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 – July 19, 2022
Version – 7.1

Contents

AWS QoreStor **4**

QoreStor tiers **5**
QoreStor™ Tier 1 5
QoreStor™ Tier 2 5
QoreStor™ Tier 3 6

Deployment **7**
Prerequisite 7
Deploying the image 7
Port usage 8
Configuring AWS Network Security Group settings 9

1

AWS QoreStor

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

The images are compatible with the Oracle enterprise Linux 8.5 operating system and support only the Object Direct mode of deployment.

2

QoreStor tiers

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

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)	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 been validated for Tier 2. Tier 2 Edition image can scale to a maximum capacity of 150 TB.

Table 2: Recommended VM instances for Tier 2

Series	Size	vCPU	Memory: GiB	Instance Storage (GiB)	Metadata disk usage
M6i	M6i.2xlarge	8	32	EBS-only	8
	M6i.4xlarge	16	64		

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
M6i	M6i.8xlarge	128	EBS-only	18

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 a AWS storage account and that you are familiar with AWS Marketplace and the AWS user interface. We recommend configuring private endpoint for the AWS 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 guidance on dealing with AWS Service Limits, refer to this documentation: https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html.

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 at https://aws.amazon.com/marketplace/seller-profile?id=55447930-653f-4592-9bb6-8a420a580d71, and then click **QoreStor 7.1.1 (Object Direct)**.

3 On the product page, click **Continue to Subscribe**.

4 On the Subscribe page, click **Continue to Configuration**.

5 On the Configure page, select your fulfillment option and region, and then click **Continue to Launch**.

6 On the Launch page, In the Choose Action drop-down, select **Launch through EC2.**

7 On the **Choose Instance Type** tab, based on your storage requirements select the QoreStor instance type from Tier 1, Tier 2, and Tier 3.

8 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"
```

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

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

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

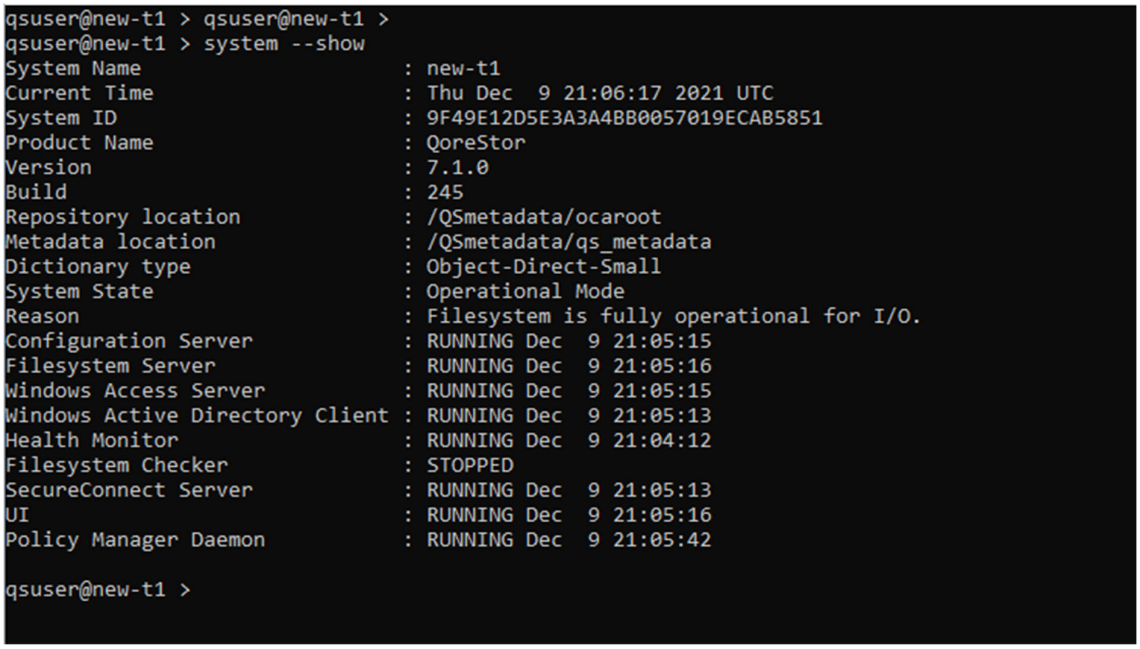
After the QoreStor instance deploys, take note of the public DNS name and login with the default user “ec2-user” using the previously selected private SSH key pair.

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.

Figure 2: Filesystem list confirming operations



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.

11 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
```

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

12 To access the QoreStor UI, use the public IP assigned in the section **Error! Reference source not found.**. 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 AWS 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 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 default NSG settings for all incoming traffic.	5233: ENABLE
Object (S3)	9000	TCP	Object container uses port 9000 for data transfer. By default, NSG disables port 9000. However, to use Object container, enable the port in NSG.	9000: 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 AWS Network Security Group settings

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

To configure AWS Network Security Group settings

1 In AWS console, find “Services” and click **Network security groups**.

13 Click the NSG name you want to modify. This is the same NSG that is deployed with the AWS Marketplace image of QoreStor.

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

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

15 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.

16 On this dialog, you can add rules that open other ports. For example, if Object container 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 AWS 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.

17 Click **Add**.

The NSG Inbound rules will look like the following example.

You can add rules as needed for corresponding functionality. For enabling multiple ports, 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.