Quorum®

onQ Release Notes

Version 3.6 SP1

Quorum®
2890 Zanker Road, Suite 102
San Jose, CA 95134 USA
Toll Free: +1-877-99-Quorum
Phone: +1-408-708-4500
Fax: +1-408-708-4503

Copyright © 2008–2013 QuorumLabs, Inc.

ALL RIGHTS RESERVED. No part of this publication may be reproduced in any form, by photocopy, microfilm, retrieval system, or by any other means now known or hereafter invented without the prior written permission of QuorumLabs, Inc.

The information in this publication has been carefully checked and is believed to be accurate. However, QuorumLabs, Inc. assumes no responsibility for inaccuracies. QuorumLabs, Inc. retains the right to make changes to this publication at any time without prior notice. QuorumLabs, Inc. does not assume any liability arising from the application or use of this publication or the product(s) described herein.

TRADEMARKS

All trademarks or registered trademarks used in this publication are the property of their respective owners.

Table of Contents

Preface 1

Online Help 1

Chapter Organization 1

1. What's New 3

2. Support 5

2.1 Platform Support 5

2.2 Hypervisor Support 6

2.3 Browser Support 6

2.4 Bare Metal Restore Support 7

2.5 Ontrack Support 7

3. Limitations 9

3.1 Linux RN Limitations 9

3.2 Windows Server Limitations 10

3.3 Volume Mount Limitations 12

3.4 CIFS Mount Limitations on Windows 12

3.5 Bare Metal Restore Limitations 13

3.6 Windows Cluster Services Limitations 14

4. Updates 17

4.1 Upgrade Support 17

4.2 Update Appliance software 18

Preface

This guide is intended for System Administrators who need to keep abreast of new onQ features and ongoing support and who want to upgrade their onQ Appliance.

Online Help

Online Help for onQ and Archive Vault products are available through their respective portals. Online documentation is available at:

Help	Where to go...
onQ	http://www.quorum.net/help/3.6SP1/onQ/index.html
AV	http://www.quorum.net/help/3.6SP1/Vault/index.html

Chapter Organization

The chapters and appendices of this manual are as follows:

- Chapter 1, *What's New*
- Chapter 2, *Support*
- Chapter 3, *Limitations*
- Chapter 4, *Updates*

1

What's New

This release includes the following new features and enhancements:

- **PCI compliance**: Hybrid Cloud, Quorum's DRaaS solution, is now certified PCI compliant. As the first vendor in the industry to offer cloud recovery that meets the payment card industry's (PCI) security specifications, Quorum ensures credit card data obtained by retail establishments, and any other organization that handles credit card information, is kept secure throughout the backup and recovery process.
- **Bare Metal Restore (BMR)**: The BMR wizard automates boot corrections by detecting the PN's os configuration and the required boot mode (BIOS/EFI). For more information, go to the Online Help.
- **CIFS Support**: onQ supports backing up of CIFS-enabled remote shares on the platforms outlined in Platform Support. These shares need be mounted when PNs are configured on the onQ for backup as outlined in Enable onQ to back up shared volumes. However, there are a few limitations as outlined in CIFS Mount Limitations on Windows.
- **Alert Throttling**: In this release, alerts are easier to manage. To minimize the number of email alerts that you receive, alerts are no longer sent as soon as they occur; rather, specific alerts are sent immediately while other, need-to-know alerts collect in a queue pending optimal delivery. Each alert now has a unique error code for identification purposes. Also, the daily report now summarizes alert activity.
- **Internet Explorer 11.0**. In this release, IE 11.0 is supported when using onQ Portal, including PN installations.
- **Windows Server 2012 R2, 64-bit**. Added support for PNs running Windows Server 2012 R2, Datacenter and Standard, 64-bit.
- **Orphan Snapshots**. onQ Portal enables you to search and delete orphan snapshots so that you can free up disk space on your onQ Appliances. For more information, go to Online Help

2

Support

- Platform Support
- Hypervisor Support
- Browser Support
- Bare Metal Restore Support
- Ontrack Support

2.1 Platform Support

Both physical and virtual PNs are supported on the following platforms:

Operating System	Backup Supported	RN Supported
Windows		
Windows Server 2012 R2, Datacenter and Standard, 64-bit	Yes	Yes
Windows Server 2012, Datacenter and Standard, 64-bit	Yes	Yes
Windows 2008 R2, 64-bit	Yes	Yes
Windows 2008, 32-bit and 64-bit	Yes	Yes
Windows 2003 R2, 32-bit and 64-bit	Yes	Yes
Windows 7, 64-bit	Yes	Yes
Linux		
Red Hat Enterprise Linux 5.6, 5.7, 5.8, 5.9, 6.0, 6.1, 6.2, 6.3; 32-bit and 64-bit.	Yes	Yes
Oracle Enterprise Linux 5.8, 32-bit and 64-bit	Yes	Yes

2.2 Hypervisor Support

The guest operating systems outlined in “Platform Support” on page 5 are supported on the following hypervisors:

Hypervisor	Version
VMWare ESX	4.0
VMWare ESXi	5.0 and 5.1.0
Hyper-V	6.x
XenServer	5.0, 5.5, and 6.0.2

2.3 Browser Support

onQ supports the following browsers:

Browser	onQ Portal	PN Installation (“Protect Me” button)
Mozilla Firefox 10.0 and above	Yes	No[a]
Internet Explorer 8, 9 10, and 11	Yes	Yes
Internet Explorer 7	No	Yes

a.Firefox is not supported for enrollment on 64-bit operating systems because Firefox is unable to retrieve the node information that’s required.

In addition:

- JRE (Java) 1.5 or above must be installed to use the RN console from the UI.

- You might need to modify security and popup settings for proper RN console operations from the UI.

2.4 Bare Metal Restore Support

A Bare Metal Restore (BMR) is supported on the following platforms:

Operating System	To Same Hardware	To Dissimilar Hardware
Windows Server 2012 R2, Datacenter and Standard, 64-bit	Yes	Yes
Windows Server 2012, Datacenter and Standard, 64-bit	Yes	Yes
Windows 2008 R2, 64-bit	Yes	Yes
Windows 2008, 32-bit and 64-bit	Yes	Yes
Windows 2003 R2, 32-bit and 64-bit	Yes	Yes

2.5 Ontrack Support

As outlined in Perform WSR Restore, you can use Kroll's Ontrack application to restore Exchange Server data and mailboxes.

Ontrack is independent of onQ; as such, onQ should work with any version of Ontrack so long as onQ supports the underlying operating system (see Platform Support).

Kroll OnTrack Power Controls for Exchange application version 7.0.x is required for using Ontrack with Exchange 2013, in order to support EDB files.

3

Limitations

- Linux RN Limitations
- Windows Server Limitations
- Volume Mount Limitations
- CIFS Mount Limitations on Windows
- Bare Metal Restore Limitations
- Windows Cluster Services Limitations

3.1 Linux RN Limitations

Recovery Nodes running Linux have the following limitations:

- To support booting of Recovery Nodes (RN) for RHEL 5.x servers, you must download the appropriate version of Xen-compatible kernel packages and install them on the Protected Nodes (PN) before enrolling or attempting to build the RNs for such clients. The installed Xen kernel will not be an active kernel on the PN; instead, that kernel will be used to boot the RNs. For more information, go to the Online Help.
- The filesystem format is required to be set in the Protection Node Configuration for each RN disk to ensure that onQ protection starts correctly.
- For RHEL 5.x, the root disk partition (`/`) must be set to Format (file system type) parameter `ext3` for the RN to boot correctly. The enrollment procedure, outlined in the Online Help, accounts for this limitation.
- After upgrading the onQ to 3.6, you need to do the following to upgrade your Linux nodes:
  - For 32-bit Linux nodes, after performing an automatically upgrade you must restart protection twice to upgrade the client services.
  - For 64-bit Linux nodes, the client services will not automatically

upgrade; therefore, you must run the `install.py` utility as outlined in the Online Help.

- Linux PNs may return 256 code during an auto-upgrade. If you encounter this error, restart (stop/start) protection to re-initiate the auto-upgrade.
- Network Manger on RHEL 5.9 (Tikanga) is required to be turned off to have self-test work correctly. Similar action need be taken if Kudzu services are running on the RHEL 5.x versions.
- BMR and incremental failback for Linux nodes are not supported in this release.

3.2 Windows Server Limitations

Consider the following limitations if any RN is running Windows Server:

- (*Windows Server 2012 & R2*) Any PN running XenTools 6.1 or later is not supported; in this case, the RN fails to boot. However, a PN running on XenServer 6.1 or later without XenTools installed is supported.
- (*Windows Server 2012 R2 Only*) It is possible that the mouse may not be activated when an RN is running in test mode via Java console. Attempt to run the RN in production mode, and use an RDP session to access the RN. This bug will be resolved pending a XenServer release of a new BIOS or Microsoft fix.
- (*Windows Server 2012 & R2*) When a REFS volume in Windows Server 2012 or R2 is protected, the Recovery Node for the same will be in standard NTFS. This is also true of a Bare Metal Restore.
- (*Windows Server 2012 & R2*) When a deduplicated volume in Windows Server 2012 R2 is protected, the Recovery Node for the same will again be a standard NTFS. This is also true of a Bare Metal Restore. Additional caution should be used in allocating RN disk space as the Quorum agent on the Protected Node will report actual disk usage, which might be far less than when data is stored in its normal form.
- (*All Windows Server platforms*) When onQ event log reports 3010 code for any Windows PNs, both 32-bit and 64-bit, the auto-upgrade fails. Perform *one* of the following workarounds in the order that they are listed:
  - Restart onQ Service on the PN.
  - Reboot the PN.

- Uninstall and reinstall the last msi package at `C:\Program Files\Quorum\installer`.

3.3 Volume Mount Limitations

- Volumes only reachable through a GUID path are not supported.
- Backup source arguments that aren't drive letters or volume mount paths that begin with a drive letter are not supported.
- Paths as backup source arguments to onQ that are not volumes or volume mount points are not supported when using with VSS.
- Volume mount points cannot contain the characters outside of A-Z, a-Z, 0-9, underscore and a dash. Volume mount points with spaces are not supported.
- Total string length of drive letter mounts and volume mount points, including separators in excess of 250ch/s, are not supported.
- Volume mount point that are based on a volume that has other mount points that refer to it (multiple mount points) are not supported.
- Volume mount points used to protect MS cluster environment on onQ are not supported.
- Volume mount points might not be visible on the RN under certain circumstances if the folder that contains the mount points is hidden or in a system folder. You might need to set the folder attributes to display system/hidden folders so as to display mount points.
- A maximum of 15 logical drives can be protected per PN.

3.4 CIFS Mount Limitations on Windows

- In order for onQ to back up shared volumes, there are some prerequisite steps that you need follow as outlined in the Online Help.
- In order to FLR to a NAS share:
    1. Choose **File Level Restore** > **Other** option. Provide the IP address of the destination PN and follow the onQ Portal instructions to start wvhds on the target.
    2. From the FLR interface, choose a local drive on the PN.
    3. Restore the files from the NAS partition to this local drive.

4. Move the data from the fixed drive to the NAS partition.

- When file objects are restored from a NAS backup, the kernel security objects may not be written. The data contents of the file will be restored as it was backed up.
- You cannot specify the size of a vdisk when you create or update the vdisk. This limitation is true for both automatic enrollment and manual enrollment.
- You cannot perform a BMR for CIFS drives. BMR continues to support only fixed drives on protected Windows systems.
- Network shared volumes can be extremely large; therefore, restoring to a specific PN is not an efficient way to retrieve data. Instead, restore the data to a NAS appliance. A BMR can only restore to local drives.
- Recovery Nodes will not include data for a network shared drive. However, Recovery Nodes started in production mode can connect to the configured remote drives.
- When an RN boots as part of a self-test or because you choose to boot it in test mode, the remote mounts will not be accessible.
- Backup performance depends on your PN's and NAS's bandwidth, I/O limitations, and other resources.
- File Backup Only option cannot be used with a remote drive.

3.5 Bare Metal Restore Limitations

- When you perform a failback to restore a VMware-based protected node to a dissimilar hardware or virtual environment, Windows might require reactivation.
- BMRs that are performed to the same or new hardware require that you upload specific drivers for any disk, network adapter, and any other hardware.
- After an incremental failback to a non-Xen PN (physical PN, ESX PN, Virtual PC PN), users are required to reinstall drivers.
- For a Windows 2012 server, a REF's partition/volume will be restored as standard NTFS.
- For a Windows 2012 server, if you choose to restore a volume with deduplication enabled, the data will be restored to its full size. Simply enable deduplication after the BMR completes.

- For restored images of Windows 2008 and later, the boot correction script needs to be manually executed while in the QUARK environment. Failure to do so will result in the restored image not booting with its operating system.
- Volume Mount Points need be configured manually before starting to restore the image. Volume Mount Points created this way are not listed in the disk configuration interface along with other volumes.
- Disk configuration interface does not display the file format type for a volume created without a drive letter assigned.
- When adding each volume in the disk configuration interface, you might need to wait a short period of time while the volumes are being created.
- There is a maximum allowed duration of 72 hours for a restore to complete. Exceeding 72 hours might result in a reboot of QUARK and a loss of the restored image to that point.

3.6 Windows Cluster Services Limitations

- Suppose cluster nodes A and B are configured to use the same disks for their operation. If both of them are enrolled for protection, along with their shared disk configuration, only the cluster node that is currently using the shared disks can be backed up. If you attempt to back up the cluster node that does not have access to the shared disks, the backup will fail. Because the IP address of all the cluster nodes in the host table are set to the IP address of the cluster, any passive node in the cluster will indicate a RED status and backups will fail.
- When you start a cluster RN, you must select the RN for the node that was active at the time your desired backup was generated. For example, if you want the most recent data, then select the node with the most recent backup.The RN for the other nodes will contain stale information. If you want to roll back to a previous backup, you must select the RN that was active at that point in time.
- Recovery Node disks used in this context are basic disks, each with a maximum size limit of 2TB. The logical volume size for these disks is not expandable.
- If the PN configuration is switched between a standard and a cluster, the RN will be reinitialized and rebuilt.

- A cluster node that is protected with this configuration whose RN is brought in production can only be configured to work with virtual SAN. Registry modifications are done in the RN from the information provided in the onQ Portal for the specific node.
- A cluster node protected with this configuration is not suitable for a Bare Metal Restore as cluster service configurations are modified on the RN to work with a virtual SAN. Also, the failover cluster node is evicted from the configuration while preparing the RN. Only application data (SQL database, for example) can be retrieved/restored.

4

Updates

- Upgrade Support
- Update Appliance software

4.1 Upgrade Support

Upgrading *directly* to version 3.6 SP1 is supported for onQ Appliances and protected nodes running 3.6 HF2.

When upgrading, take note of the following:

- After an onQ upgrade, you must refresh your browser using CTRL-F5. If you don’t, portal changes will not be activated and some user actions will not work.
- After an onQ upgrade, restart protection on the DR Appliance.
- You must manually reboot the onQ Appliance after the onQ upgrade completes.
- An onQ upgrade to 3.6 SP1 does not involve any major repository migration or restructuring.
- Upgrade packages are deployed through onQ Central. onQ and AV will auto-download the necessary onQ packages when the daily cron job runs. This job runs between 10pm and 2am each day. This deployment occurs for all onQ Appliances for which onQ Central is set to allow download of the latest software packages.

4.2 Update Appliance software

Quorum releases a new version of onQ Appliance software, service pack and hot fixes as required from time to time. If the onQ Appliance is registered with Quorum's onQ Central system for licensing, alert redirection and receiving updates, then updates are automatically downloaded on to the onQ Appliance between 10pm and 2am when the updates become available.

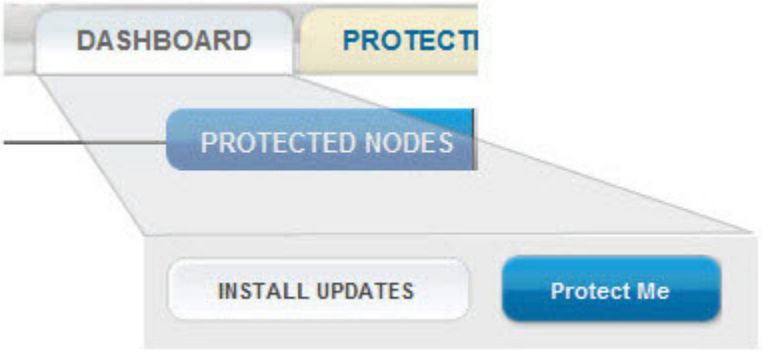
To *automatically* install an update:

Before you begin, verify that your upgrade path is supported.

1. Trigger the download of the onQ package, if it hasn't already downloaded.
   a. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **Software Upgrades** page.
   b. Click the **Check for Updates** button.

   Mouse-over the Check for Updates button to display the status of the download.

   The onQ Portal's **DASHBOARD** displays an **Install Updates** button after the new onQ Archive VaultonQ Appliance software downloads from onQ Central.



   Unless instructed, there is no need to stop protection to apply the updates. If protection is on, onQ quiesces the system, stops protection, applies the new software, then restarts protection. The upgrade process reboots the onQ, if required. The length of time that onQ requires to complete the upgrade depends on the number of active jobs currently running.

2. Apply the new software:
   a. Go to the **DASHBOARD** tab.
   b. Scroll down and click the **Install Updates** button.
   c. Click the **Upgrade** button when prompted to initiate the upgrade.

   From the **DASHBOARD**, mouse-over the Install Updates icon  to display the status of the upgrade.
3. Restart protection.
4. From your browser, press CTRL-F5 to load and activate the onQ Portal changes.