Quest® QoreStor™

# AWS Deployment Guide

### 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.**

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

QoreStor AWS Deployment Guide
Updated – September 27, 2023
Version – 7.2.1

# Contents

# 1

# AWS QoreStor

This document outlines the Quest® QoreStor™ Object Direct offerings available on the Amazon AWS Marketplace, as well as the steps to deploy an image into a subscription.

The images are based on the Oracle Enterprise Linux 8.8 operating system and support only the Object Direct mode of deployment.

# QoreStor tiers

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

## QoreStor™ Tier 1

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

**Table 1: Recommended VM Instances for Tier 1**

| Series | Instance Type | vCPU | Memory (GiB) | Instance Storage (GiB) | Metadata disk usage (TiB) |
|---|---|---|---|---|---|
| **m6i** | m6i.2xlarge | 8 | 32 | EBS-only | 1.5 |

## QoreStor™ Tier 2

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

**Table 2: Recommended VM instances for Tier 2**

| Series | Instance Type | vCPU | Memory: GiB | Instance Storage | Metadata disk usage (TiB) |
|---|---|---|---|---|---|
| **m6i** | m6i.2xlarge | 8 | 32 | EBS-only | 8 |
| | m6i.4xlarge | 16 | 64 | | |

# 3

# Deployment

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

- Prerequisite
- Deploying the image
- Port usage

# Prerequisite

The following procedures assume that you have an AWS account with IAM permissions for creating Amazon EC2 instances, Amazon S3 service, and Amazon Elastic Block Store services and that you are familiar with AWS Marketplace and the AWS user interface. For optimal performance, the S3 bucket for the Object storage backend and the QoreStor instance should reside in the same region.

# Deploying the image

In AWS Marketplace, complete the following steps.

***To deploy the image***

1. Log in to your AWS account.
2. Navigate to the Quest landing page on AWS Marketplace at:

   https://aws.amazon.com/marketplace/seller-profile?id=55447930-653f-4592-9bb6-8a420a580d71
3. Click QoreStor 7.2.1 (Object Direct).
4. On the product page, click **Continue to Subscribe**.
5. On the Subscribe page, click **Continue to Configuration**.
6. On the Configure page, select your fulfillment option and region, and then click **Continue to Launch**.
7. On the Launch page, in the Choose Action drop-down, select **Launch through EC2.**
8. On the **Choose Instance Type** tab, based on the deployment Tier, select the recommended AWS EC2 instance type from Tier 1 or Tier 2.
9. On the **Configure Instance** tab, under **User data**, select **As text** and enter the following details:

```
cloud-container: <S3_Bucketname>
connection-string: "accesskey=<>;secretkey=<>;region=<>;loglevel=warn"
```

> **NOTE:** This is an important step, and the two parameters need to be passed in colon-separated format as shown above to bring up the QoreStor in operational mode after deployment.

10. Leave the remaining tabs with the default entries, and then click **Review and Launch.**

11 In the pop-up window, either select an existing key pair or create a new key pair, select the acknowledgment, and then click **Launch Instances**.

**NOTE:** Password-based login is disabled by default. The initial login to the QoreStor instance must be through password-less SSH.

After the QoreStor instance deploys, take note of the public DNS name, and log in with the default user “ec2-user” using the previously selected private SSH key pair.

On the Linux Client, use the following command:

```
ssh -i /path/my-key-pair.pem ec2-user@my-instance-public-dns-name
```

For more information about connecting to a Linux instance, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstancesLinux.html.

12 Run 'system --show' and check System State is in ‘Operational Mode’.

**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.

13 If the system is in Manual Intervention mode, use the following command to update the AWS storage account connection string:

```
object_direct --update_sentinel --cloud_container <containername> --
cloud_provider AWS-S3
```

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

14 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 security group settings in AWS for each of the ports. Please refer to the next section for instructions on how to change the default/recommended EC2 security group settings.

**Table 4: Port functions and settings**

| Component / Function | Ports used | Protocol | Details | Default Security Group setting in AWS |
|---|---|---|---|---|
| SSH | 22 | TCP | SSH uses port 22. We recommend keeping this port open to enable secure connections within and from outside QoreStor. | 22: ENABLE |
| UI | 5233 | TCP | QoreStor uses 5233 for HTTPS connections (and not 443). Since this connection is secure, the port remains open in security group settings for all incoming traffic. | 5233: ENABLE |
| Object (S3) | 9001-9005 | TCP | Object container uses ports 9001-9005 for data transfer. By default, NSG disables access to these ports. However, to use an Object container, enable the ports in the security group. | 9001-9005: DISABLE |

| | | | | |
|---|---|---|---|---|
| Secure Connect | 9443 | ANY | Port used by secure connect. Secure connect is enabled by default and we recommend keeping this port open in security group settings. | 9443: ENABLE |

# Configuring AWS Security Groups settings

The settings for enabling or disabling ports in the EC2 Security Group (SG) settings are available in AWS using the following instructions.

### *To configure AWS EC2 Security Group settings*

1 In the AWS console, navigate to EC2 Dashboard and click **Security groups**.

2 Click the security group name you want to modify. This is the same **security group** that is deployed with the AWS Marketplace image of QoreStor.

**NOTE:** Any modification to this Security Group will change the default settings recommended by QoreStor.

3. After you click the SG name, a settings page like the one in the following image shows where you can modify the security group settings.
4. When opening an additional port, to add inbound rules for that specific port, click **Edit Inbound rules**, and then click the **Add Rule**, to get the option to add an additional port.
5. On this dialog, you can add rules that open other ports. For example, if the Object container is enabled, then the corresponding ports – 9001-9005 per the table in the earlier section – need to be open. In that case, complete the following options:

**Table 5: Add inbound security rule options**

| Option | Description |
|---|---|
| Type | Select TCP or UDP based on the port. In this case, for Object Container select “Custom TCP”. |
| Protocol | Gets populated based on Type. |
| Port Range | Input the port or port range based on the configuration required. Enter port range 9001-9005 for Object Container. |
| Source | Select an IP, CIDR range, or an AWS Security Group. If the port can be used from any external interface, select **Anywhere-IPv4**. |
| Description | Enter an appropriate name for this rule, ObjectServer. |

6. Click **Save Rules**.

   The Security Group Inbound rules will be saved and applied to the QoreStor Instance.

   You can add rules as needed for corresponding functionality. For enabling multiple ports, EC2 Security Group allows port ranges and comma-separated lists of ports so that multiple ports can be enabled as part of one rule. Refer to the *Networking Requirements* section in the *QoreStor Interoperability Guide* for more details about specific protocol ports to be enabled in the security group for enabling protocol access.