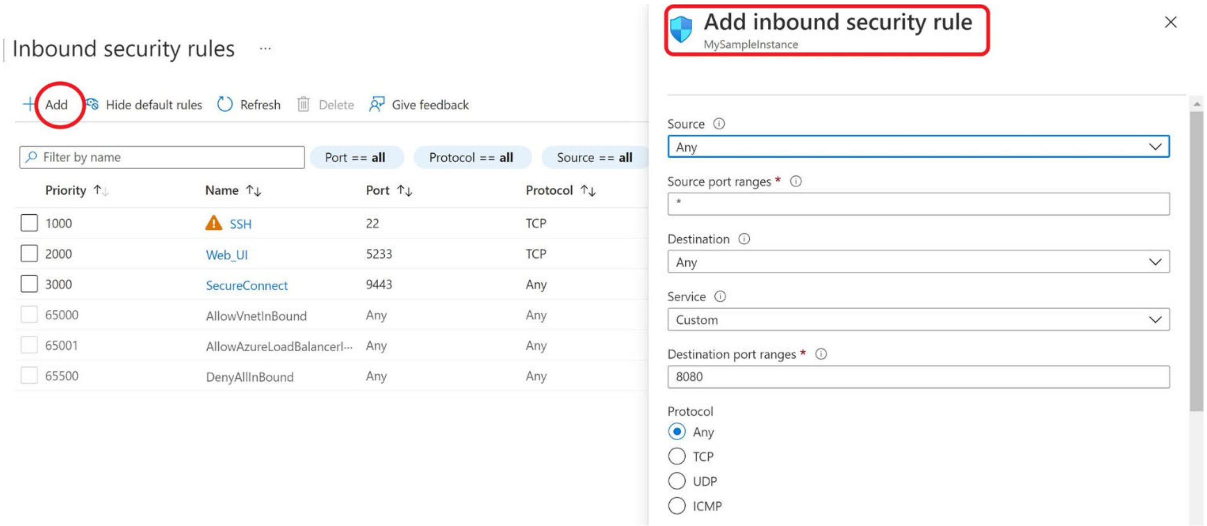
Associated with : 0 subnets, 0 network interfaces

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
1000	⚠ SSH	22	TCP	Any	Any	✓ Allow
2000	Web_UI	5233	TCP	Any	Any	✓ Allow
3000	SecureConnect	9443	Any	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerI···	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

4. When opening an additional port, to add inbound rules for that specific port, click **Inbound security rules** on the left side, and then click the **Add** tab on the top side of the page.

   The following dialog opens.

Figure 4: Inbound security rules table and dialog in Azure



	Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓
□	1000	⚠ SSH	22	TCP
□	2000	Web_UI	5233	TCP
□	3000	SecureConnect	9443	Any
□	65000	AllowVnetInBound	Any	Any
□	65001	AllowAzureLoadBalancerI···	Any	Any
□	65500	DenyAllInBound	Any	Any

Add inbound security rule

MySampleInstance

Source ⓘ: Any

Source port ranges * ⓘ: *

Destination ⓘ: Any

Service ⓘ: Custom

Destination port ranges * ⓘ: 8080

Protocol

● Any

○ TCP

○ UDP

○ ICMP

5 On this dialog, you can add rules that open other ports. For example, if Object Tier is enabled, then the corresponding port – 9000 per the table in earlier section – needs to be open. In that case, complete the following options:

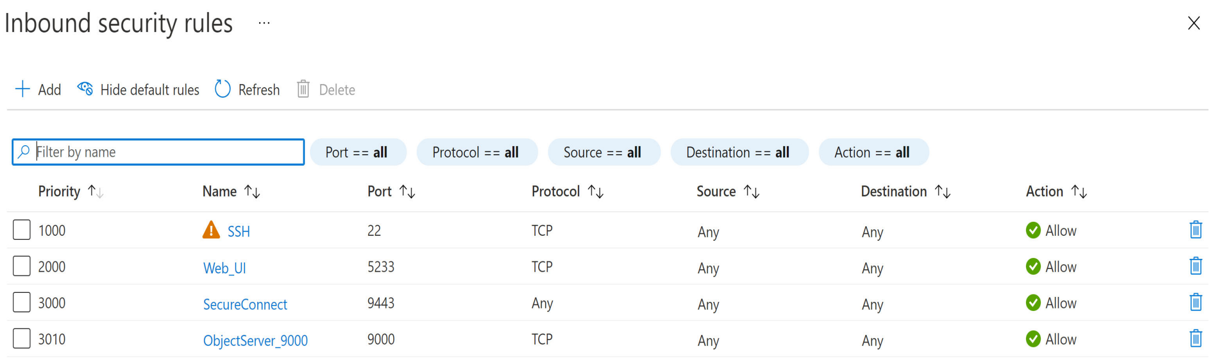
Table 5: Add inbound security rule options

Option	Description
Source	Select an IP or an Azure NSG. If the port can be used from any external interface, select **Any**.
Source port ranges	Select a port range on the specified source. To select any range, select *****.
Destination	Leave as the default selection, **Any**.
Service	Leave as the default selection, **Custom**.
Destination port ranges	(Required) Enter **9000** for this port.
Protocol	Select **TCP**.
Action	Select **Allow**.
Priority	Select an appropriate priority. The rules execute by priority, with the lowest number representing the highest priority. When selecting priorities, leave spaces between the numbers so that you can insert new priorities later.
Name	Enter an appropriate name for this rule; for example, ObjectServer_9000, which highlights the port number and the functionality. Add a description as needed.

6 Click **Add**.

The NSG Inbound rules will look like the following example.

Figure 5: Inbound security rules example



	Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
□	1000	⚠ SSH	22	TCP	Any	Any	✓ Allow
□	2000	Web_UI	5233	TCP	Any	Any	✓ Allow
□	3000	SecureConnect	9443	Any	Any	Any	✓ Allow
□	3010	ObjectServer_9000	9000	TCP	Any	Any	✓ Allow

You can add rules as needed for corresponding functionality. For enabling multiple ports (like the case of RDA-NDMP), NSG allows port ranges and comma-separated lists of ports so that multiple ports can be enabled as part of one rule. However, the Marketplace offer configuration does not allow for ranges or comma-separated ports, so a Marketplace image’s NSG template might mention each port number as a separate rule in such cases.