Quorum®

onQ Administrator’s Guide

Version 3.9

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

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

Table of Contents

Preface

This guide is intended for System Administrators who need to deploy, configure, manage, and monitor their onQ Appliances. The guide can be used by both newbies and experienced users.

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/3.9/onQ/index.html
AV	http://www.quorum.net/help/3.9/Vault/index.html

Chapter Organization

The chapters and appendices of this manual are as follows:

- Chapter 1, *Product Overview*
- Chapter 2, *Requirements*
- Chapter 3, *Deployment*
- Chapter 4, *The Basics*
- Chapter 5, *Enrollment in non-cluster Environment*
- Chapter 6, *Enrollment in Windows Cluster Services Environment*
- Chapter 7, *Updates*
- Chapter 8, *Protection*
- Chapter 9, *Backup and Restore*
- Chapter 10, *Security and Communications*
- Chapter 11, *Disaster Recovery and DR Preparedness*
- Chapter 12, *Monitoring*
- Chapter 13, *Troubleshooting*

- Chapter 14, *User Management*
- Chapter 15, *Example Configurations*
- Chapter 16, *Example Logs*
- Chapter 17, *Tech Notes*
- Chapter 18, *Glossary*

1

Product Overview

1.1 About onQ

Businesses today depend upon the continuous availability of information systems and business applications. Any downtime is disruptive and expensive.

An effective business continuity plan is essential for any business that wants to remain viable and competitive even when systems fail or business is interrupted.

Typical business continuity solutions require a variety of technologies provided by different vendors, and involve physical duplication of production resources at remote locations. This approach works but is very expensive.

The advent of new technologies such as virtualization, replication, storage, and de-duplication have reduced the cost of business continuity for some businesses, but the overall cost and degree of expertise required has still kept these newer approaches beyond the reach of most small and medium businesses.

Quorum has created an affordable, all-in-one business continuity solution that includes all the technologies required to protect and restore physical and virtual machines. This solution is delivered on a single physical device called, simply, onQ.

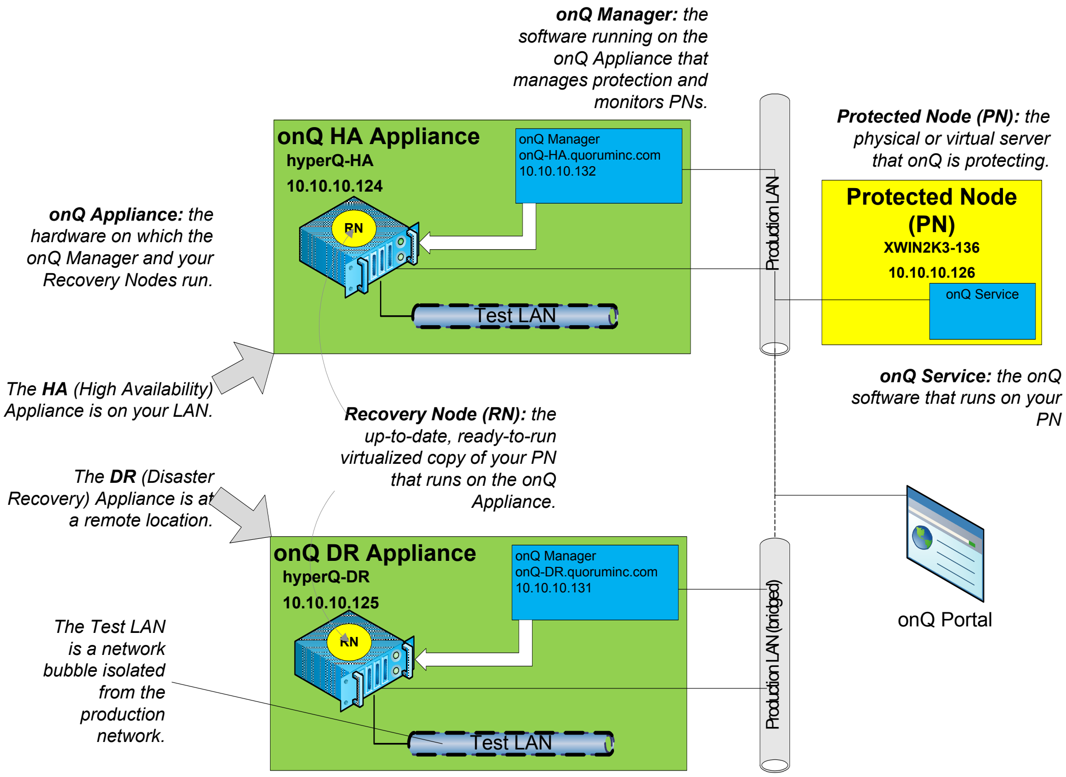
onQ is based on Quorum’s feature-rich management and automation platform and comes complete with all the technologies necessary to provide high-availability and disaster-recovery protection for any workload. With its intuitive user interface onQ is simple to install and manage.

onQ automates high availability (HA), disaster recovery (DR) and business continuity (BC) in a turnkey Appliance by integrating all of the following features and benefits:

- **Full system imaging** of all Operating System, Application and Data files to allow bare metal restoration of your servers.
- **Incremental snapshot archiving**: crash-consistent updates of all files, even if they are open, allows efficient archiving as frequently as every 15 minutes.
- **Deduplication**: only the changes on your server are saved in the archive, and only if they are different than any of the “chunks” of data already stored.
- **Replication**: your entire archive is replicated to a second remote onQ Appliance over an encrypted, compressed, bandwidth-controlled link.
- **Virtualization**: onQ maintains an up-to-date virtual copy of your servers, which are immediately available on the onQ Appliance upon request.
- **Recovery Infrastructure**: you don’t need to have spare, standby servers—the onQ Appliance has the resources to run the virtual copies of your servers and make them immediately available upon request.
- **Monitoring, Reports and Alerts**: onQ Manager monitors all activities and lets you know when things go wrong—and when they go right.
- **Single Web-based Interface**: accessible from anywhere, the onQ Portal lets you manage all operations without complexity.

1.2 Terminology

The figure below shows some of the terminology we use when discussing onQ and its components. For a complete list of terms, go to Glossary.



onQ Manager: *the software running on the onQ Appliance that manages protection and monitors PNs.*

Protected Node (PN): *the physical or virtual server that onQ is protecting.*

onQ Appliance: *the hardware on which the onQ Manager and your Recovery Nodes run.*

*The **HA** (High Availability) Appliance is on your LAN.*

onQ Service: *the onQ software that runs on your PN*

Recovery Node (RN): *the up-to-date, ready-to-run virtualized copy of your PN that runs on the onQ Appliance.*

*The **DR** (Disaster Recovery) Appliance is at a remote location.*

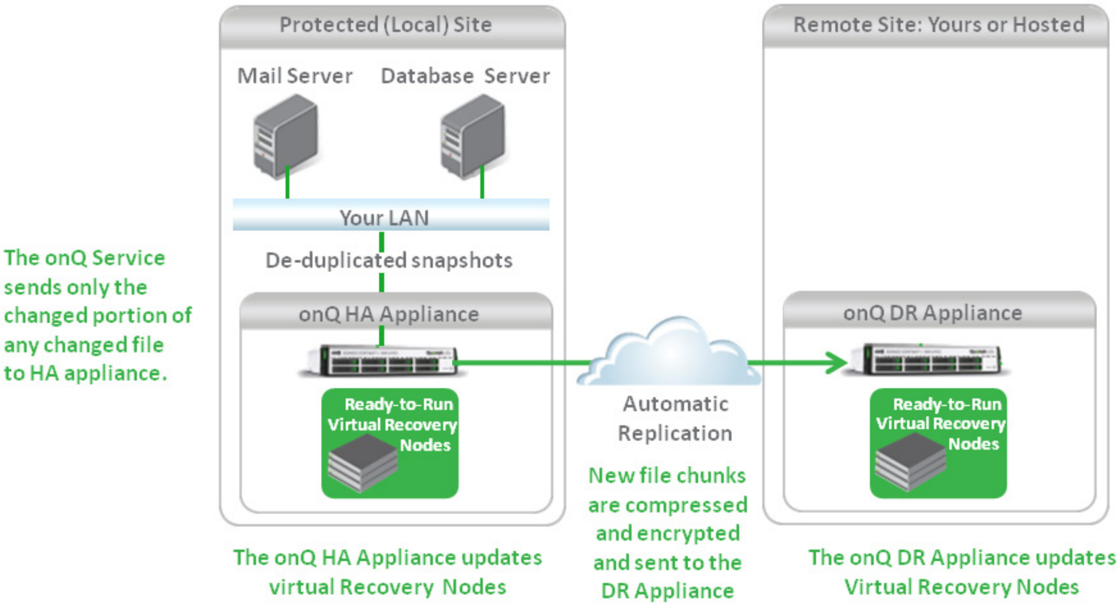
The Test LAN is a network bubble isolated from the production network.

1.3 How does onQ work?

Basically, onQ works like this:

- **onQ** is a fully integrated turnkey Appliance solution. One onQ Appliance is deployed for high-availability (HA) protection. Most businesses add a second onQ Appliance at another location for disaster recovery (DR) or use Quorum’s Hybrid Cloud offering to host their DR.
- Each onQ Appliance hosts the **onQ Manager**, Quorum’s core software.
- Your HA is connected to the same network as your protected nodes. The DR Appliance is typically connected to the HA (not the protected nodes) through a VPN over a WAN.
- One of the following:
  - (*agent-based PNs*) **onQ Service** software is installed on each protected node (PN). The **onQ Manager** communicates with this software to determine operational status and to schedule snapshots. For more information go to (Agent-based PNs) Restart the onQ Service and (Agent-based Linux PNs) Enroll protected nodes.
  - (*agent-less PNs*) **Proxy hosts** are installed on the ESX/ESXi host. The **onQ Manager** communicates with these proxy hosts to determine operational status and to schedule snapshots. For more information, go to (Agent-less Linux/Windows PNs) Enroll protected nodes.
- You manage **onQ Manager** through an intuitive, browser-based, user interface called the **onQ Portal**. When you install your onQ Appliance(s), you use the UI to configure the onQ Appliance to take incremental snapshots for each protected node. You also use the UI to control and monitor the protection process.
- Once protection is started, the HA manages your backup schedule, taking deduplicated, incremental snapshots of your protected nodes at specified intervals.
  - After each snapshot is added to the repository, the onQ Manager on the HA updates the recovery node corresponding to the protected node.
  - At the same time, the DR Appliance is synchronized and independently updates its own recovery node. Thus, there are individual up-to-date recovery nodes on both the HA and the DR Appliance.

- onQ Manager alerts you by e-mail if a protected node or an incremental snapshot fails.


Protected (Local) Site
Mail Server
Database Server
Your LAN
De-duplicated snapshots
onQ HA Appliance
Ready-to-Run Virtual Recovery Nodes
Remote Site: Yours or Hosted
onQ DR Appliance
Ready-to-Run Virtual Recovery Nodes
Automatic Replication
The onQ Service sends only the changed portion of any changed file to HA appliance.
The onQ HA Appliance updates virtual Recovery Nodes
New file chunks are compressed and encrypted and sent to the DR Appliance
The onQ DR Appliance updates Virtual Recovery Nodes

1.4 Product Comparison

onQ comes in many flavors. Use the following table to help you understand the features available in your configuration and the applicable topics in this documentation. For pricing and complete product descriptions, go here.

	onQ Flex	onQ On-Site	onQ Prime	onQ Plus
HA	On-premises	On-premises	On-premises	On-premises
DR	Cloud	On-premises	Cloud	Cloud
RN Availability	Flexible RTO	Optimum RTO	Optimum RTO	Optimum RTO
Archive Vault	Optional	Optional	Optional	Optional
Automatic Testing	Optional	Included	Included	Included
Restore Options (BMR, WSR, File-Level)	Included	Included	Included	Included

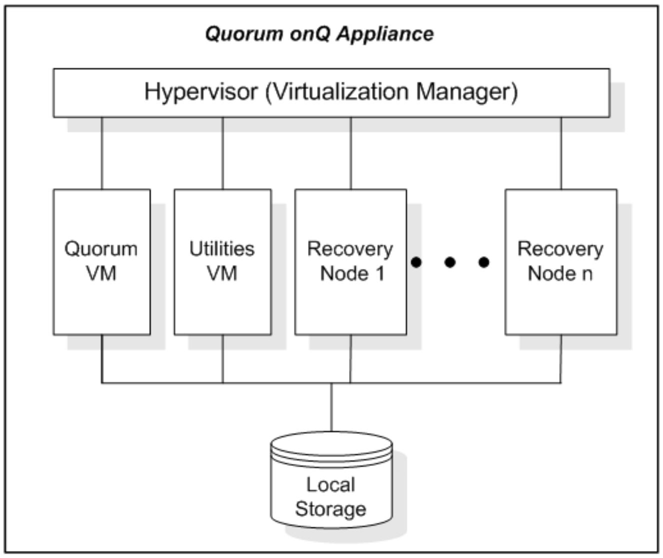
1.5 Inside onQ Appliance

Each Quorum onQ Appliance is a server class x86-based computer running on a bare-metal hypervisor for efficient automated virtualization.

The onQ Appliance typically contains several terabytes of redundant internal disk storage. This internal storage is used to efficiently store deduplicated snapshots of your protected nodes and to host the recovery nodes (RNs).

onQ is organized as a set of virtual machines. Each onQ Appliance runs several virtual machines (VMs): (1) potentially one virtual machine (RN) for each protected node; and (2) one VM to host the onQ Manager itself.

onQ builds the RNs from snapshots of your protected nodes and makes them available based on the RN’s build policy.



1.6 About Hybrid Cloud

Hybrid Cloud is a DR Appliance as a Service (DRaaS). The Deployment of a Hybrid Cloud-enabled HA is virtually identical to an on-premises HA. The only difference is that you must also add information to the Hybrid Cloud-enabled HA so that it can VPN to your DRaaS. This secure connection enables the HA to send snapshots to your DRaaS.

In the event of an HA site disaster, Quorum can ship you the cloud DR Appliance, replacing it with a new DR instance. This onsite DR Appliance assumes the HA role.

The Quorum Data Center that will be hosting your applications are SAS-70 Type II certified. All data transferred from the HA Appliance to the DR Appliance goes through a 128-bit AES encrypted session behind a 256-bit AES VPN tunnel that is connected directly from the HA Appliance to the DR Appliance. There is a dedicated virtual firewall isolating each individual custom virtual network. All connections to the DR Appliance or the DR RNs are via VPN to that firewall.

Moreover, Hybrid Cloud is 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.

Related Topics

Product Comparison
About onQ Flex

1.7 About onQ Flex

onQ Flex is a Hybrid Cloud configuration where your business-critical Recovery Nodes (RNs) are one-click away in the event of a disaster and eligible for automatic testing and the remaining RNs can be manually created on-demand from up-to-date snapshots. This flexibility provides you fine-tuning of your RTO (Recovery Time Objective) and the costs for that objective in an effort to conserve system resources and minimize up-front deployment costs. onQ tracks all RN changes, so you can modify the RN type and build policy at any time.

Related Topics

onQ Flex Limitations
(onQ Flex) Modify RN type and/or RN build policy
(onQ Flex) Build recovery nodes
Remove recovery nodes

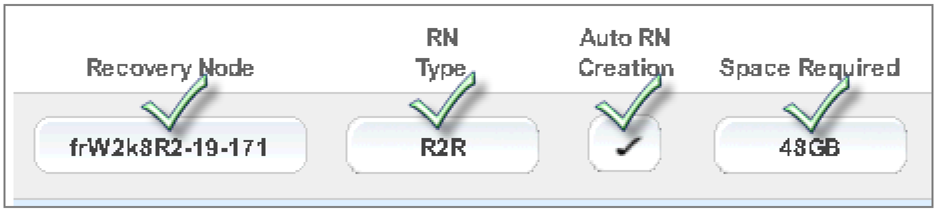
1.8 About onQ Flex Manager

From the onQ Flex Manager dialog you can manage your onQ Flex configuration. In fact, after you enroll your PNs, verify that the RN type for your PNs reflects your preferred RTO plan: all newly enrolled PNs default to *OD* (RN type) and *Build-on-Demand* (build policy).

Build the Recovery Node	Depending on your RN's build mode (aka build policy), you might need to build your RN manually in the event of a disaster. For more information, go to (onQ Flex) Build recovery nodes.
Change the RN Type	The build policy represents your RTO (Recovery Time Objective) and the RN type indicates your preferred RTO cost (or plan) for that objective. Choose one of the two RN types: • **R2R**. Reiterates that you prefer a Ready-to-Run objective. • **OD**. Reiterates that you prefer a Recovery-on-Demand objective. All newly enrolled PNs default to *OD* (RN type) and *Build-on-Demand* (build policy). You can change the RN type or build policy at any time. For more information, go to (onQ Flex) Modify RN type and/or RN build policy.
Change the Build Mode	onQ can build RNs either automatically with each backup cycle or on-demand as needed. You can change this policy at any time. For more information, go to (onQ Flex) Modify RN type and/or RN build policy.
Remove the Recovery Node	You might need to remove RNs to free up disk space. For more information, go to Remove recovery nodes.

To launch the onQ Flex Manager:

1. Log on to the onQ Appliance’s onQ Portal.
2. Go to **DASHBOARD** tab > **RECOVERY NODES** page.
3. Unlock the page.
4. Click on any of the following GUI components: the **Recovery Node** button, **RN type** button, **Auto RN Creation** button, or the **Space Required** button:



The onQ Flex Manager appears.

1.9 Product Support

Quorum Support is committed to providing the best product support in the computer industry. Customer support is available 6am–6pm (PST), Monday through Friday, via telephone, fax, e-mail, and our Web site.

Quorum Support:

Telephone:	+1.408.708.4502
E-mail:	support@quorum.net
Web Site:	http://www.quorum.net/support

Sales & Marketing:

The Sales & Marketing Department can be reached at info@quorum.net.

2

Requirements

2.1 Configuration Guidelines & Requirements

Before you install onQ you will need to gather some information about your site. These preparation steps are usually completed by your Reseller or Quorum using Quorum Site Survey tools and guidelines.

If you are performing this function yourself, you can request the onQ Site Survey kit from Quorum Support which includes forms and tools to streamline your deployment.

- **Network Configuration:** For all servers you wish to protect, whether virtual or physical, you will need host names and IP addresses. You will also need two addresses for each of your onQ Appliances: one for the hypervisor and the other for onQ.
- **Operating System:** The Operating System on your Protected Nodes must be supported. See "Platform Support" in onQ Release Notes.
- **Data Usage:** During setup, onQ will check storage usage for each disk on each server you protect. By default, onQ assigns 1.5 times the amount of space currently in use. You can increase this if you anticipate higher growth in the next few years.
- **Memory:** onQ uses an algorithm to assign RAM based on how much is used by your server and what is available on the onQ Appliance. If you decide to change this default allocation, consider allocating the minimum memory required for each Recovery Node for adequate operation. Only

exceed 2GB per node when you know that it is necessary for that node’s workload.

- **Processors:** onQ uses an algorithm to assign virtual CPUs based on how many CPU cores are on your server and how many are available on the onQ Appliance. Because there are multiple Recovery Nodes operating concurrently on each onQ Appliance and not all will have peak activity at the same time, more virtual CPUs can be allocated than are physically present. Allocating more virtual CPUs does not necessarily improve performance and can actually hurt performance if Recovery Nodes are reserving CPUs that they do not need.
- **Microsoft VSS**. Microsoft VSS must be enabled and have adequate snapshot space allocated. For more information, go to “Protected Node Parameters” on page 66.
- **Database backups and restores**. Verify that your database backup and restore scripts are performing as expected. You should not have any issues using these same scripts in an onQ environment because such operations are independent of onQ. Do not deploy onQ if you are having database backup or restore failures. Resolve these issues before you proceed with your deployment.

2.2 Network and Firewall Requirements

Ensure that the following ports are open on the network, onQ Appliance, and PNs:

- LAN/Network Communications
- onQ Appliance-to-PN Communications
- HA-to-DR Communications
- WAN-DR Site Communications

Note: Traffic to onQ Appliances should not be open to any public access, except 443 and 123.

2.2.1 LAN/Network Communications

The following port(s) are required for administrative access to the portal on each onQ Appliance and for alerts, updates, and licensing. These ports should not be open to public access:

Direction	Port	Protocol	Purpose
LAN-only Inbound	80 & 443	TCP	onQ Portal access. Needed internally on private network LAN only. No Internet access recommended.
Inbound	443	TCP	https from onQ IP needed to the Internet for licensing and alerts
Outbound	443	HTTPS	Access for alerts (httpsalerts.onqcentral.com), updates and licensing (updates.onqcentral.com).
Inbound & Outbound	123	UDP	Communication with NTP (ntp.org).

Related Topics

onQ Appliance-to-PN Communications
HA-to-DR Communications
WAN-DR Site Communications

2.2.2 onQ Appliance-to-PN Communications

Generally, onQ-to-PN communications are over a LAN that is not secured. In the event that there are any filtering devices between the PN and the onQ Appliance, the following ports need to be accessible on the PN:

Direction	Port	Protocol	Purpose
Outbound	3000	TCP	Allows squirtcopy communications
Inbound	5000	TCP	For FLR processing, allows WVhds for Windows and Netcat for Linux to receive data from onQ Manager
Inbound	5990	TCP	Allows DCRM to accept connections from onQ Manager
Inbound	5990	UDP	Allows LAMD to communicate with onQ Manager
Inbound	5991	UDP	Allows LAMD to monitor the PN
Inbound	5992	UDP	Allows LAMD to send PN heartbeat

Related Topics

LAN/Network Communications
HA-to-DR Communications
WAN-DR Site Communications

2.2.3 HA-to-DR Communications

The following ports must be accessible between the HA and the DR Appliance pairs across WAN or LAN:

Direction	Port	Protocol	Purpose
Inbound & Outbound	22	TCP	Allows secure TCP connections between onQ Appliances. May be remapped.
Inbound & Outbound	81	TCP	Allows inter-appliance link monitoring. May be remapped.

Related Topics

LAN/Network Communications
onQ Appliance-to-PN Communications
HA-to-DR Communications

2.2.4 WAN-DR Site Communications

The following ports must be accessible/inaccessible between your WAN and DR site:

Direction	Port	Protocol	Purpose
Inbound & Outbound	22	TCP	<DR IP> to <HA IP>
Inbound & Outbound	81	TCP	<DR IP> to <HA IP>
Inbound	80	TCP	Deny ANY PUBLIC / External / Internet to <DR IP> (HTTP protocol)
Inbound	443	TCP	(https) Allow <DR IP> outbound to Public / External / Internet
Outbound	443	SSL, SMTP, & SSH, TCP	Access for alerts (alerts.onqcentral.com), updates (updates.onqcentral.com), and licensing (lic.onqcentral.com).

2.3 Host-based Firewall and Anti-Virus Requirements

The following four files require specific attention so as to enable upgrades on agent-based PNs and prevent backups and scanning from taking a long and undesirable period of time.

- `C:\Program Files\Quorum\QuorumDCRM-NODE\acd.exe`
- `C:\Program Files\Quorum\QuorumDCRM-NODE\lamd.exe`
- `C:\Program Files\Quorum\usr\squirtcopy.exe`
- `C:\Program Files\Quorum\usr\WVhdS.exe`

For each file, do the following:

- Create local firewall and antivirus exceptions to allow inbound and outbound access for these files across all networks—local, private, and public.
- Exclude these files (and the entire `\Quorum` folder) from any local, realtime antivirus software products.
- Any host-based firewall local to the Protected Node (PN) should either have the same ports opened, or local firewall exceptions added for these files in order for them to function in private, local, and public modes.

Related Topics

onQ Appliance-to-PN Communications

2.4 Operational Considerations

- Adjust bandwidth throttling, if necessary, to speed up data transfers.
- Perform initial backup on LAN, not WAN, to improve performance. Quorum suggests that you perform the initial setup, and then the initial backup, with both your HA and DR Appliance on the same LAN. For more information, go to Seed the DR Repository.
- Identify interdependencies.

2.5 Identify interdependencies

Beware of interdependent resources on your Protected Nodes. For example, if your mail server depends on a Domain Controller to function properly, both machines must be protected by onQ. Similarly, if there are critical functions that depend on DNS, ensure that onQ protects your DNS server too; otherwise, those functions might fail. onQ itself generally maintains critical IP addresses in the onQ Appliance's HOSTS file.

In the event of an HA site disaster, the boot order for your recovery nodes must take into account these dependencies. During the installation workflow, you will be prompted to configure these startup dependencies using the onQ Portal.

3

Deployment

3.1 Installation Overview

Most installations use two Appliances. One onQ Appliance is deployed to provide high availability (HA) protection while the other is deployed in a more remote location to provide disaster recovery (DR) protection.

The two onQ Appliances are architecturally identical, although they can have different physical resources available, such as processors and memory. If your installation uses two onQ Appliances, you'll make two passes through some of the installation steps—once for the HA and once for the DR Appliance. Also, during installation, you will assign the onQ Appliance its role as the HA or the DR Appliance.

Before you can use onQ you need to install the onQ Appliances on your network and enroll your Protected Nodes (PNs). You make these initial settings and manage the ongoing operations of the onQ Appliance using the onQ Portal.

Some settings, such as network parameters, are usually pre-configured at the factory and you rarely, if ever, need to change them.

Setting up the onQ Appliances requires a special user, `VARAdmin`, with privileges to perform the following tasks. `VARAdmin` is not needed for day-to-day administration and operation.

- Changing the onQ Appliance network configuration
- Setting up Security

- Setting the `VARAdmin` password
- Preparing the onQ Appliance for re-deployment

You will need to log on as `VARAdmin` in order to configure your Appliances. After you log on, you should change this password. Contact Quorum Support for the default password.

Warning: It is critical that you remember your password: Quorum Support cannot recover it and cannot perform certain support tasks without it.

3.2 (Workflow) Install onQ Appliances

Use this procedure to set up your onQ Appliances. These instructions apply to each onQ Appliance, whether it provides high availability (HA) or disaster recovery (DR) protection.

Install your onQ Appliance in the environment in which it is to be used. If you have problems during setup, go to Deployment Problems.

To set up your onQ Appliances, perform the following sequence of tasks:

Task	For instructions, Go to...
1. Get an overview of the installation process.	Installation Overview
2. Collect information about your site(s)	Step 1: Prepare to install
3. If not pre-configured, configure the onQ Appliance.	Step 2: Configure the onQ Appliances
4. (Hybrid Cloud Only) Create a VPN connection to your DR Appliance so that you can access its web portal.	Step 3: (Hybrid Cloud Only) Create VPN connection to Hybrid Cloud
5. Connect the onQ Appliance to your network.	Step 4: Connect the Appliance to your network
6. Change hypervisor's NTP server	Step 5: Change hypervisor's NTP server
7. Enroll the protected nodes you want to protect.	Step 6: Enroll protected nodes
8. (onQ Flex only) Change the RN type or build policy to reflect your company's preferred RTO objective and cost.	Step 7: (onQ Flex) Modify RN Type and Build Policy

Task	For instructions, Go to...
9. Configure the boot order for your recovery nodes.	Step 8: Configure RN startup dependencies
10. Start protection on the nodes.	Step 9: Start automated protection process
11. (Optional) Install onQ Archive Vault, if you intend to archive backups.	After the hardware is up and running, refer to the AV online help for configuration instructions. For supported configurations, go to Archive Vault Configuration Support.
12. (Recommended) Test your existing backup and recovery procedures using an RN in test mode.	See also: • Back up and restore Oracle 11g database on Linux • Back up and restore Oracle 10g+ database on Windows

3.2.1 Step 1: Prepare to install

The setup process requires a supported browser. Go to Browser Support.

To prepare to install:

1. Enable JavaScript on your browser.
2. Ensure that the list of trusted websites maintained by the Internet Explorer Enhanced Security Configuration (IEESC) includes **about.blank** and the onQ Appliance IP addresses.

   IEESC is a Windows component only shipped with Windows Server.
3. Collect information about your site using the worksheets available on the Customer Support Portal.

   Read the requirements and best practices outlined in Requirements.

Next Step: If your Appliances were pre-configured prior to delivery, skip to Step 4: Connect the Appliance to your network; otherwise, proceed to Step 2: Configure the onQ Appliances.

3.2.2 Step 2: Configure the onQ Appliances

If your onQ Appliance(s) was pre-configured prior to delivery, skip to Step 4: Connect the Appliance to your network. If you're an MSP, perform the following procedure on the HA, DR Appliance, and if applicable, DR Mirror.

To configure an onQ Appliance:

Perform the following steps on all onQ Appliances, including the HA, DR Appliance and, if applicable, the DR Mirror.

1. Use a standalone computer with an available Ethernet port and configure the IP address to **169.254.2.99** and net mask **255.255.255.0**.
2. Connect your computer's Ethernet port directly to Port 0 on the rear of the onQ Appliance.
3. Log on to the onQ Portal with user ID `VARAdmin`. Contact Quorum Support for the default password. If you are prompted to clear the EULA acceptance, click **Yes**.
4. For security purposes, change both the default `VARAdmin` and `Admin` passwords. Go to Change user passwords.

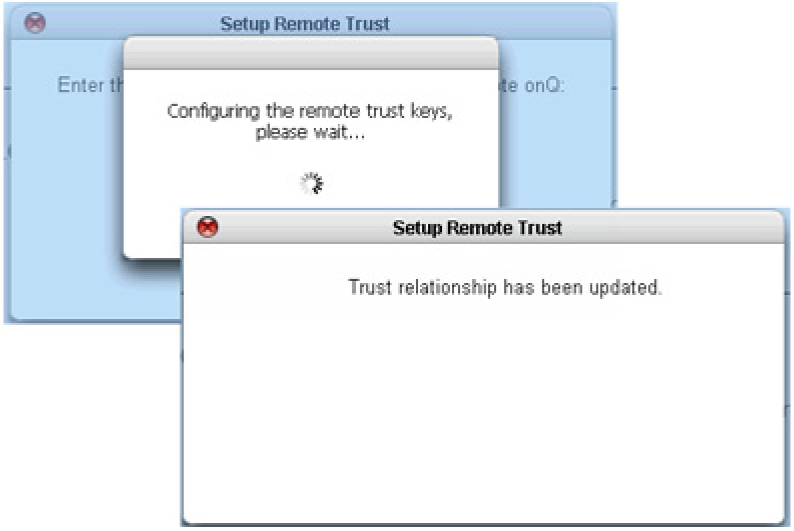
5. If Protection is on, stop protection.
6. Specify local onQ Appliance configuration:
   a. Go to **APPLIANCE CONFIG** tab > **onQ (LOCAL)** page, then **MODIFY**.
   b. Specify the parameters, including networking information and onQ Role, then **SAVE**.

      If your PNs need to go through a proxy, go to About onQ Proxy.

   For examples:
   - Local: Example of DR Appliance
   - Local: Example of DR Mirror
7. Specify remote onQ Appliance configuration:
   a. Go to **APPLIANCE CONFIG** tab > **onQ (REMOTE)** page, then **MODIFY**.
   b. Click **MODIFY** and set the parameters, including networking information, DR mirroring, and bandwidth limits, then **SAVE**.

   For examples:
   - Remote: Example of HA with Hybrid Cloud
   - Remote: Example of HA with Remote DR Appliance
   - Remote: Example of DR Appliance with DR Mirror
   - Remote: Example of DR Mirror
8. Set up the trust relationship.

You must set up the HA-to-DR link. If you have a DR Mirror, set up the DR-to-Mirror link too. For more information, go to Set up trust relationships.



Setup Remote Trust

Enter th... te onQ:

Configuring the remote trust keys, please wait...

Setup Remote Trust

Trust relationship has been updated.

a. Test the link.

9. Configure e-mail alerts.
10. Configure the hypervisor.
11. Reboot onQ.

Next Step: Step 3: (Hybrid Cloud Only) Create VPN connection to Hybrid Cloud

3.2.3 Step 3: (Hybrid Cloud Only) Create VPN connection to Hybrid Cloud

To access your Hybrid Cloud, you must do so using a VPN connection. Afterward, you can launch the web portal from your browser using the DR's LAN IP address that your Quorum Support Engineer provided you.

The PPTP VPN connection to your Hybrid Cloud is very much dependent on the Internet performance available to you and the system performance of the computer from which you are initiating the connection.

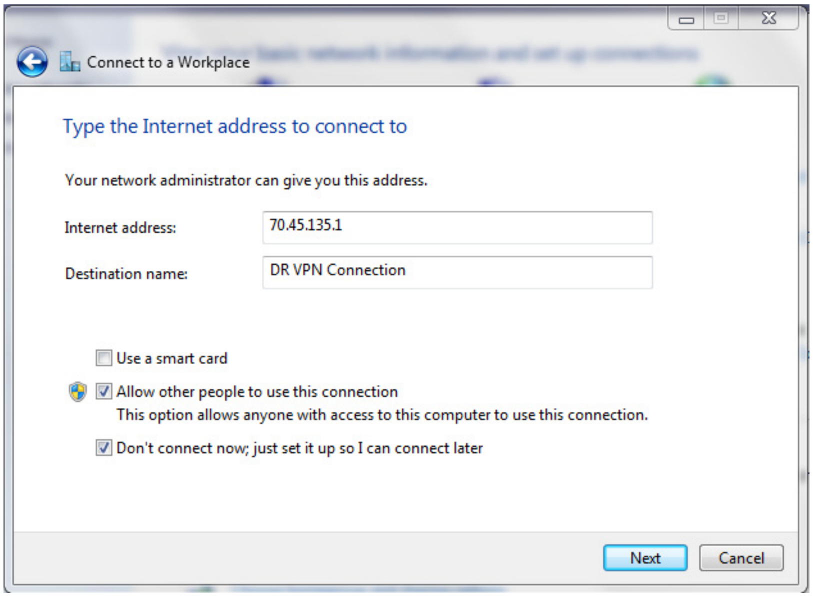
For support with connecting to the Hybrid Cloud, contact Quorum Support at support@quorum.net.

To create a connection to Hybrid Cloud (Windows 7):

This procedure assumes that the client on which you are creating this VPN connection is running Windows 7 with XenCenter installed.

1. Retrieve the following information:
   - Public IP address and logon credentials of the DR. This information was provided by your Quorum Support Engineer.
   - LAN IP address of DR in the Quorum cloud.
2. Configure your network firewall to allow PPTP Outbound Traffic.
3. Run Software Update to ensure that your installation is running the latest updates.
4. From the Control Panel, launch the **Network and Sharing Center**, then click **Set up a new connection or network** link.
5. In the **Choose a connection option** pane, choose `Connect to a workplace`, then **Next**.
6. In the **How do you want to connect** pane, select `Use my Internet connection (VPN).`
7. Complete the following fields and options as follows, then **Next**.

Internet Address	Provide the public IP that Quorum Support provided you.
Destination Name	Type a name for the connection. For example, `DR VPN Connection`.
Allow other people to use this connection	Select this check box.
Don't Connect now; just set it up so I can connect later	Select this check box.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 70.45.135.1

Destination name: DR VPN Connection

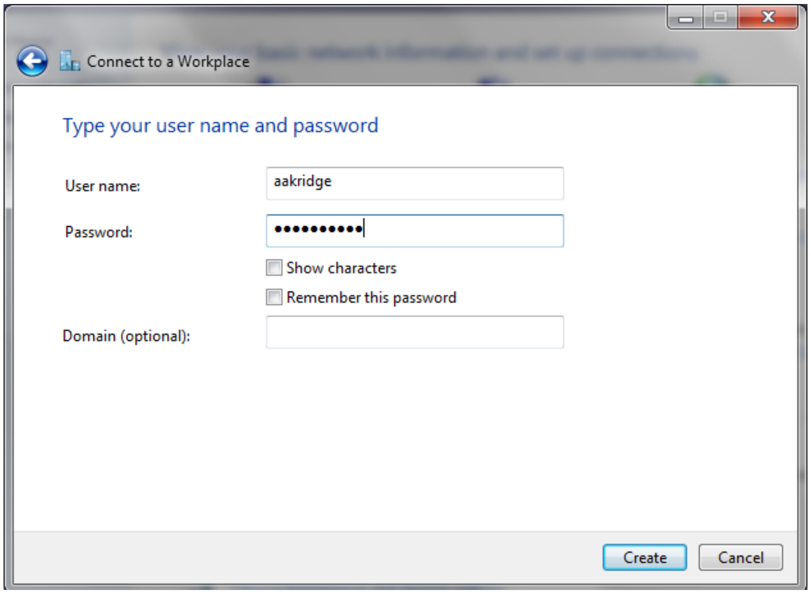
□ Use a smart card

☑ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☑ Don't connect now; just set it up so I can connect later

8. Type in your user name and password that your Quorum Support Engineer provided you and leave the domain field blank, then **Create**.

   Do not connect yet. Click **Close**.



Connect to a Workplace

Type your user name and password

User name: aakridge

Password: ••••••••••

□ Show characters

□ Remember this password

Domain (optional):

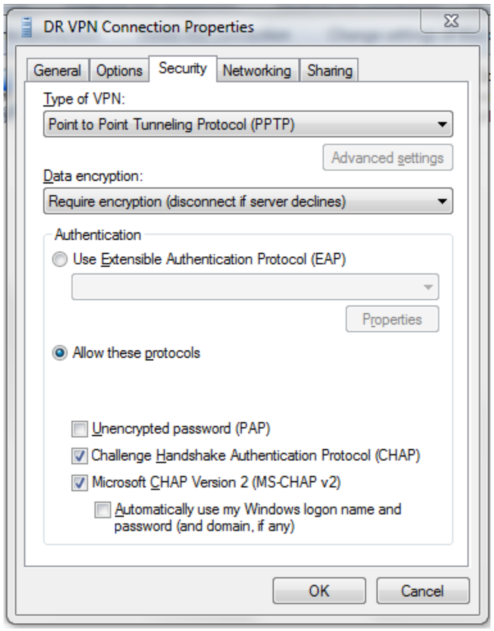
9. Configure the connection to use PPTP protocol:

   a. From **Network and Sharing Center**, click on the **Change Adapter Settings** link in the left pane.

b. Right-click on **DR VPN Connection**, then **Properties**.

c. From the **Security** tab > **Type of VPN** drop-down, choose `Port to Port Tunneling Protocol (PPTP).`

d. Accept all remaining defaults. No further settings are required, then **OK**.



DR VPN Connection Properties

Type of VPN: Point to Point Tunneling Protocol (PPTP)

Data encryption: Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

□ Unencrypted password (PAP)

☑ Challenge Handshake Authentication Protocol (CHAP)

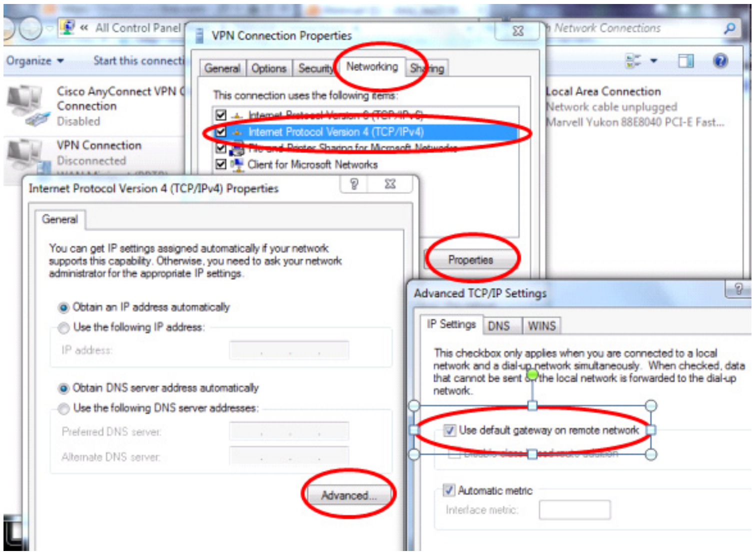
☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)

10. Set remote gateway as the default gateway:

a. Right-click on **DR VPN Connection**, then **Connect**.

b. Go to the **Networking** tab > **IPv4** > **Properties** > **Advanced**. Deselect the **Use default gateway on remote network** check box.



This connection uses the following items:

☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ File and Printer Sharing for Microsoft Networks
☑ Client for Microsoft Networks

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically
○ Use the following IP address:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

This checkbox only applies when you are connected to a local network and a dial-up network simultaneously. When checked, data that cannot be sent on the local network is forwarded to the dial-up network.

☑ Use default gateway on remote network
□ Disable class based route addition

☑ Automatic metric

11. Establish the VPN connection.

12. Verify that the DR is up. From a command line prompt, ping the DR DR's LAN IP address.

13. Log on to the DR's web portal. From a web browser, go to `https://<DR-LAN-IP-Address>`.

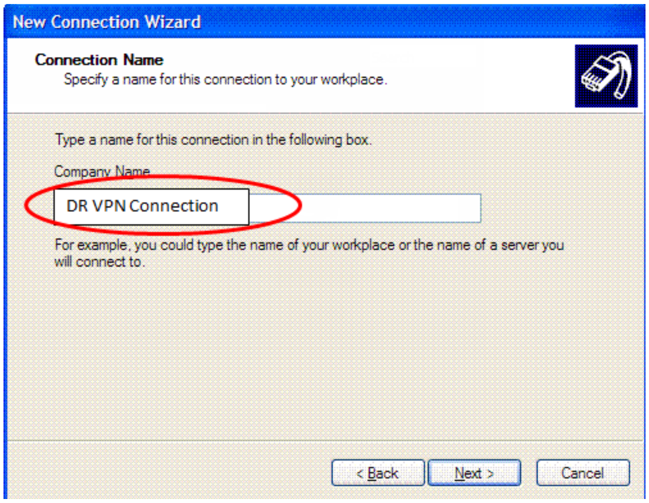
    You should now have full access to the RNs and File Level Backups on the DR.

To create a connection to Hybrid Cloud (Windows XP):

This procedure assumes that the client on which you are creating this VPN connection is running Windows XP with XenCenter installed.

1. Retrieve the following information:
   - Public IP address and logon credentials of the DR. This information was provided by your Quorum Support Engineer.
   - LAN IP address of DR in the Quorum cloud.
2. Configure your network firewall to allow PPTP Outbound Traffic.
3. Run Software Update to ensure that your installation is running the latest updates.

4. From the Control Panel, launch the **Network and Sharing Center**, then click **Create a new connection** link.
5. In the New Connection wizard, click **Next**.
6. Select **Connect to the network at my workplace** radio button, then click **Next**.
7. Select **Virtual Private Network connection** radio button, then **Next**.
8. In the **Company Name** text box, type `DR VPN Connection` as the connection name, then **Next**.



Connection Name

Specify a name for this connection to your workplace.

Type a name for this connection in the following box.

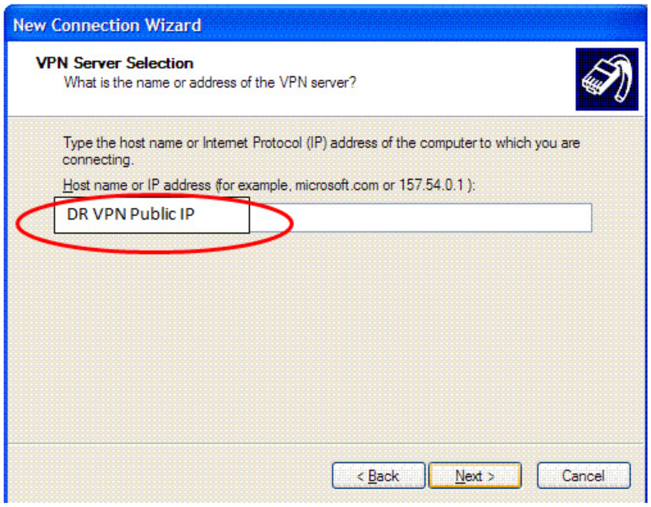
Company Name

DR VPN Connection

For example, you could type the name of your workplace or the name of a server you will connect to.

9. If prompted select the **Do not dial the initial connection** radio button, then **Next**.

10. In the **Host name or IP Address**... text box, type the DR's Public IP address provided by your Quorum Support Engineer, then **Next**.



New Connection Wizard

VPN Server Selection

What is the name or address of the VPN server?

Type the host name or Internet Protocol (IP) address of the computer to which you are connecting.

Host name or IP address (for example, microsoft.com or 157.54.0.1):

DR VPN Public IP

11. If prompted select either **Anyone's use** or **My use only**, then Next, then **Finish**.

12. Modify the connection's settings:

    a. Click on the **Properties** button.

    b. Click on the **Networking** tab.

    c. Highlight **Internet Protocol (TCP/IP)**, then **Properties**.

    d. Click on the **Advanced** button.

    e. Clear the **Use default gateway on remote network** check box, then **OK** until you return to the logon window, accepting all previously defined settings.

13. Establish the VPN connection.

14. Verify that the DR is up. From a command line prompt, ping the DR's LAN IP address.

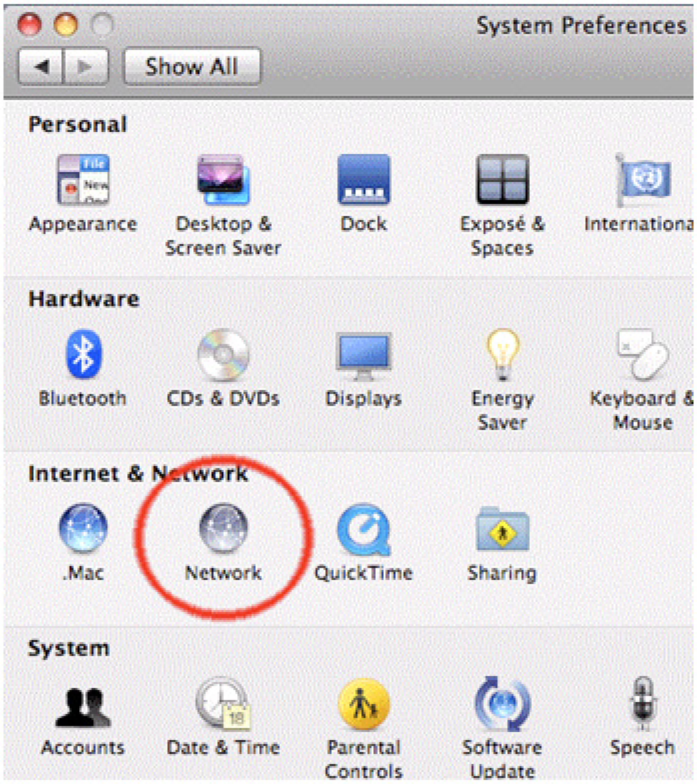
15. Log on to the DR's web portal. From a web browser, go to `https://<DR-LAN-IP-Address>`.

    You should now have full access to the RNs and File Level Backups on the DR.

To create a connection to Hybrid Cloud (Mac OS X):

This procedure assumes that the client on which you are creating this VPN connection is running Mac .OS X.

1. Retrieve the following information:
   - Public IP address and logon credentials of the DR. This information was provided by your Quorum Support Engineer.
   - LAN IP address of DR in the Quorum cloud
2. Configure your network firewall to allow PPTP Outbound Traffic.
3. Run Software Update to ensure that your installation is running the latest updates.
4. Open the Network Control Panel: **System Preferences** > **Network**.



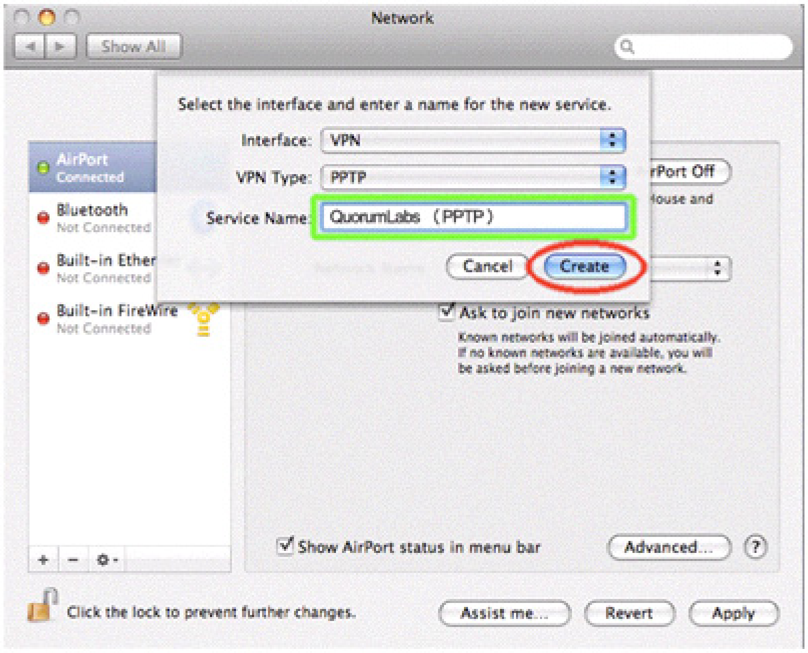
5. Create a new VPN connection:
   a. From the **Network** page, click the plus (**+**) icon in the left panel.

      A new service sheet appears.

   b. Click on the **Interface** popup menu to specify the properties for this new connection.
   c. In the **Interface** drop-down list, choose `VPN`.

d. In the **VPN Type** drop-down list, choose `PPTP`.

e. In the **Service Name** field, name this new connection `Quorum (PPTP)`.



Select the interface and enter a name for the new service.

Interface: VPN

VPN Type: PPTP

Service Name: QuorumLabs (PPTP)

☑ Ask to join new networks

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

☑ Show AirPort status in menu bar

Click the lock to prevent further changes.

f. Click **Create**.

This new connection appears in the list of connections in the left pane.

6. Make a new Quorum configuration:

a. From the **Network** page, click the **Configuration** drop-down list, then **Add Configuration**.

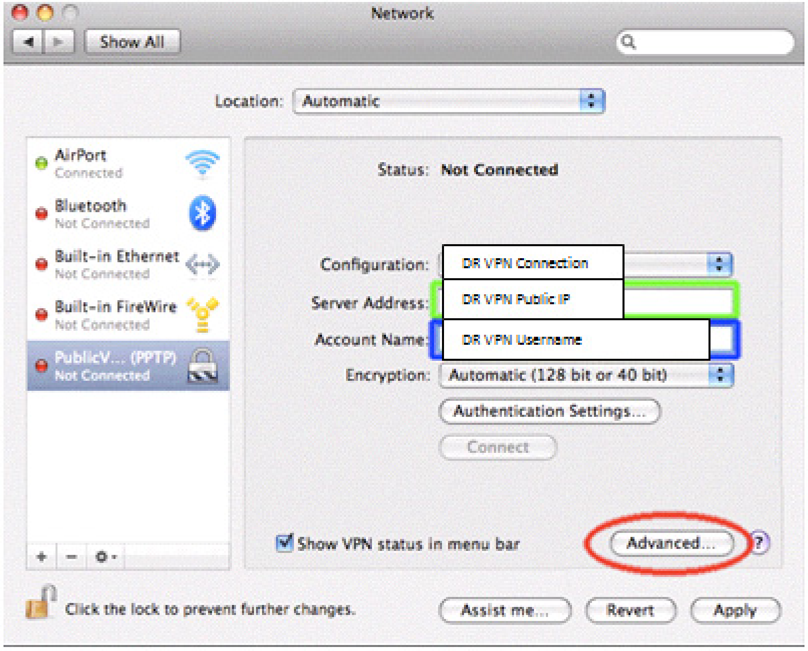
If you set up the VPN previously, the configuration appears in the list.

b. In the **Configuration** field, type `Quorum (PPTP)`, then **Create**.

c. In the **Server Address** and **Account Name** fields, specify the Quorum IP address (WAN IP address) and Quorum username.

d. In the Encryption drop-down, choose **Automatic (128 bit or 40 bit)**.

e. Click on the **Authentication Settings...** button. The **User Authentication** dialog appears.



Network

Location: Automatic

Status: **Not Connected**

Configuration: DR VPN Connection

Server Address: DR VPN Public IP

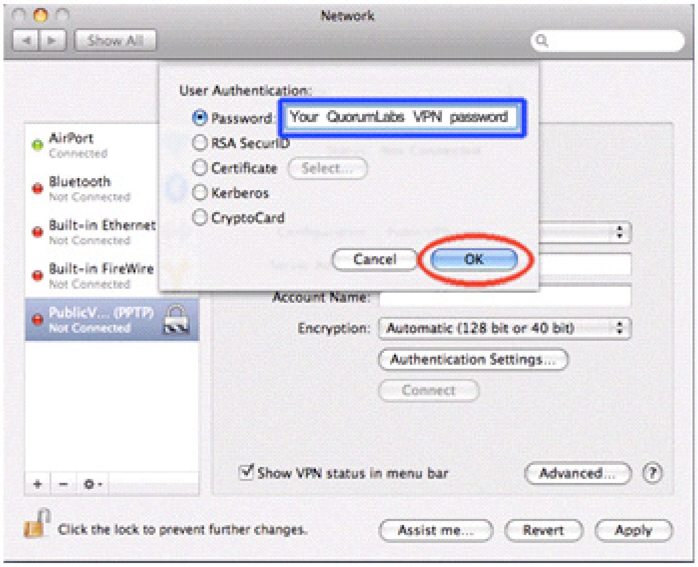
Account Name: DR VPN Username

Encryption: Automatic (128 bit or 40 bit)

☑ Show VPN status in menu bar

Click the lock to prevent further changes.

f. In the **Password** radio button field, specify your Quorum username, then **OK**.



User Authentication:

● Password: Your QuorumLabs VPN password

○ RSA SecurID

○ Certificate

○ Kerberos

○ CryptoCard

Encryption: Automatic (128 bit or 40 bit)

☑ Show VPN status in menu bar

Click the lock to prevent further changes.

7. Adjust the VPN settings:

a. From the **Network** page, click the **Advanced...** button at the bottom of the page.

b. Select the **Send all traffic over VPN connection** check box. You must do so in order for the connection to work effectively.

c. (Recommended) Select the **Use verbose logging** check box. This option makes it easier to see additional information in the event that you have connection problems.

d. Click **OK**.

8. Save the configuration. Click **Apply** in the bottom right of the Network page.

9. Establish the VPN connection.

10. Verify that the DR is up. From a command line prompt, ping the DR's LAN IP address.

11. Log on to the DR's web portal. From a web browser, go to `https://<DR-LAN-IP-Address>`.

    You should now have full access to the RNs and File Level Backups on the DR.

Next Step: Step 4: Connect the Appliance to your network

3.2.4 Step 4: Connect the Appliance to your network

To connect the onQ Appliance:

1. Disconnect the standalone computer and connect the onQ Appliance to your target network using the active RJ-45 connection.

2. Verify that you can launch the onQ Portal.

   After the onQ Appliances reboot, you should be able to launch the onQ Portal from a browser anywhere on your network to the onQ local and onQ remote addresses (or names, if DNS is properly configured) that were configured above.

3. Reboot the onQ Appliance.

Next Step: Step 5: Change hypervisor's NTP server

3.2.5 Step 5: Change hypervisor’s NTP server

Your onQ Appliance’s hypervisor uses a default NTP server (`clock.fmt.he.net`). Set the NTP server to a local NTP server. To change the hypervisor’s settings, go to Configure Appliance’s hypervisor settings.

Next Step: Step 6: Enroll protected nodes

Related Topics

Synchronize system time

3.2.6 Step 6: Enroll protected nodes

Each protected node must be enrolled with the HA. For instructions, go to:

- (Agent-based Windows PNs) Enroll protected nodes
- (Agent-based Linux PNs) Enroll protected nodes
- (Agent-less Linux/Windows PNs) Enroll protected nodes
- Enrollment in Windows Cluster Services Environment

When you log on to the HA’s onQ Portal, don’t forget to use the new password that you set in Step 4 of Step 2: Configure the onQ Appliances.

Next Step: Step 8: Configure RN startup dependencies

3.2.7 Step 7: (onQ Flex) Modify RN Type and Build Policy

All newly enrolled PNs default to *OD* (RN type) and *Build-on-Demand* (build policy). You can change the RN type or build policy go to (onQ Flex) Modify RN type and/or RN build policy.

3.2.8 Step 8: Configure RN startup dependencies

If any of your recovery nodes depend on other recovery nodes (for example, your mail server depends on a Domain Controller), configure startup dependencies for such nodes. For instructions, go to “Configure startup dependencies” on page 328.

Next Step: Step 9: Start automated protection process

3.2.9 Step 9: Start automated protection process

Now you’re ready to start the automated protection process on both the HA and the DR Appliance. For instructions, go to Start node protection.

3.3 Initial Backup

When you first start protection on your nodes, onQ initiates a full disk image of the disks’ entire contents, including operating system, configuration, applications, and user data. Performing initial deduplication and storing the data on the HA takes time.

Transferring gigabytes or terabytes of data over a relatively low-bandwidth WAN can be time consuming even with onQ’s integrated deduplication and compression.

One way to minimize the time consumed by this process is to take advantage of onQ’s exclude list feature, which enables you to specify folders and files that do not need to be backed up. See Edit backup exclude list for details.

After the initial cycle, or “base image”, the onQ backup process is always incremental, meaning that subsequent backups involve only new files or only the parts of large files that have changed. Subsequent backups involve far less data and are generally quite fast.

If practical, Quorum suggests that you perform the initial backup with both your HA and DR Appliance on the same LAN. You can also use a removable drive for the initial synchronization as outlined in Seed the DR Repository.

The subsequent backups begin based on the **Window Start** time, which you specified when you configured your PN’s **Backup Schedule** (see “Schedule backups” on page 274).

You can monitor progress of the backups. See Monitor protected nodes and Monitor DR Appliance. If you receive any email alerts, follow the instructions in Backup Alerts.

You know that the initial backup has finished on an HA by checking the **Backup Status** field on a **PN Status** page, and on a DR Appliance by checking the **RN Status** field on the **DR Status** page. After the initial DR backup completes, you can shut it down and move it to its permanent locale.

Related Topics

Backup and Recovery Workflow
Seed the DR Repository

Initiate immediate backups

3.4 Seed the DR Repository

The replication process between the HA Appliance (HA) and DR Appliance (DR) ensures that the DR repository is current with that of the HA. The repository synchronization process (aka “seeding”) can take place in different forms depending on different factors:

Reasons for seeding:

- Deploying onQ Appliances as part of an initial deployment.
- Re-synchronizing onQ Appliances due to other factors such as replacement/repair of onQ Appliances in the field.
- Enrolling new nodes on an HA that is currently in production. This process requires sending a full PN payload to the DR.
- Deploying a DR after an HA is up and running in production and, consequently, has a populated repository.

Location of the DR relative to the HA:

- HA and DR are on a local network.
- HA is local but DR is at a remote customer datacenter.
- Customer subscribes to the Quorum Hybrid Cloud service (aka *DRaaS*).

Forms of synchronization:

- LAN
- WAN
- Using a transportable, large capacity USB-attached disk
- Using a transportable, large capacity, encryption-capable NAS device (*ReadyNAS*)

The HA Appliance (HA) is designed to automatically seed the DR Appliance (DR) as part of its normal operation. When first deployed, the HA captures new, full snapshots of all the PNs and sends the snapshots to the DR. If both onQ Appliances are on the same LAN, the initial seeding process is no different than any follow-on, incremental snapshot, except in size. This automated process can also work when the HA is separated from the DR over a WAN but the link is fast enough to make the full synchronization practical. The data stream is de-duplicated against the repository on the DR, encrypted, and compressed to secure and optimize the transfer.

During the initial deployment it is best to co-locate the HA and DR so that the initial seeding can occur as soon as possible after the initial capture of the backup sets. After you enroll all the servers that need to be protected and their backups transfer to the DR, the DR can be disconnected and shipped to the desired, remote location. After the onQ Appliances are reconnected over the WAN, they begin synchronization of the newly captured snapshots.

If the co-location of the HA and DR is not possible during initial deployment and the bandwidth between the respective sites is not adequate to send the large, initial backup snapshots, other procedures can be used to facilitate the seeding of the DR. Quorum Support will work with you to determine and implement the best procedure for your environment.

- **Using externally-attached disk**: A large USB disk can be attached to the onQ Appliance that is large enough to accommodate the repository. This process involves copying the entire repository to the disk and transporting it to the remote site for seeding the DR. A large NAS storage device can be used instead of the USB disk to perform the same function. Quorum Support assists in attaching the NAS device to the onQ Appliances.
- **Using a NAS Storage device (Hybrid Cloud/**DRaaS**)**: To facilitate the seeding of your DR in the Quorum cloud (aka *DRaaS*), Quorum loans you an encryption-capable NAS device (*ReadyNAS*). Upon initial deployment of your HA, the NAS is attached and configured to receive all initial snapshots intended for the DR. After you enroll all PNs and onQ captures all the initial snapshots, the NAS device is detached and shipped to Quorum for seeding your DR in the Quorum cloud. Quorum transfers the data from the seed unit to the storage repository and wipes the NAS device. After the seeding completes, the HA begins to transfer new snapshots over the WAN to the Quorum cloud as they are captured.

To help discern whether or not WAN seeding/synchronization to the DR is practical, the estimates below are provided as a reference point. Seeding estimates are a function of your internet connection speed.

WAN Speed (mbps)	Estimated DRaaS Seeding Time (hrs)/TB[a]
50	117
100	58

[a] Assumes 50% WAN bandwidth utilization for seeding

Related Topics

(Workflow) Fail over HA to DR Appliance
Backup and Recovery Workflow
Resize protected node’s vdisk

4

The Basics

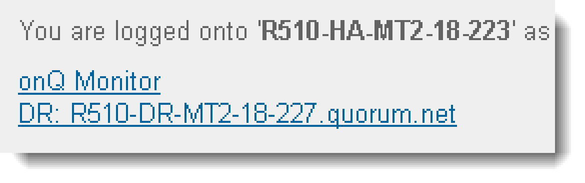
4.1 Log on to Appliance's user interface

You need a supported browser (see Browser Support) to access the onQ Appliance's user interface.

- onQ is delivered with pre-defined user names and passwords for `Admin` and `VARAdmin`. If you did not change the default passwords as recommended in Step 2: Configure the onQ Appliances, use the defaults outlined in Change user passwords.
- Each onQ user is pre-assigned one of three roles: *Administrator*, *Operator*, *VARAdmin* or *Restore.* Each role implies a different level of permission to access certain UI features. For more information, go to Add users.

To log on to the onQ Appliance:

1. (Hybrid Cloud Only) Initiate a VPN connection to Hybrid Cloud.
2. Ensure that:
   - JavaScript is enabled on your browser.
   - the onQ Appliance is in your browser's Trusted Sites list.
3. Point the browser to the onQ Appliance's LAN IP address. You assigned this IP address during the configuration process. See Step 2: Configure the onQ Appliances.

> **Note:** Alternatively, you can access a DR Appliance from the HA's page footer links:
>
> 
>
> You are logged onto 'R510-HA-MT2-18-223' as
>
> onQ Monitor
>
> DR: R510-DR-MT2-18-227.quorum.net

4. Type in your user credentials.

4.2 Establish a VPN connection to Hybrid Cloud

How you establish a VPN connection to Hybrid Cloud depends on your operating system.

To establish a VPN connection to Hybrid Cloud (Windows 7):

1. From the **Network and Sharing Center**, right-click on **DR VPN Connection**, then **Connect**.
2. Type the credentials that your Quorum Support Engineer provided you, then **Connect**.
3. Wait a few seconds for your client to establish a VPN Connection to the Quorum Data Center.

To establish a VPN connection to Hybrid Cloud (Windows XP):

1. From **Network Connections**, right-click on **DR VPN Connection**, then **Connect**.
2. Type the credentials that your Quorum Support Engineer provided you, then **Connect**.
3. Wait a few seconds for your client to establish a VPN Connection to the Quorum Data Center.

   If authentication is successful, the Connection window minimizes to your taskbar as a dual computer icon. Run your mouse over it to see the status of the connection.

To establish a VPN connection to Hybrid Cloud (Mac OS X):

1. Do one of the following:
   - Choose the VPN configuration from the VPN menu.
   - From the **Network** page, select your VPN connection from the connection list, then click the **Connect** button.
2. Wait a few seconds for your client to establish a VPN Connection to the Quorum Data Center.

4.3 Log off from Appliance's user interface

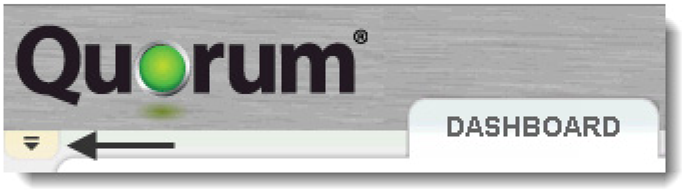
Logging off closes the user interface. You will need to log on again to restore the UI.

To log off:

1. Select the drop-down menu.
2. Choose **Log Off**.

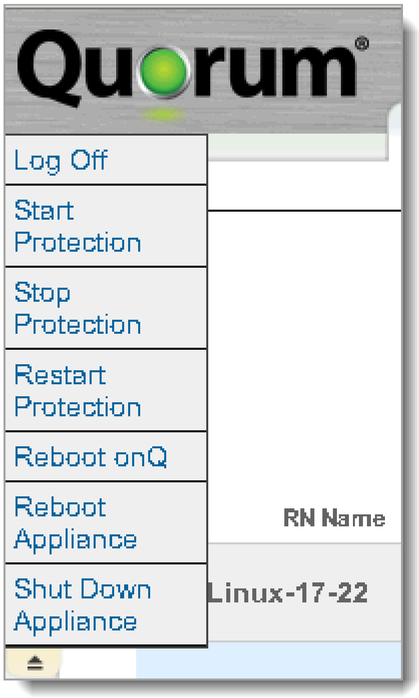
4.4 Drop-down menu

If you examine the left margin of the display, in the space to the left of the tabs and below the letter Q in the Quorum logo, you will discover a tiny icon that includes a representation of an arrowhead pointing downwards.



You can see this icon regardless of which major tab you have selected. When you click the icon, a pull-down menu appears as shown below:

The **Change Password** option does not display for users assigned to the `Administrator` role because such users can perform this task via the **USERS** page, unlike users assigned to the `Operator` or `Monitor` roles, which only have the **Change Password** and **Log Off** options.



When you open the menu, the drop-down icon migrates to the bottom of the menu and the arrowhead points upward. Click the icon again to close the menu.

The menu offers the following five critical actions. These are actions that must be selected cautiously. They can have undesired consequences if invoked accidentally. The tiny drop-down icon helps avoid unintended choices.

Log Off

Start Protection

Stop Protection

Restart Protection

Reboot onQ Manager

Reboot onQ Appliance

Shut Down onQ Appliance

4.5 Reboot onQ Manager

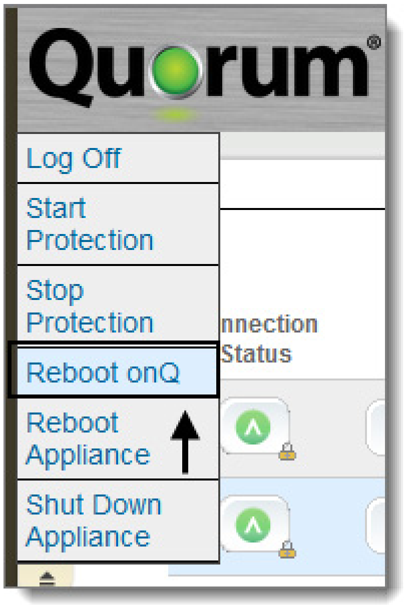
Some software upgrades require that you reboot the virtual machine on which the onQ Manager depends. In doing so, all processes managed by the onQ Manager are restarted. The underlying hypervisor, however, is not affected and neither are any RNs running in production or test mode.

A reboot temporarily stops protection. However, onQ Manager returns the onQ Appliance to its original protection state after the reboot:

- If protection was *on* prior to the reboot, onQ Manager turns on protection after the reboot.
- If protection was *off* prior to the reboot, onQ Manager does not turn on protection after the reboot.

To reboot the onQ virtual machine:

1. Log on to the onQ Appliance's onQ Portal.
2. Select the drop-down menu.
3. Choose **Reboot onQ**.



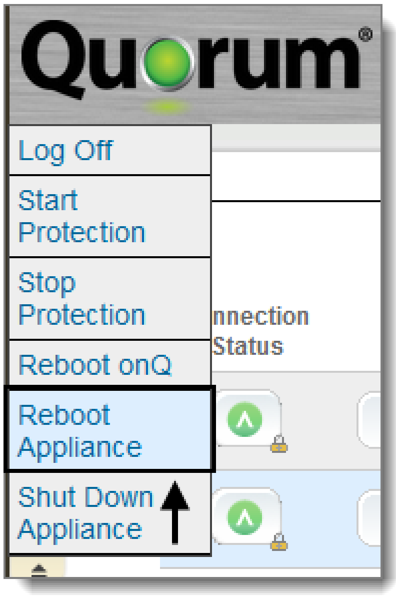
4. Click **Continue** to initiate the reboot.
5. After the onQ Manager reboots, verify that protection is on.

4.6 Reboot Appliance

Use this procedure to restart the entire onQ Appliance. The hypervisor and all processes managed by the hypervisor are restarted. Rebooting the onQ Appliance interrupts all protection operations and stops all recovery nodes.

To reboot the onQ Appliance:

1. Log on to the onQ Appliance's onQ Portal.
2. Select the drop-down menu.
3. Choose **Reboot Appliance**.



4. Click **Continue** to initiate the reboot.

   After the onQ Manager reboots, don't forget to restart protection.

4.7 Shut down or Restart Appliance

Use this procedure to immediately halt the onQ Appliance. The hypervisor and all processes managed by the hypervisor are halted. Shutting down the onQ Appliance interrupts all protection operations and stops all recovery nodes.

To shut down the onQ Appliance:

1. Log on to the onQ Appliance’s onQ Portal.
2. Select the drop-down menu.
3. Choose **Shut down** onQ Appliance.

To restart the onQ Appliance:

1. Ensure that the power is off, then turn it on (power-cycle).
2. Restart protection.
3. Restart any recovery nodes that were in use before the reboot occurred, if they don’t start automatically.

   Virtual machines hosted on a hypervisor (specifically XenServer) start automatically when the onQ Appliance reboots. However, sometimes a virtual machines do not start up automatically upon reboot of the onQ Appliance.

4.8 About onQ Proxy

PNs need the onQ Proxy, not to be confused with onQ Central Proxy and PN Proxy or Proxy Host, to communicate with onQ for backups. PNs can share an onQ Proxy (aka *global* onQ Proxy) or each PN can have a separate onQ Proxy.

If you do not specify an onQ Proxy for the PN, onQ uses the global onQ Proxy. If you do not specify a global onQ Proxy, onQ uses its own IP address.

If you have any PNs on a different subnet, such as in a DMZ, you must specify an onQ Proxy on the PN itself. However, at the time of enrollment, the PN does not have a configuration so you cannot set its onQ Proxy until after enrollment. Therefore, before enrollment of a PN on a different subnet, you must temporarily set the global onQ Proxy to the onQ Proxy for that PN. After enrollment, revert to the global onQ Proxy.

4.9 Configure Appliance’s network settings

Your onQ Appliance has a variety of network settings:

- Fully Qualified Host name
- onQ Role (see Change Appliance’s role)
- IP Address
- Subnet Mask
- Default Gateway
- onQ Proxy Address (see About onQ Proxy)
- Preferred DNS Server
- Alternate DNS Servers
- onQ Appliance’s role
- Time zone (except in the case of DRaaS/AVaaS, set this time zone to match hypervisor’s time zone as outlined in “Configure Appliance’s hypervisor settings” in onQ Administrator’s Guide.)

To modify an onQ Appliance’s network settings:

Renaming of onQ is rare, but there are circumstances that might require that you to do so:

- Your company name or location changed, and your host name needs to realign with this new identity.
- You initially deployed one onQ, and now you’re adding another.
- You are replacing your onQ Appliance so as to upgrade the hardware. There cannot be two onQs with the same name. In this case, you would have two onQs with the same name until after the data from old onQ Appliance migrates to new onQ Appliance.

In the case of an agent-less PN enrollment, if you need to rename your onQ, do one of the following:

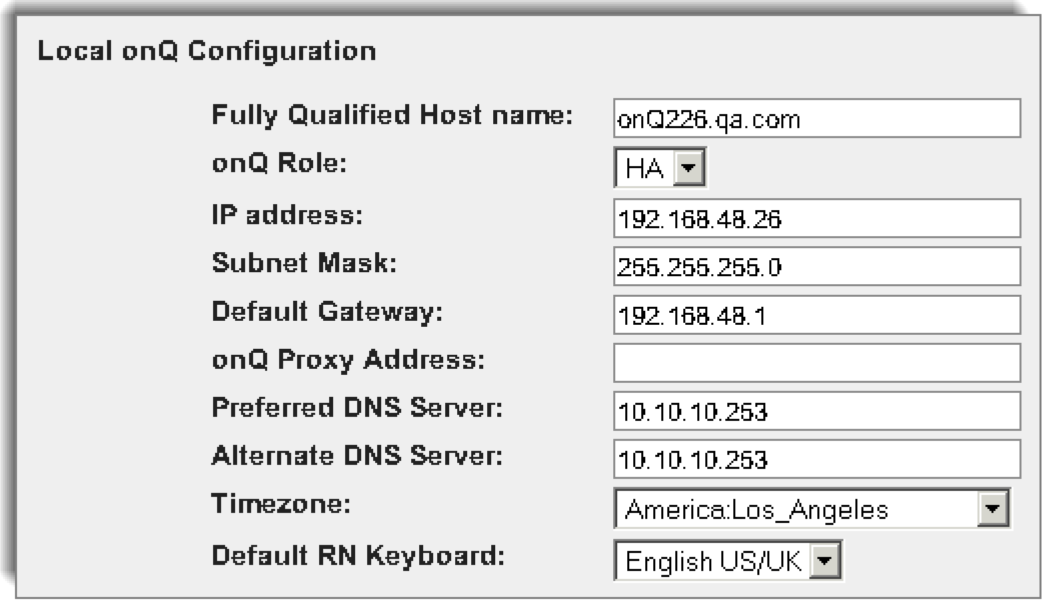
- If you have only one PN: (1) From the onQ Portal, delete the PN (Delete protected nodes), choosing to retain ...`the associated data from the repository and corresponding RN`.... (2) Rename the onQ. (3)

Re-enroll the PN as outlined in (Agent-less Linux/Windows PNs) Enroll protected nodes.

- If you have multiple PNs: (1) Rename the onQ; (2) On each ESXi/ESX server, delete from disk all PN proxies that use the old onQ host name. (3) Re-enroll the PNs as outlined in (Agent-less Linux/Windows PNs) Enroll protected nodes.

1. Log on to the onQ Appliance's onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **onQ (LOCAL)** page > **MODIFY** button.

   The **Modify Local onQ Setup** page appears:



Local onQ Configuration

Fully Qualified Host name:	onQ226.qa.com
onQ Role:	HA
IP address:	192.168.48.26
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.48.1
onQ Proxy Address:	
Preferred DNS Server:	10.10.10.253
Alternate DNS Server:	10.10.10.253
Timezone:	America:Los_Angeles
Default RN Keyboard:	English US/UK

3. Make your change, then click **SAVE**.

   Click **REVERT** to return the fields to their initial values, or click the cancel icon (at the upper left) to discard your changes and return to the previous page.

4.10 Configure Appliance's hypervisor settings

Except in the case of DRaaS/AVaaS, you can configure a variety of settings related to your onQ Appliance's hypervisor, including:

- Hypervisor name
- NIC Speed (not configurable: onQ Portal reports the speed that’s detected)
- Hypervisor IP Address
- Hypervisor Password
- Subnet Mask
- Default Gateway
- Preferred DNS Server
- Alternate DNS Server
- NTP Server (default is `0.us.pool.ntp.org`)
- Time zone (set this time zone to match the onQ Appliance’s time zone as outlined in “Configure Appliance’s network settings” in onQ Administrator’s Guide.)
- iDRAC (see Configure iDRAC)

To configure an onQ Appliance’s hypervisor settings:

Your onQ Appliance’s hypervisor is XenServer. The onQ Appliance ships with the hypervisor information pre-configured.

The hypervisor name is based on a Quorum naming convention: Hyper-Q-*CustomerName-ApplianceType*. This naming convention provides you the best customer support possible because it communicates the onQ Appliance’s role and your topology.

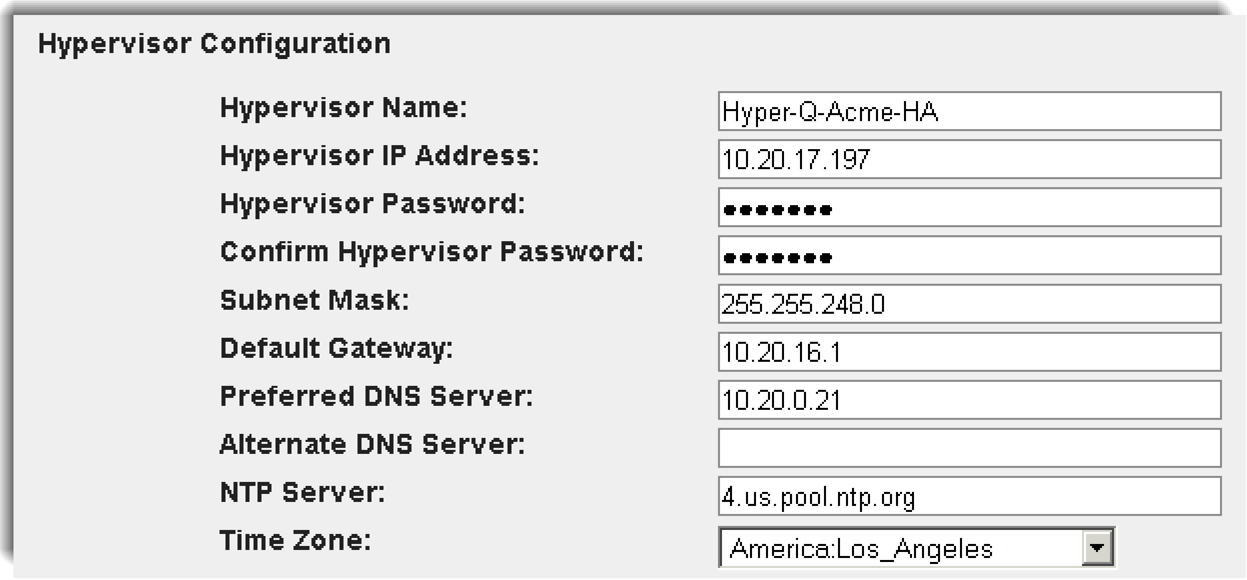
Quorum recommends that you retain the pre-configured hypervisor name; however, Quorum recognizes that your company might have its own naming conventions. Before you change the hypervisor’s name, contact Quorum Support with your naming convention requirements so that we can rename the hypervisor. without losing sight of the relationships between onQ Appliances.

Hyper-Q-Acme-HA	Acme’s HA.
Hyper-Q-Acme-DR	Acme’s DR Appliance.

Hyper-Q-Acme-DRaaS	Acme's Hybrid Cloud.
AV-Acme-DR	Acme's AV Appliance, which is an archive of the DR Appliance.
AV-Acme-HA	Acme's AV Appliance, which is an archive of the HA.
Hyper-Q-Acme-MT1	One of Acme's multi-tenant onQ Appliances. Multi-tenancy is identified by the Configuration field under **Dashboard** tab > **onQ Status** page.

1. Log on to the onQ Appliance's onQ Portal. You must log on as `varadmin` user.
2. Click the **APPLIANCE CONFIG** tab > **HYPERVISOR** page > **MODIFY** button.

   The **Modify Hypervisor Config** page appears.



Hypervisor Configuration

Hypervisor Name:	Hyper-Q-Acme-HA
Hypervisor IP Address:	10.20.17.197
Hypervisor Password:	●●●●●●●
Confirm Hypervisor Password:	●●●●●●●
Subnet Mask:	255.255.248.0
Default Gateway:	10.20.16.1
Preferred DNS Server:	10.20.0.21
Alternate DNS Server:	
NTP Server:	4.us.pool.ntp.org
Time Zone:	America:Los_Angeles

3. Make your changes, then click **SAVE**.

   Click **REVERT** to return the fields to their initial values, or click the cancel icon (at the upper left) to discard your changes and return to the previous page.
4. Reboot the onQ Appliance.

4.11 Configure iDRAC

iDRAC (integrated Dell Remote Access Controller) is a "lights out" remote management capability included in most onQ Appliance models. The iDRAC allows Quorum Support to:

- determine the health of the onQ Appliance’s hardware.
- diagnose hardware problems.
- start a remote console to observe the onQ Appliance boot messages.
- change settings.

The iDRAC is an important tool for the support and maintenance of your onQ Appliance. Quorum strongly recommends that you connect and configure the iDRAC when you deploy your onQ Appliance(s).

Quorum and Quorum MSPs pre-configure the iDRAC’s default password. If you don’t know the default password, contact Quorum Support. Quorum Support can provide more efficient support if you retain the default password. However, Quorum recognizes that some customers (banks and health care organizations) might have policies that instruct you to change the default password to a unique password; in this case, Quorum Support or Quroum MSP can use a TeamViewer session as an alternative to using the default password or communicating your unique password.

To connect iDRAC:

The iDRAC network port is located on the rear, left side of your onQ Appliance. The port is a standard RJ45 Ethernet connection. The network port is identified by an icon that looks like a wrench or the word `iDRAC`. Use a standard Ethernet patch cable to connect the iDRAC port to an Ethernet switch.

> **Note:** The Quorum onQ T20 model does not have an iDRAC. All other onQ Appliances include the iDRAC as a standard feature.

To configure iDRAC:

Configure your iDRAC network settings for your subnet. If you later make a change to your network, or move the onQ Appliance to another subnet, the iDRAC settings must change too for your onQ Appliance to be reachable.

1. Log on to the onQ Appliance's onQ Portal. You must log on as `varadmin` user.
2. Click the **APPLIANCE CONFIG** tab > **HYPERVISOR** page.
3. Click the **iDRAC** button. The iDRAC dialog appears.

   The onQ Portal displays an error if your onQ Appliance does not have iDRAC. If you know that the onQ Appliance has iDRAC, click the iDRAC button again: Sometimes a temporary networking glitch can cause iDRAC to become unavailable.
4. Click **MODIFY**, make your changes, then **SAVE**.

4.12 Unlock UI

The onQ Portal has pages that have icons that lock and unlock. This feature ensures that you don't make an unintentional change to your protection configuration. Only users of role *Administrator* or *Operator* can unlock these icons; users of role *Monitor* cannot unlock these icons.

After you unlock the icons they become command buttons, enabling you to perform certain actions. To unlock these icons, simply use the padlock icon to toggle between these two states:

🔒	click to enable UI command buttons
🔓	click to disable UI command buttons

For example, if the padlock icon shows a closed padlock and is labeled **Unlock to enable actions**, you can view the status information related to protected nodes, but you cannot perform any actions.

To unlock the UI for a given page:

1. Go to the page you want to unlock:
   - (HA) **DASHBOARD** tab > **PROTECTED NODES** page
   - (DR) **DASHBOARD** tab > **DR STATUS** page
   - (HA and DR) **DASHBOARD** tab > **RECOVERY NODES** page

2. Locate the closed padlock icon in the lower left corner.
3. Click on the icon to switch the icon to the open state, assuming the icon is in the closed state.

   The icon changes to an open padlock and is unlabeled. Some of the fields in the table are revealed to be clickable buttons:

4.13 (Agent-based PNs) Restart the onQ Service

If the onQ Service is not running on the protected node, the HA cannot establish a secure connection to that protected node. Restarting the onQ Service during a backup or upgrade can cause backup/upgrade failures.

(Windows) To restart the service:

1. RDP to the PN.
2. Go to:

   Start > **Programs** > **Control Panel** > **Services**

   OR

   Start > **Administrative Tools** > **Services**
3. Right-click on **Quorum onQ Monitor** (aka onQ Service), and choose **Restart**.

(Linux) To restart the service:

1. Verify that the service is installed:

   ```
   > rpm -qa | grep node
   ```
2. Start the service:

   ```
   > service dcrm-node start
   ```

4.14 Modify protected nodes

During the setup process you identified the nodes you wanted to protect. From time to time you might need to change the settings on these nodes.

To edit a protected node (HA):

1. Log on to the HA’s onQ Portal.
2. Click the **PROTECTION CONFIG** tab.
3. Select the node that you want to modify, then click **MODIFY**.

   The Modify a Protected Node page appears.
4. Make your changes to the node parameters. You cannot change the **Hostname** field from the **MODIFY** window.
5. Click **SAVE** to save your changes and return to the **PROTECTION CONFIG** tab.

   A newly modified protected node appears in the list.
6. Restart protection, if applicable.

To edit a protected node (DR Appliance):

1. Log on to the DR Appliance’s onQ Portal.
2. Click the **PROTECTION CONFIG** tab.
3. Select the node that you want to modify, then click **MODIFY**.

   The Modify a Protected Node page appears.
4. Specify values for the node parameters.

   You cannot change the **Hostname** field from the **MODIFY** window.
5. Click **SAVE** to save your changes and return to the **PROTECTION CONFIG** page.

   A newly modified protected node appears in the list.

4.15 Delete protected nodes

During the setup process you identified the Protected Nodes (PN) that you want to protect.

You might want to delete a specific PN if:

- You removed the host from production. In this case, you want to "free up" a license or vdisk disk space, especially if you don't have enough disk space to enroll protected nodes in production. Licensing is based on the number of nodes being protected.
- You want to move the PN to another HA. Only one HA can protect a given PN.

The onQ Portal will not let you delete a PN if:

- PN is in production.
- PN is being backed up.
- HA's RN is in test mode, production mode, or in the process of being tested (self-test) or updated.
- DR Appliance's RN is in the process of being tested (self-test) or updated.

However, if you think you might have plans for the PN in the future, disable it instead.

To delete a PN:

After you delete the PN, you cannot start the RN on the HA. Also, When you delete a PN on an HA, onQ automatically propagates that deletion on the DR Appliance, in addition to removal of PN data if you instruct onQ to do so.

1. Log on to the HA's onQ Portal.
2. Ensure that the HA-to-DR link is working. Go to Test HA-to-DR Link.
3. Disable protection for the PN that you want to delete, then do the following if applicable:
   - If PN backup is in progress, either wait for it to complete or stop the backup.
   - If RN update is in progress, either wait for it to complete or stop the update.
   - If RN is running a self-test, wait for it to complete.

- If RN is running in test or production mode, power off the RN.

4. Click on the **PROTECTION CONFIG** tab, then select the PN from the list.
5. Click the button labeled with the minus sign (**-**).

Warning: Deleting a PN purges the PN’s virtual machine (vdisk); a deletion does not purge all the data associated with that PN. If you delete orphan data for a given PN, Quorum recommends that you do so for both the HA and the DR. If you remove orphan data for a given PN from the HA—but not from the DR, then later re-enroll that same PN on the same HA, the DR fails to add the future snapshots for this PN thereby compromising disaster recovery.

6. (Optional) Select the **Remove**... check box to delete all the PN’s data, then **Yes**. Alternatively, delete the orphan data later.

   The onQ Portal returns you to the **PROTECTION CONFIG** tab, and the PN disappears from the list.

4.16 Protected Node Parameters

Specify these parameters when you want to change a protected node's configuration from the **PROTECTION CONFIG** tab.

- Basic Parameters
- Recovery Node Configuration Parameters
- Advanced Parameters

4.16.1 Basic Parameters

- **Hostname:** If you are adding a protected node, type the host name of the node to protect. This field is display-only in **MODIFY** dialog.
- **IP Address:** If you are adding a protected node, type the IP address of the node to protect. This field isn't dispayed in **MODIFY** dialog.
- **Proxy Host**. (This parameter is not applicable for agent-based enrollment.) This is the ESX/ESXi server that's hosting the PN proxies.
- **onQ Proxy Service Rev**: (This parameter is not applicable for agent-based enrollment.) The software revision running on the PN proxies.
- **onQ Node Service Rev**: (This parameter is not applicable for agent-less enrollment.) The software revision running on the PNs.
- **Backup Mode**: (This parameter is not applicable for agent-based enrollment.) As outlined in "(Workflow) Fail over a PN to an RN" on page 337 and "(Workflow) Fail back an RN to a PN" on page 339, this parameter reflects whether onQ is currently backing up the agent-less PN (`Agentless`) or the RN (`Recovery Node`) in production mode. onQ Portal changes this parameter automatically as it powers on and off the RN.
- **Group Name**. A logical means of grouping your PNs. Groups are required to configure startup dependencies as outlined in Configure startup dependencies. For Agent-less PNs, the onQ Portal groups the PNs by ESXi server. If you do not want these PNs in such a group, clear the default Group Name field at the time of enrollment to remove the PNs from this group and place them in the shared pool.
- **Backup Schedule**. onQ performs an initial backup of your PNs when you first start protection. Modify the default backup schedule to instruct onQ

when and how often to perform subsequent backups. Go to Schedule backups.

- **Backup Retention Time**. PN's retention policy. The maximum number of days to retain backed-up data that is no longer referenced. Go to Change Backup Retention Policy.
- **File Backup Only**: PN's file backup policy. When set to **Yes**, squirtcopy backs up only those files and folders that you specify in the Backup Include List and only if you specify the disk drives and mount points for those files and folders, as outlined in Edit backup include list. This parameter can only be enabled by Quorum Support and is typically used only for file servers. Note the following when this parameter is enabled:
  - **Auto RN Creation?** parameter is hidden when **File Backup Only**=Yes because it is not applicable.
  - **Recovery Node Configuration** pane is hidden when **File Backup Only**=Yes because the protected drives are determined via the Backup Include List.
- **OS Type?**: PN's operating system. Both Linux and Windows operating systems are supported, though the parameters available vary. This field isn't displayed in the **Modify a Protected Node** dialog.
- **Auto RN Creation?**: PN's RN build policy, which instructs onQ when to create a recovery node. On-Site/Prime/Plus users can change this policy from the **Add a Protected Node**/**Modify a Protected Node** dialog, but onQ Flex customers must do so from the onQ Flex Manager. This policy represents your potential downtime in the event of a disaster (aka RTO). See also "(On-Site/Prime/Plus) Modify RN build policy" on page 240 or "(onQ Flex) Modify RN type and/or RN build policy" on page 243, depending on your configuration.
- **Disable Protection?**: PN's protection policy. Select **No** to enable or **Yes** to disable protection for this node. If you disable protection, the most recent re-build of the recovery node is retained but backups are suspended. If you disable protection while a backup is in progress or an RN is being rebuilt, that process continues to completion but further backups are suspended. When you re-enable protection, backups resume and subsequent RN rebuilds are based on the existing RN. See "Disable protection of nodes" on page 247.

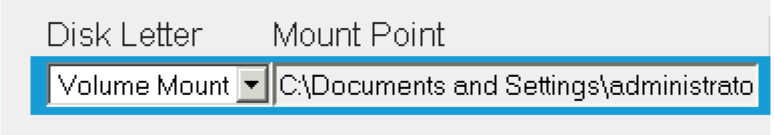
4.16.2 Recovery Node Configuration Parameters

There are a few recovery node parameters that vary slightly depending on the operating system:

- **Number of CPUs**: # of CPUs for this recovery node.
- **RN Memory**: RN’s memory in GBs.
- **RN Keyboard** (for console use). The supported keyboard that you want to use with the RN’s console.
- **Disk Letter**: Disk’s letter, Volume mount, or CIFS mount.
- **Mount Point**: This parameter varies by platform:
  - (Linux) Where the protected node’s filesystem is mounted.
  - (Windows) Full path to the directory in which this drive is mounted. Windows drives can be mounted to appear as a directory in another disk. These mounted drives must be protected separately:

    1.Select **Disk Letter** drop-down list > **Volume Mount**.

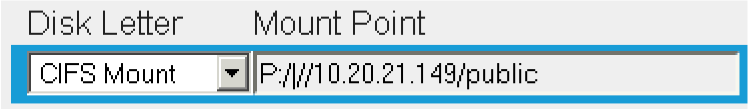
    2. In the Mount Point text box, provide the path to the directory. For example: `C:\Documents and Settings\administrator\My Documents\public`.



Disk Letter	Mount Point
Volume Mount	C:\Documents and Settings\administrato

  - (Windows) Full path (***<mount-point>|<url>*** where `url` is ***//<ip-address>/<path>***) to the mounted shared volume:

    1.Select **Disk Letter** drop-down box > **CIFS Mount**. For example: `P:/|//10.20.21.149/public`.



Disk Letter	Mount Point
CIFS Mount	P:/|//10.20.21.149/public

To avoid mapping conflicts, refer to Enable onQ to back up shared volumes.

2. In the Mount Point text box, provide the path to the directory.

3. Set the necessary privileges as outlined in Enable onQ to back up shared volumes.

- **Format**: File system type. This parameter is for Linux only. For requirements and limitations, go to Linux Filesystem Format Requirements.
- **VDs**: # of virtual disks required to hold the configured disk. Every multiple, or portion thereof, of 1980GB requires a virtual disk. For Unix RNs, each configured disk must fit on a single VD: spanning of virtual disks is only supported for Windows RNs.
- **Size**: Size of the disk in GBs. Due to a XenServer limitation, a single protected volume for Linux PNs is limited to a maximum size of 2TB. See Linux RN Limitations for more information.
- **+**: Adds a new line to the Recovery Node Configuration list. In some cases, you need to manually add mount points. See Linux Filesystem Format Requirements for more information.
- **-**: Removes a highlighted line from the Recovery Node Configuration list.
- **REVERT** button REVERT : Reverts all the fields to the last saved values.

4.16.3 Advanced Parameters

There are several advanced parameters that are accessible from the **PROTECTION CONFIG** tab > **ADVANCED** button.

- **Disable Replication to DR?**: Select **No** to enable or **Yes** to disable replication for this node. You might want to disable replication if this node is not important for business continuity, but you do want backups and the ability to archive them. If you are unsure, keep this setting enabled. See Disable replication for individual nodes.
- **Execute Pre Snapshot script?** (This parameter is not applicable for agent-less enrollment.) Executes before a snapshot starts on the protected node. See "Run custom backup scripts" on page 298.
- **Execute Post Snapshot script?** (This parameter is not applicable for agent-less enrollment.) Executes soon after a snapshot completes on the protected node. See "Run custom backup scripts" on page 298.
- **Enable Filter Driver?** (This parameter is not applicable for Linux-based protected nodes and agent-less enrollment.) See "(Agent-based PNs) Methods of Performing Incremental Backups" on page 302.
- **Truncate SQL logs after backup?** (This parameter is not applicable for Linux-based protected nodes.) After a successful backup, onQ truncates the SQL logs.
- **VSS Copy Only?** (This parameter is not applicable for agent-less enrollment.) onQ's backup utility clears VSS flags after it performs backups. This process can conflict with some applications (for example, Backup Exec) that depend on these VSS flags. For example, other backup products can trigger Exchange and SQL Server to truncate log files after incremental backups. Only change this setting to **Yes** if you are using an application that relies on and updates these VSS flags; otherwise, set this parameter to **No** (default). Setting this parameter to **Yes** ensures that onQ does not alter or reset VSS flags and leaves your files, generally transaction logs, as-is.
- **PN Scan Threads:** This is the number of threads used during the scan process. The more threads used, the more likely you are to lock up your PN. If you are unsure, specify 1 thread.
- **PN Transfer Threads**: The number of threads used during the backup process. The more threads used, the sooner the backup process completes. Ensure that the client machine has enough resources to handle the number of threads you specify. If you are unsure, specify 4 threads.

- **CPU Resource Limit:** Sets the CPU usage limit for the backup process on the protected node during the transfer phase. The default is 30% of all cores.
- **Disk Resource Limit:** Sets the disk bandwidth limit for the backup process on the protected node during the transfer phase. The default is 170 MB/second.
- **Network Resource Limit:** Sets the network bandwidth limit for the backup process on the protected node during the transfer phase. The default is 170 MB/second.
- **Enable Cluster Support?**: (This parameter is not applicable for Linux-based protected nodes. Also, for information on how to work with PNs/RNs in a cluster environment, refer to Enrollment in Windows Cluster Services Environment.) If you select **Yes**, specifies that the node is part of an MSFT cluster (Microsoft Cluster Server/MSCS). In a nutshell, cluster support works by creating a virtual SAN to replicate your physical SAN. The PN accesses the SAN using a virtual IP address. For each volume, the onQ Appliance creates a virtual disk.
  - **Cluster Volumes**: PN's volumes/partitions. List of non-boot drives. From this list, choose the volumes that correspond to your cluster.
  - **Virtual SAN IP Address**: Any dedicated and unique IP other than the SAN's physical IP address. This IP address must be on the same sub-net as the onQ Appliance's physical IP address.
  - **Virtual SAN Gateway Address**: Virtual SAN's Gateway address.
  - **Virtual SAN Subnet Mask**: Virtual SAN's subnet.
- **onQ Proxy Address**: Specifies the onQ Proxy that the PN needs to use to communicate with the onQ for backups. Unless your PN is on a separate subnet, leave this field blank. For more information, go to About onQ Proxy.
- **Backup Exclude List**: The button shows the exclude list to be either **DEFAULT** (as defined by Quorum) or **CUSTOM** (as defined by your administrator). Click the button to modify the backup exclude list for this protected node. See "Edit backup exclude list" on page 268.
- **Backup Include List**: onQ backups up only those files and directories that you specify. This button appears if **File Backup Only** is enabled. See "Edit backup include list" on page 271.
- **Startup Dependencies**. onQ will start a given RN after the RNs on which it depends are up and running. See Configure startup dependencies.

- **RN Services**. Some services installed on a PN will cause problems if they attempt to run on the RN. In this case, you can configure the startup settings for these services. See Edit RN services list.
- **RN Networks**. onQ enables your RNs to run on multiple networks. See Create Custom Networks for RNs.

Related Topics

Modify protected nodes
(Agent-based PNs) Add protected nodes manually
(Agent-based PNs) Restart the onQ Service

5

Enrollment in non-cluster Environment

5.1 (Agent-based Windows PNs) Enroll protected nodes

onQ supports both agent-based and agent-less PNs. Nodes that are not hosted by VMware require that an agent (onQ Service) be installed. Agent-based enrollment enables you to use all of the operation and monitoring features that onQ has to offer.

Each agent-based PN must be "enrolled" with the onQ HA using the **Protect Me** button and the onQ EZ Installer, which analyzes your PN and pre-configures it on the onQ Appliance.

Even if you added the new node manually and it appears in the list of protected nodes, you must enroll the node before the onQ Manager can protect it. Previously protected nodes that are still running the onQ Service do not need to be enrolled; in this case, simply add the nodes manually, then start protection.

This *Protect Me-based* enrollment instructs the PN to download and extract the `QuorumWinBCVSetup<bitVersion>-BCV<build>.ez` package from the onQ Portal's **Downloads** tab. This package is only used for Protect Me-based enrollments, not *manual* installs.

Warning: In almost all instances, Non-NTFS partitions are *not* supported for VSS-based snapshots. Do not protect such partitions with onQ. Protecting such non-NTFS partitions might result in the Quorum agent terminating the backup. The only exception is a volume configured with REFS, which is available in Windows Server 2012.

(Recommended) To enroll an agent-based Windows PN:

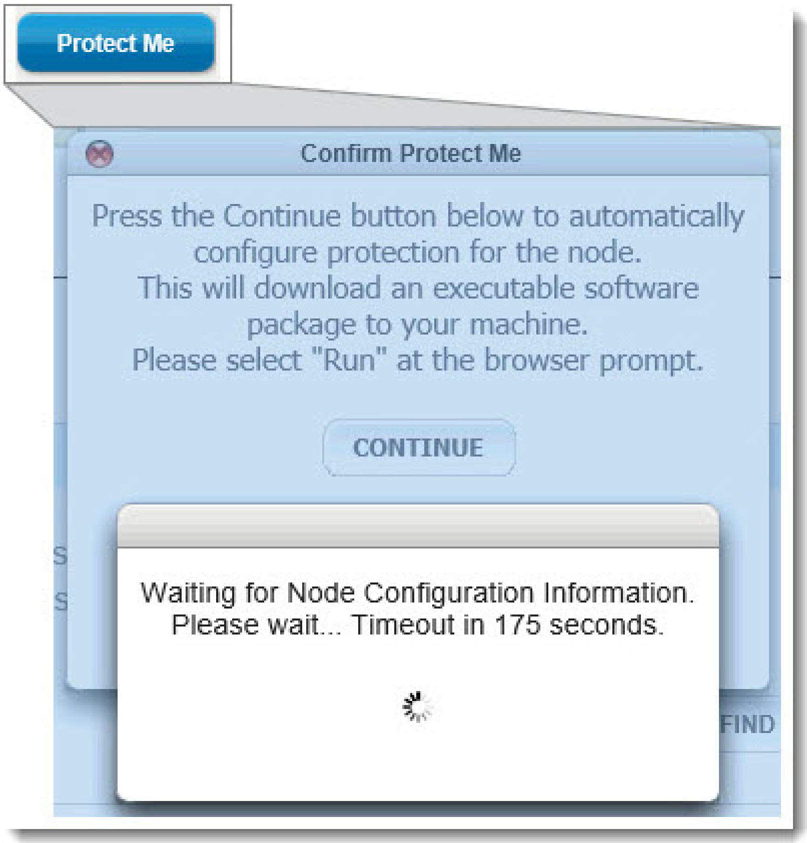
Use this procedure if you're trying to install an agent-based Windows PN for the first time. You must perform this procedure from the node that you want to enroll. Repeat this procedure for each node that you want to enroll.

Warning: If your Windows 2012 PN is running on the VMware host and uses the VMware E1000E network interface adapter, squirt-server might receive a corrupted `source.info` from squirtcopy due to a problem with VMware's NIC, as outlined in VMware KB 2058692. To prevent this problem, on the VMware-hosted PNs, switch the NIC type from E1000E to E1000.

1. Verify that your platform is supported. Go to Platform Support.
2. (Important!) If any of your PNs were previously enrolled, search for and delete all orphan data for those PNs on both the HA and the DR.

   If you remove orphan data for a given PN from the HA—but not from the DR, then later re-enroll that same PN on the same HA, the DR fails to add the future snapshots for this PN thereby compromising disaster recovery.
3. RDP to the server that you want to enroll as a PN, then log on as a user with administrative privileges.
4. From that server, launch a browser (see "Browser Support" in onQ Release Notes).
5. Log on to the HA's onQ Portal as `varadmin`.
6. In the onQ Portal, go to **PROTECTION CONFIG** tab > **Protect Me** button, then **CONTINUE**.

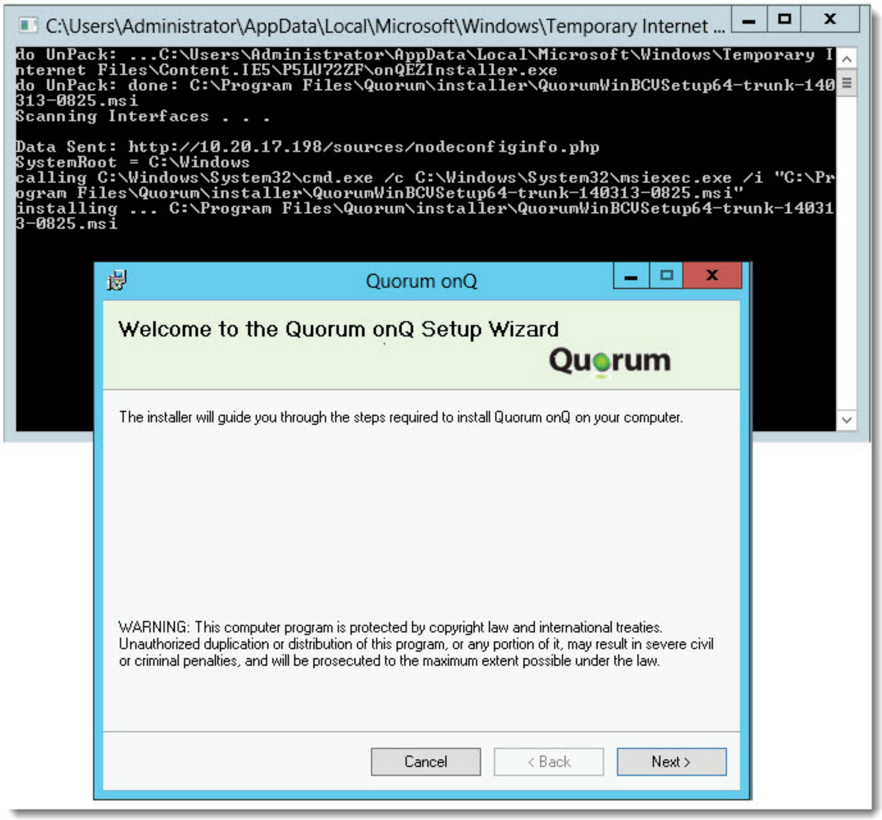
Note: The protection process instructs the PN to download and extract the `QuorumWinBCVSetup<bitVersion>-BCV<build>.ez` package from the onQ Portal's **Downloads** tab. This package is only used for *Protect Me-based* enrollments, not *manual* installs. The `.msi` installer only upgrades the onQ service component, while the `.ez` installer also enables enrollment.



Press the Continue button below to automatically configure protection for the node.
This will download an executable software package to your machine.
Please select "Run" at the browser prompt.

Waiting for Node Configuration Information.
Please wait... Timeout in 175 seconds.

7. From your browser, run the onQ Service installer (`onQEZInstaller.exe`) to launch the **Setup Wizard**.



C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet ...

```
do UnPack: ...C:\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary I
nternet Files\Content.IE5\P5LU72ZF\onQEZInstaller.exe
do UnPack: done: C:\Program Files\Quorum\installer\QuorumWinBCVSetup64-trunk-140
313-0825.msi
Scanning Interfaces . . .

Data Sent: http://10.20.17.198/sources/nodeconfiginfo.php
SystemRoot = C:\Windows
calling C:\Windows\System32\cmd.exe /c C:\Windows\System32\msiexec.exe /i "C:\Pr
ogram Files\Quorum\installer\QuorumWinBCVSetup64-trunk-140313-0825.msi"
installing ... C:\Program Files\Quorum\installer\QuorumWinBCVSetup64-trunk-14031
3-0825.msi
```

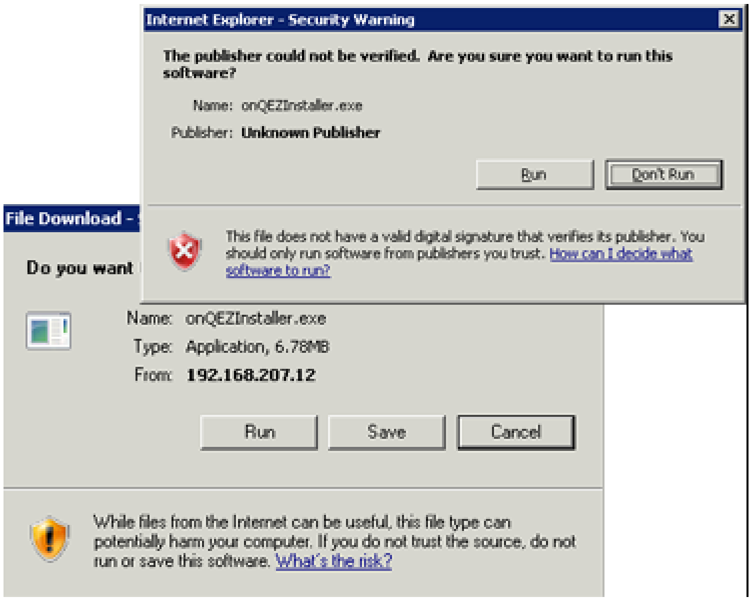
Quorum onQ

Welcome to the Quorum onQ Setup Wizard

The installer will guide you through the steps required to install Quorum onQ on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

When prompted by your browser, click **Run**, the **Run** again to confirm the `Unknown Publisher`. If you're using Firefox, you need to double-click on the executable before you can run the installer.



Internet Explorer - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: onQEZInstaller.exe

Publisher: Unknown Publisher

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

File Download -

Do you want

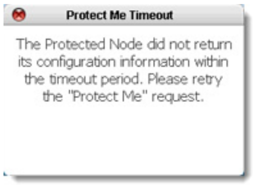
Name: onQEZInstaller.exe

Type: Application, 6.78MB

From: 192.168.207.12

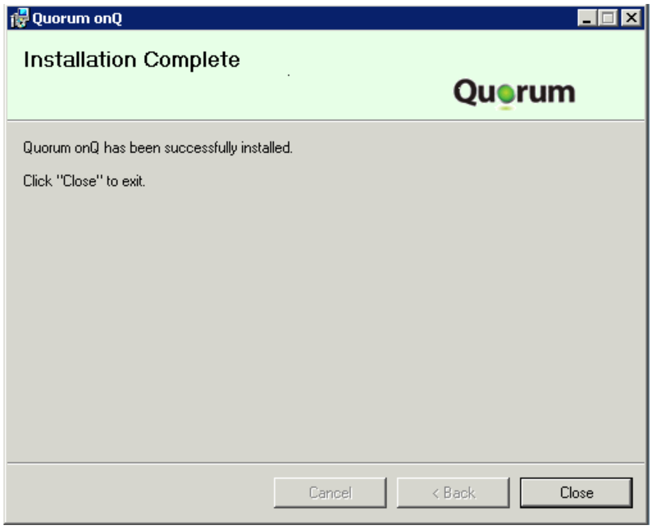
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Table 1: (Agent-based Windows Enrollment) Problems *Before* Enrollment

Dialog Message	Possible Cause	Solution
`The Protected Node did not return its configuration information within the timeout period. Please retry the "Protect Me" request`  Protect Me Timeout The Protected Node did not return its configuration information within the timeout period. Please retry the "Protect Me" request.	If you don't install the onQ Service within 180 seconds, onQ returns the following error.	In this case, simply close the window and repeat this procedure again.

8. Install the onQ Service by following the on-screen instructions in the **Setup Wizard**.

Congratulations, you've installed the onQ Service.



Quorum onQ has been successfully installed.

Click "Close" to exit.

9. Modify PN parameters.

   The **Modify Protection Parameters** dialog presents you with a summary of the PN's proposed configuration.

   Specify values for the node parameters, then click **SAVE** to add the node to the list of protected nodes.

   Optionally, you can click **SAVE** without modifications. You can modify the node at any time.

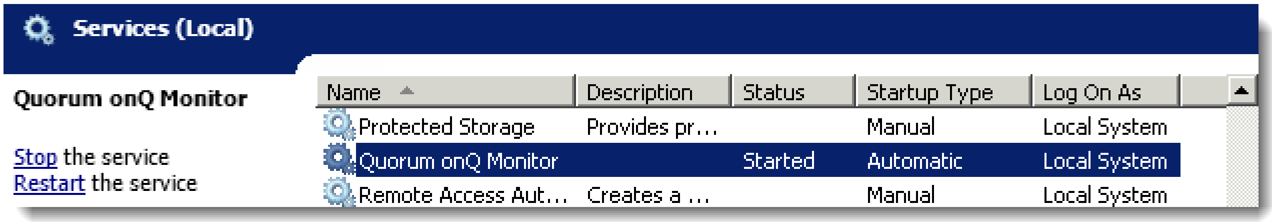
   If the installer fails at this point because there isn't enough disk space, refer to (Agent-based PNs) Add protected nodes manually; otherwise, the PN appears in the list.

10. On the protected node, open the following ports in order for onQ to see the protected node.
    - UDP port `5990`
    - TCP ports `5000` and `5990`

11. Verify enrollment. If the PN is not enrolled, see (Agent-based Enrollment) Protected Node Enrollment Problems.

    a. Verify that the PN appears in the list of protected nodes.

b. Verify that the onQ Service is running on the PN:



Services (Local)

Quorum onQ Monitor

Stop the service
Restart the service

Name	Description	Status	Startup Type	Log On As
Protected Storage	Provides pr…		Manual	Local System
Quorum onQ Monitor		Started	Automatic	Local System
Remote Access Aut…	Creates a …		Manual	Local System

(Alternative) To *manually* install or reinstall agent-based Windows PN software:

Use this procedure to:

- Manually install an agent-based Windows PN for the first time. Normally, there’s no need to perform this procedure in this case because the Protect Me-based enrollment, as outlined in (Recommended) To enroll an agent-based Windows PN:, simplifies the installation process for you by retrieving the appropriate package from the onQ Portal’s **Downloads** tab. However, you might need to perform a manual enrollment (install) if the initial Protect Me-based enrollment of the PN failed. Sometimes this happens. For example, old versions of Firefox cannot automatically select the correct operating system version (32-bit or 64-bit) for your PN.
- Reinstall (aka manually upgrade) node software on a PN that is already on onQ’s protection list so as to fix a PN upgrade or connectivity failure. As outlined in (Agent-based Windows PNs) Update node software, the automatic upgrade process keeps your PNs up to date. However, sometimes upgrade failures occur, requiring that you reinstall the node software. For example, a PN can go offline and miss an auto-update.

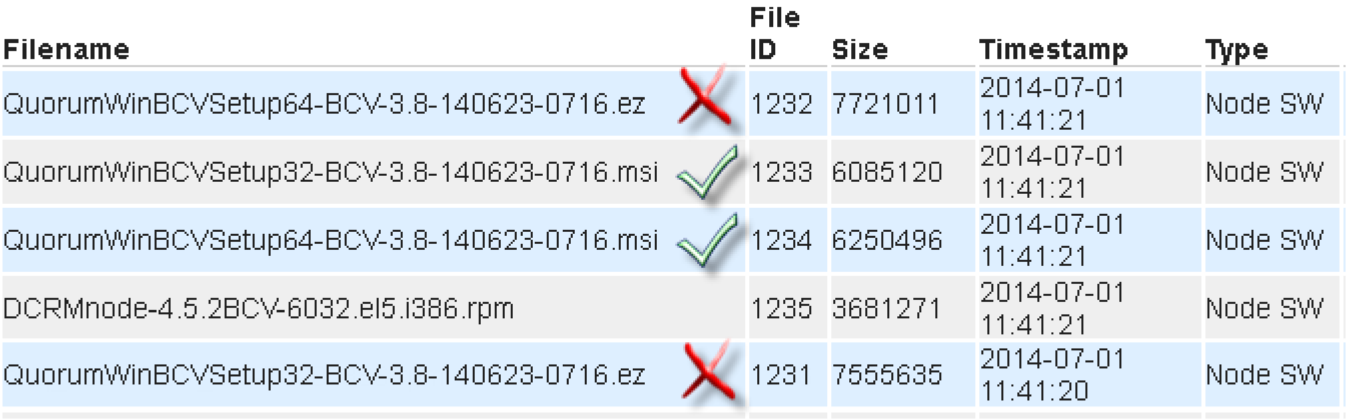
> **Note:** There are cases where a **Protect Me** > **Setup Wizard** > **Repair** | **Remove** methods can resolve most PN upgrade problems, but uninstalling from the Windows Control panel and manually installing as outlined below corrects all issues.

1. **(Existing PNs Only)** If this is a previously enrolled PN, uninstall the existing node software on the PN: From the Windows Control panel, select the Quorum onQ Monitor service, then **Uninstall**.
2. RDP to the server that you want to protect, then log on to that server as a user with administrative privileges.

3. From that server, launch a browser (see Browser Support), then log on to the HA's onQ Portal as `varadmin`.
4. Download the onQ Service installer.
   a. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **DOWNLOADS** page.

Warning: Do not download the `.ez` file, which is only intended for Protect Me-based enrollments as outlined in (Agent-based Windows PNs) Enroll protected nodes, not manual installs. The `.msi` installer only upgrades the onQ service component, while the `.ez` installer also enables enrollment.

   b. Scroll down and select the `QuorumWinBCVSetup<bitVersion>-BCV<build>.msi` file that matches your server's operating system.



Filename		File ID	Size	Timestamp	Type
QuorumWinBCVSetup64-BCV-3.8-140623-0716.ez	✗	1232	7721011	2014-07-01 11:41:21	Node SW
QuorumWinBCVSetup32-BCV-3.8-140623-0716.msi	✓	1233	6085120	2014-07-01 11:41:21	Node SW
QuorumWinBCVSetup64-BCV-3.8-140623-0716.msi	✓	1234	6250496	2014-07-01 11:41:21	Node SW
DCRMnode-4.5.2BCV-6032.el5.i386.rpm		1235	3681271	2014-07-01 11:41:21	Node SW
QuorumWinBCVSetup32-BCV-3.8-140623-0716.ez	✗	1231	7555635	2014-07-01 11:41:20	Node SW

   c. Click the **DOWNLOAD** button, saving the file to your `Downloads` folder.
   d. Open the `Downloads` folder. Execute the newly downloaded msi installer.
5. Follow the wizard's instructions to install the onQ Service on the PN.

Related Topics

(Agent-based PNs) Add protected nodes manually

(Agent-based PNs) Verify PN software compatibility

5.2 (Agent-based Linux PNs) Enroll protected nodes

onQ supports both agent-based and agent-less PNs. Nodes that are not hosted by VMware require that an agent (onQ Service) be installed. Agent-based enrollment enables you to use all of the operation and monitoring features that onQ has to offer.

Linux PN preparation is very important for RN builds to succeed. In some cases, different RHEL release distributions require unique tasks:

- **install xen-aware kernel package**. Unlike with RHEL 5.x, RHEL 7 and RHEL 6.x have a xen-aware kernel built-in; therefore, there's no need to install xen-aware kernel package on theses versions.
- **install agent software**. This task is required for all supported versions.
- **enforce grub boot menu**. This task is required for all supported versions in order to boot the RN successfully, though the specific steps might vary for each version.

(RHEL 7.0) To enroll an agent-based Linux PN:

Use this procedure to enroll an agent-based Linux PN running RHEL 7.0.

1. (Important!) If any of your PNs were previously enrolled, search for and delete all orphan data for those PNs on both the HA and the DR.

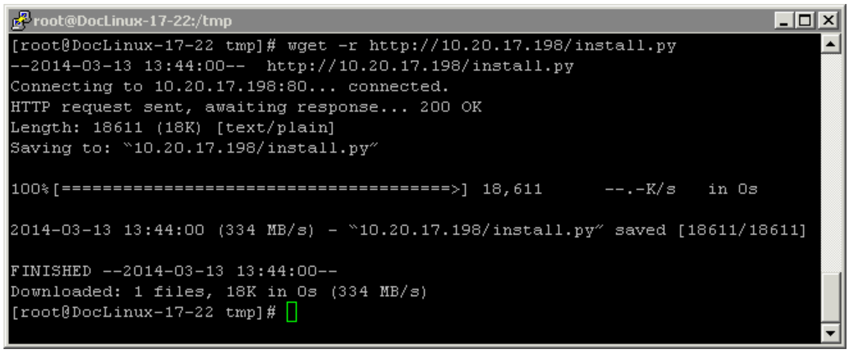
   If you remove orphan data for a given PN from the HA—but not from the DR, then later re-enroll that same PN on the same HA, the DR fails to add the future snapshots for this PN thereby compromising disaster recovery.
2. Log on to the HA's onQ Portal as varadmin.
3. SSH to the to the server that you want to enroll as a PN, then log on as `root`.
4. Install the agent software:

a. Launch the installer:

> **Note:** By default, wget preserves the original files. Newly retrieved install.py is saved with extensions `.1`, `.2`, etc. Use the `-r` option (see wget man page) to overwrite the existing file.

b. From within a folder (`/tmp`) where you want to save the install script, run the following command:

```
# wget -r http://<onQ-IP-address>/install.py
```

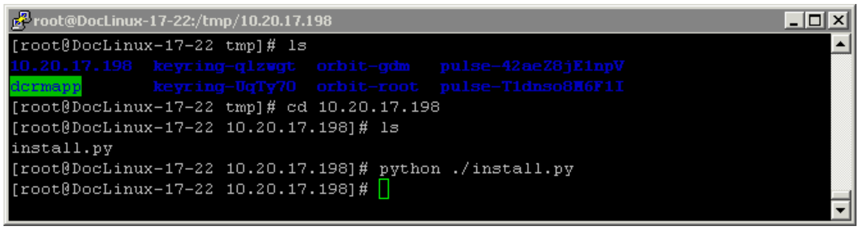


root@DocLinux-17-22:/tmp

```
[root@DocLinux-17-22 tmp]# wget -r http://10.20.17.198/install.py
--2014-03-13 13:44:00--  http://10.20.17.198/install.py
Connecting to 10.20.17.198:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18611 (18K) [text/plain]
Saving to: `10.20.17.198/install.py'

100%[======================================>] 18,611      --.-K/s   in 0s

2014-03-13 13:44:00 (334 MB/s) - `10.20.17.198/install.py' saved [18611/18611]

FINISHED --2014-03-13 13:44:00--
Downloaded: 1 files, 18K in 0s (334 MB/s)
[root@DocLinux-17-22 tmp]#
```

c. Start the installer:

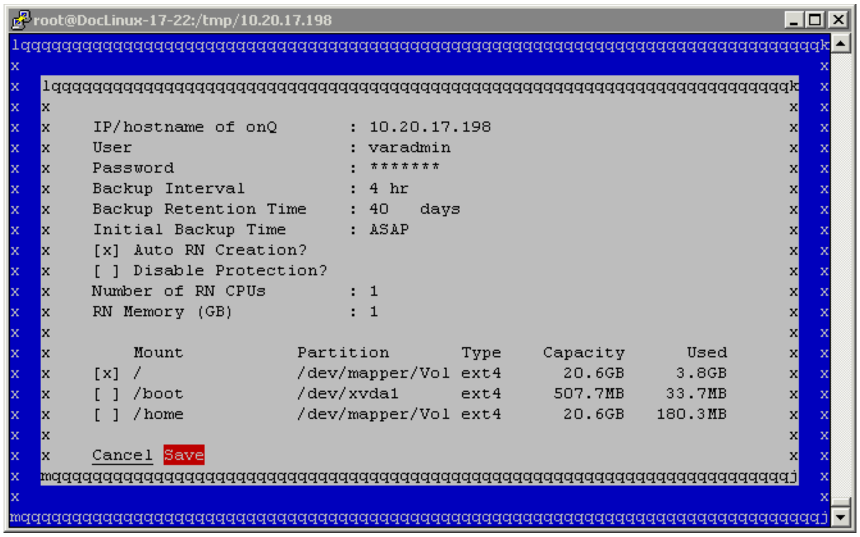
```
# cd <onQ-IP-address>
# python ./install.py
```



root@DocLinux-17-22:/tmp/10.20.17.198

```
[root@DocLinux-17-22 tmp]# ls
10.20.17.198  keyring-qlzwgt  orbit-gdm   pulse-42aeZ8jE1npV
dcrmapp       keyring-UqTy70  orbit-root  pulse-T1dnso8M6F1I
[root@DocLinux-17-22 tmp]# cd 10.20.17.198
[root@DocLinux-17-22 10.20.17.198]# ls
install.py
[root@DocLinux-17-22 10.20.17.198]# python ./install.py
[root@DocLinux-17-22 10.20.17.198]#
```

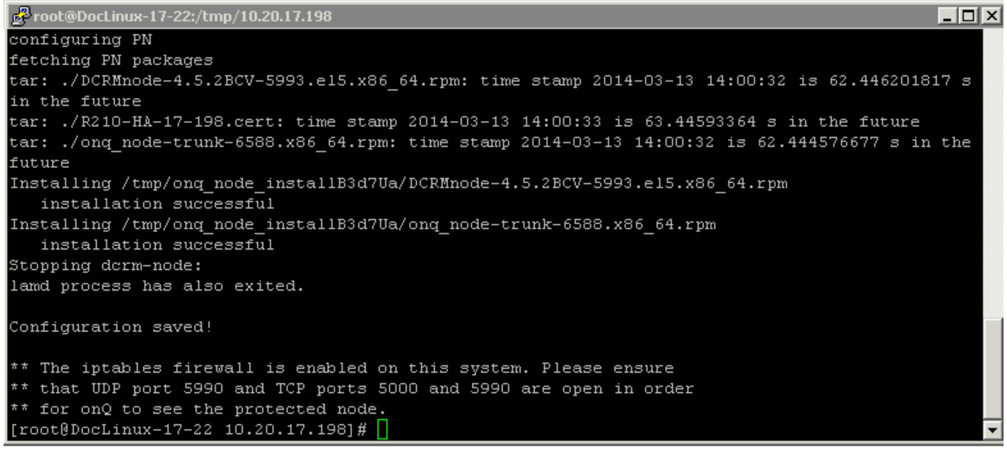
d. Type the credentials for either onQ varadmin or admin user.



```
    IP/hostname of onQ        : 10.20.17.198
    User                      : varadmin
    Password                  : *******
    Backup Interval           : 4 hr
    Backup Retention Time     : 40   days
    Initial Backup Time       : ASAP
    [x] Auto RN Creation?
    [ ] Disable Protection?
    Number of RN CPUs         : 1
    RN Memory (GB)            : 1

        Mount             Partition       Type     Capacity       Used
    [x] /                 /dev/mapper/Vol ext4       20.6GB      3.8GB
    [ ] /boot             /dev/xvda1      ext4      507.7MB     33.7MB
    [ ] /home             /dev/mapper/Vol ext4       20.6GB    180.3MB

    Cancel Save
```

e. (Optional) Specify all valid values, excluding file system type and capacity because these values aren't editable, in the node parameter fields provided and modify defaults as needed. (The install utility lists all available volumes/partitions/mount points and the onQ portal enforces any file system requirements as outlined in Linux Filesystem Format Requirements.) You can make these node changes at any point after enrollment via the **Protection Config** tab in the onQ Portal.

f. Select **Save** to update/install the client node package on the Linux node.



```
configuring PN
fetching PN packages
tar: ./DCRMnode-4.5.2BCV-5993.el5.x86_64.rpm: time stamp 2014-03-13 14:00:32 is 62.446201817 s
in the future
tar: ./R210-HA-17-198.cert: time stamp 2014-03-13 14:00:33 is 63.44593364 s in the future
tar: ./onq_node-trunk-6588.x86_64.rpm: time stamp 2014-03-13 14:00:32 is 62.444576677 s in the
future
Installing /tmp/onq_node_installB3d7Ua/DCRMnode-4.5.2BCV-5993.el5.x86_64.rpm
   installation successful
Installing /tmp/onq_node_installB3d7Ua/onq_node-trunk-6588.x86_64.rpm
   installation successful
Stopping dcrm-node:
lamd process has also exited.

Configuration saved!

** The iptables firewall is enabled on this system. Please ensure
** that UDP port 5990 and TCP ports 5000 and 5990 are open in order
** for onQ to see the protected node.
[root@DocLinux-17-22 10.20.17.198]# 
```

g. Wait! Do not press Enter. Was the installation successful? Use the error messages below to evaluate the screen output.

- If yes, exit the script.
- If no, press `Enter` to launch the installer UI again. Correct the problem, then repeat Step e through Step g.

Table 2: (Agent-based Linux PNs) Problems *Before* Enrollment

`Completed Successfully`
`The iptables firewall is enabled on this system....`
	Message appears in the shell, after the GUI curser exits. In addition, you'll be instructed to open up ports.

`Incorrect/invalid values entered`	Install utility stops if you type incorrect/invalid values. Correct the problem and **Save** again or **Cancel**.
`not authorized`	You either typed the credentials incorrectly or the user account does not have root privileges.

5. **Install the Netcat (`nc`) utility**, if not already installed. On your yum-enabled PN, run the following command, then verify that the package was installed. This utility reads and writes data across network connections using TCP or UDP. onQ depends on this utility for FLR restores.

```
# yum install nc
# which nc
nc is /usr/bin/nc
# rpm -qf /usr/bin/nc
nmap-ncat-6.40-4.el7.x86_64
```

6. **Create the grub boot menu**. In order to boot the RN successfully, the PN needs to prepare the init ram disk image with the required drivers and legacy grub boot menu.

   a. Verify OS version:

```
# cat /etc/redhat-release

Red Hat Enterprise Linux Server release 7.0
(Maipo)
```

b. Make sure `ext2`/`ext3`/`ext4` file systems utilities are installed.

```
# rpm -qa | grep e2fsprogs
e2fsprogs-libs-1.42.9-4.el7.x86_64
e2fsprogs-1.42.9-4.el7.x86_64
```

If not installed, do so now:

```
# yum install e2fsprogs
```

c. Generate the init ram disk with xen drivers and `ext4` file system modules.

Print the kernel release:

```
# uname -r
3.10.0-123.13.2.el7.x86_64
```

Where the `3.10.0-123.13.2.el7.x86_64` is the kernel release by default, change it to match PN's kernel release:

```
# cd /boot
# mkdir -p /boot/grub
# dracut --force --filesystems "ext4 ext3"  \
--add-drivers  "xen:vbd xen:vif" \
initramfs-3.10.0-123.13.2.el7xen.x86_64.img
```

d. Verify the legacy grub boot loader:

```
# vi /boot/grub/grub.conf.xvf5
```

Where the `3.10.0-123.13.2.el7.x86_64` is the kernel release by default, change `vmlinuz` and `initramfs` to match PN's kernel release. The kernel parameters are on a single line. Simply copy and paste from following screen.

Where the `root=UUID=855cd484-3852-4984-b568-ee0408c6b590`, the `855cd`... (UUID) is a temporary placeholder and will be replaced by read “`/`”'s UUID during the RN build. Do not make any changes to this parameter.

For example: The contents of `/boot/grub/grub.conf.xvf5`:

```
default=0
timeout=5
title onQ Red Hat Enterprise Linux (3.10.0-123.13.2.el7.x86_64)
root (hd0,0)
kernel /vmlinuz-3.10.0-123.13.2.el7.x86_64 ro root=UUID=855cd484-3852-
4984-b568-ee0408c6b590 plymouth.enable=0 console=hvc0 loglvl=all
cgroup_disable=memory sync_console console_to_ring earlyprintk=xen
nomodeset net.ifnames=0 biosdevname=0 LANG=en_US.UTF-8
initrd /initramfs-3.10.0-123.13.2el7xen.x86_64.img
```

From `/boot`, validate that `vmlinuz-3.10.0-123.13.2.el7.x86_64` and `initramfs-3.10.0-123.13.2.el7xen.x86_64.img` exist in `/boot` folder as shown in the example below:

```
# ls /boot/vmlinuz-3.10.0-123.13.2.el7.x86_64
/boot/vmlinuz-3.10.0-123.13.2.el7.x86_64
# ls /boot/initramfs-3.10.0-123.13.2.el7xen.x86_64.img
/boot/initramfs-3.10.0-123.13.2.el7xen.x86_64.img
```

7.

8. **(Recommended) Disable the Network Manager service**, if installed, for self-tests to work correctly. This service is not useful in a server environment. Due to an RHEL 7.0 bug, turning off Network Manager can prevent NICs from showing up; if this occurs, re-enable the Network Manager service.

```
# systemctl disable NetworkManager.service
# systemctl stop NetworkManager.service
# systemctl status NetworkManager.service
```

9. **Wait for the RN to build, then perform a self-test**.

   Troubleshooting RN Build or Self-test Problems

   Mistakes with the grub boot menu enforcement can prevent the RN from booting. The following list represents the most common errors.

   - Kernel parameters are not on one single line. Some file editors wrap long parameters.

- You have a typo in `grub.con` or `grub.conf.xvf5` file name.
- You have a typo in the kernel file name or the initramfs file name, or these files don’t exist.
- There is a mismatch, on the boot menu, between the kernel versions and the initramfs version. If the kernel's version does not match the contents of initramfs, the RN won't boot.The system could have more than one kernel installed:

  7.0:

  `vmlinuz-3.10.0-123.13.2.el7.x86_64`

  should match

  `initramfs-3.10.0-123.13.2.el7xen.x86_64.img`

  6.x:

  `vmlinuz-2.6.32-279.el6.x86_64`

  should match

  `initramfs-2.6.32-279.el6.x86_64.img`

  5.x:

  `vmlinuz-2.6.18-371.el5xen`

  should match

  `initrd-2.6.18-371.el5xen.img.5`

  To find the driver versions packed inside the init ram file system (`initramfs`) of the boot menu: Locate the initramfs and kernel name from the boot menu prepared for the RN (you’ll find it under `/boot)`, then use the following command to peek the contents of initramfs. For example:

RHEL 6.x or 7.0:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-3.10.0-123.el7.x86_64  ro
root=UUID=9002ec24-fb30-4d16-8a78-b352a807e82b
plymouth.enable=0 console=hvc0 loglvl=all
cgroup_disable=memory sync_console
console_to_ring earlyprintk=xen nomodeset net.if-
names=0 biosdevname=0 LANG=en_US.UTF-8
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initramfs-3.10.0-123.el7xen.x86_64.img
# lsinitrd /boot/initramsfs-3.10.0-
123.el7xen.x86_64.img|grep modules
rw-r--r--   1 root     root         1446 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep
-rw-r--r--   1 root     root         2450 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep.bin
-rw-r--r--   1 root     root           52 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.devname
-rw-r--r--   1 root     root        82512 Jun 30
2014 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.order
-rw-r--r--   1 root     root          165 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.softdep
-rw-r--r--   1 root     root        28132 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols
-rw-r--r--   1 root     root        34833 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols.bin
```

RHEL 5.x:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-2.6.18-371.el5xen ro
root=/dev/xvda1 rd_NO_LUKS rd_NO_MD rhgb crashker-
nel=auto rd_NO_LVM
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initrd-2.6.18-371.el5xen.img.5
# zcat /tmp/initrd-2.6.18-371.el5xen.img.5|cpio
-t|grep -E "xen|ext"
16524 blocks
lib/ext3.ko
lib/xennet.ko
lib/xenblk.ko
```

10. **Log on to the PN and open the** following ports on the firewall in order for onQ to communicate with the PN.
    - UDP port `5990`
    - TCP ports `5000` and `5990`

Firewalld:

By default, RHEL 7.0 has introduced a new firewall service, a dynamic firewall daemon known as `firewalld`, instead of iptables service by default; however, the traditional iptables service is supported if installed. For details, see the Red Hat Linux 7 Security Guide. If you choose to disable firewalld, there is no need to configure firewalld firewall rules: simply skip this procedure.

`firewalld` daemon and service and iptables service are using iptables commands to configure the netfilter in the kernel to separate and filter the network traffic. `firewalld` stores it in various XML files in `/usr/lib/firewalld/` and `/etc/firewalld/`.

The firewalld firewall defines how *networks zones* can be used to separate networks into different zones. Based on the level of trust, you can decide to place devices and traffic within a particular network zone. Each mutable network zone can have a different combination of firewall rules.

a. Verify that firewalld is in a running state.

b. Check the service status:

```
[root@RHEL70x64-17-167 services]# systemctl status
firewalld.service
firewalld.service - firewalld - dynamic firewall
daemon
Loaded: loaded (/usr/lib/systemd/system/fire-
walld.service; disabled)
Active: inactive (dead)
```

c. Enable the service, if not already enabled:

```
[root@RHEL70x64-17-167 services]# systemctl enable
firewalld
ln -s '/usr/lib/systemd/system/firewalld.service'
'/etc/systemd/system/dbusorg.edorapro-
ject.FirewallD1.service'
ln -s '/usr/lib/systemd/system/firewalld.service'
'/etc/systemd/system
/basic.target.wants/firewalld.service'
```

d. Start the service, if not already running:

```
[root@RHEL70x64-17-167 services]# systemctl start
firewalld
```

e. On the PN, find the network interface that is used to communicate with onQ. In this example, that NIC is `ens32`.

```
[root@RHEL70x64-17-167 services]# ifconfig
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>
mtu 1500
inet 10.20.17.167 netmask 255.255.248.0 broadcast
10.20.23.255
inet6 fe80::250:56ff:fe9d:2121 prefixlen 64 sco-
peid 0x20<link>
ether 00:50:56:9d:21:21 txqueuelen 1000 (Ethernet)
RX packets 7115713 bytes 476287831 (454.2 MiB)
RX errors 0 dropped 149791 overruns 0 frame 0
TX packets 924966 bytes 1305413839 (1.2 GiB)
TX errors 0 dropped 0 overruns 0 carrier 0 colli-
sions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 10 bytes 980 (980.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10 bytes 980 (980.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 colli-
sions 0
```

f. For the network interface that you identified above, find the network interface's network zone. In this example, the network zone is `work`.

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-
zone-of-interface=ens32
work
```

Determine your default zone. In the following example, the default zone is `Public`.

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-default-zone
public
```

g. Associate the zone(s) with the following firewall rules. The same rules can be applied to many zones as needed. In the following example, dcrm-node service is associated with `work` zone for `ens32`. The `dcrm-node.xml` is located at `/usr/lib/firewalld/services`.

```
[root@RHEL70x64-17-167 services]# firewall-cmd --add-service=dcrm-node --permanent --zone=work
success
```

h. Activate the latest firewall rules:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --reload
success
```

Now the PN can communicate with onQ.

i. Set up the rule for RN on the PN site.

The RN will be equipped with `eth0` interface, so apply the rules to `eth0` interface's zone if different from PN's zone. The PN might not have `eth0` interface; in such a case, the RN's `eth0` will be in the default zone.

Find `eth0` network interface's network zone. In this example, it is *not* set:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-zone-of-interface=eth0
no zone
```

Determine your default zone. In this example default zone is `Public`. Since `eth0` has no zone dcm-node is associated with `Public` zone:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-default-zone
public
```

j. Associate the zone(s) with the following firewall rules. The same rules can be applied to many zones as needed:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --add-service=dcrm-node --permanent --zone=public
success
```

k. Active the latest firewall rules:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --reload
success
```

Now the RN can communicate with onQ, mainly for self-tests.

l. Confirm the firewall rules. The public zone and work zone have TCP ports (5000/5990) and UDP port 5990 opened in this case.

```
[root@RHEL70x64-17-167 services]# iptables -L -n
Chain IN_public (2 references)
target prot opt source destination
IN_public_log all -- 0.0.0.0/0 0.0.0.0/0
IN_public_deny all -- 0.0.0.0/0 0.0.0.0/0
IN_public_allow all -- 0.0.0.0/0 0.0.0.0/0
Chain IN_public_allow (1 references)
target prot opt source destination
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5000 ct-
state NEW
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 ct-
state NEW
Chain IN_work (0 references)
target prot opt source destination
IN_work_log all -- 0.0.0.0/0 0.0.0.0/0
IN_work_deny all -- 0.0.0.0/0 0.0.0.0/0
IN_work_allow all -- 0.0.0.0/0 0.0.0.0/0
Chain IN_work_allow (1 references)
target prot opt source destination
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:631 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5000 ct-
state NEW
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 ct-
state NEW
```

iptables:

a. Verify that udp 5990 and tcp 5000 and 5990 ports are open and above the `REJECT` line:

```
# iptables -L -n | grep -E "5900|5000"
ACCEPT   udp -- 0.0.0.0/0       0.0.0.0/0
udp dpt:5990
ACCEPT   tcp -- 0.0.0.0/0       0.0.0.0/0
state NEW tcp dpt:5000
ACCEPT   tcp -- 0.0.0.0/0       0.0.0.0/0
state NEW tcp dpt:5990
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with
icmp-host-prohibited
```

b. If these ports are not open, open them.

Find the input chain name, which is reported in the line that appears after `INPUT`:

```
# iptables -L -line numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 RH-Firewall-1-INPUT all -- anywhere anywhere
...
10 REJECT all -- anywhere anywhere reject-with
icmp-host-prohibited
```

Using the line number of the `REJECT` line and the chain name (line `10` and line `1`, respectively, in the step above), insert the onQ ports:

```
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5990 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5000 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -p udp --
dport 5990 -j ACCEPT
```

c. Save and restart iptables.

Afterward, verify that the ports are open and above the `REJECT` line as outlined earlier.

```
# service iptables save
Saving firewall rules to /etc/sysconfig/iptables:
[ OK ]
# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules:
ip_conntrack_netbios_n [ OK ]
```

11. **(Oracle database) Install `RMAN` scripts**.

    If the PN has an Oracle database, install the `RMAN` scripts so that onQ can execute a hot backup of your database as outlined in Back up and restore Oracle 11g database on Linux.

(RHEL 6.x) To enroll an agent-based Linux PN:

Use this procedure to enroll an agent-based Linux PN running RHEL 6.x.

1. (Important!) If any of your PNs were previously enrolled, search for and delete all orphan data for those PNs on both the HA and the DR.

   If you remove orphan data for a given PN from the HA—but not from the DR, then later re-enroll that same PN on the same HA, the DR fails to add the future snapshots for this PN thereby compromising disaster recovery.

2. Log on to the HA’s onQ Portal as varadmin.
3. SSH to the to the server that you want to enroll as a PN, then log on as `root`.

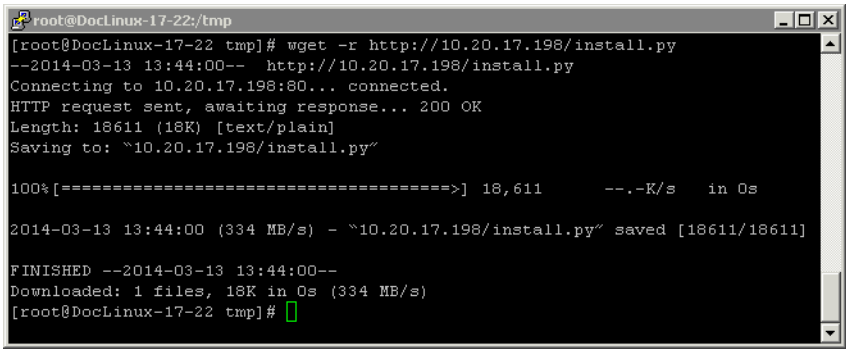
4. Install the agent software:

a. Launch the installer:

> **Note:** By default, wget preserves the original files. Newly retrieved install.py is saved with extensions `.1`, `.2`, etc. Use the `-r` option (see wget man page) to overwrite the existing file.

b. From within a folder (`/tmp`) where you want to save the install script, run the following command:

```
# wget -r http://<onQ-IP-address>/install.py
```

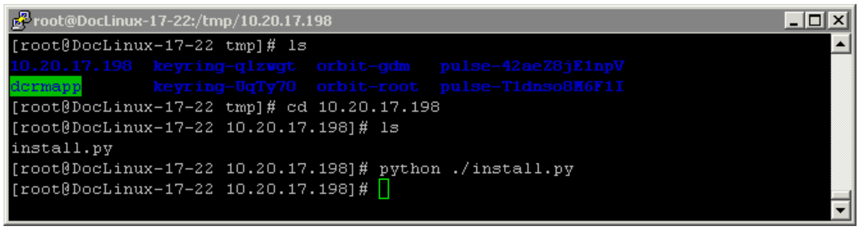


root@DocLinux-17-22:/tmp

```
[root@DocLinux-17-22 tmp]# wget -r http://10.20.17.198/install.py
--2014-03-13 13:44:00--  http://10.20.17.198/install.py
Connecting to 10.20.17.198:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18611 (18K) [text/plain]
Saving to: `10.20.17.198/install.py'

100%[======================================>] 18,611      --.-K/s   in 0s

2014-03-13 13:44:00 (334 MB/s) - `10.20.17.198/install.py' saved [18611/18611]

FINISHED --2014-03-13 13:44:00--
Downloaded: 1 files, 18K in 0s (334 MB/s)
[root@DocLinux-17-22 tmp]# 
```

c. Start the installer:

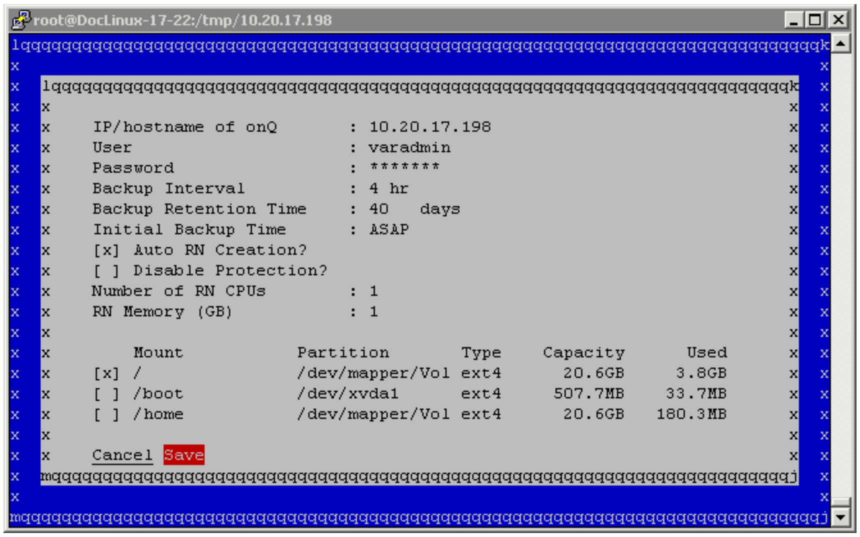
```
# cd <onQ-IP-address>
# python ./install.py
```



root@DocLinux-17-22:/tmp/10.20.17.198

```
[root@DocLinux-17-22 tmp]# ls
10.20.17.198  keyring-qlzwgt  orbit-gdm   pulse-42aeZ8jE1npV
dcrmapp       keyring-UqTy70  orbit-root  pulse-T1dnso8M6F1I
[root@DocLinux-17-22 tmp]# cd 10.20.17.198
[root@DocLinux-17-22 10.20.17.198]# ls
install.py
[root@DocLinux-17-22 10.20.17.198]# python ./install.py
[root@DocLinux-17-22 10.20.17.198]# 
```

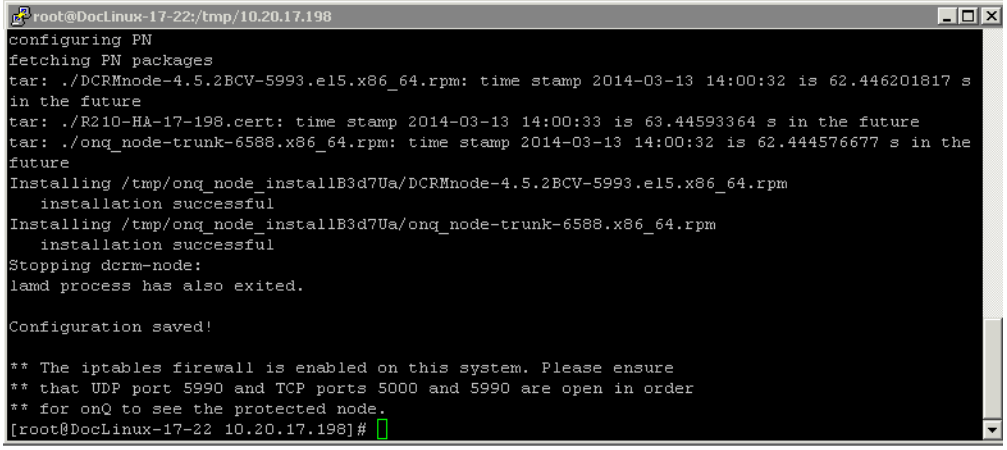
d. Type the credentials for either onQ varadmin or admin user.



```
    IP/hostname of onQ         : 10.20.17.198
    User                       : varadmin
    Password                   : *******
    Backup Interval            : 4 hr
    Backup Retention Time      : 40   days
    Initial Backup Time        : ASAP
    [x] Auto RN Creation?
    [ ] Disable Protection?
    Number of RN CPUs          : 1
    RN Memory (GB)             : 1

        Mount              Partition        Type      Capacity       Used
    [x] /                  /dev/mapper/Vol  ext4        20.6GB      3.8GB
    [ ] /boot              /dev/xvda1       ext4       507.7MB     33.7MB
    [ ] /home              /dev/mapper/Vol  ext4        20.6GB    180.3MB

    Cancel Save
```

e. (Optional) Specify all valid values, excluding file system type and capacity because these values aren't editable, in the node parameter fields provided and modify defaults as needed. (The install utility lists all available volumes/partitions/mount points and the onQ portal enforces any file system requirements as outlined in Linux Filesystem Format Requirements.) You can make these node changes at any point after enrollment via the **Protection Config** tab in the onQ Portal.

f. Select **Save** to update/install the client node package on the Linux node.



```
configuring PN
fetching PN packages
tar: ./DCRMnode-4.5.2BCV-5993.el5.x86_64.rpm: time stamp 2014-03-13 14:00:32 is 62.446201817 s
in the future
tar: ./R210-HA-17-198.cert: time stamp 2014-03-13 14:00:33 is 63.44593364 s in the future
tar: ./onq_node-trunk-6588.x86_64.rpm: time stamp 2014-03-13 14:00:32 is 62.444576677 s in the
future
Installing /tmp/onq_node_installB3d7Ua/DCRMnode-4.5.2BCV-5993.el5.x86_64.rpm
   installation successful
Installing /tmp/onq_node_installB3d7Ua/onq_node-trunk-6588.x86_64.rpm
   installation successful
Stopping dcrm-node:
lamd process has also exited.

Configuration saved!

** The iptables firewall is enabled on this system. Please ensure
** that UDP port 5990 and TCP ports 5000 and 5990 are open in order
** for onQ to see the protected node.
[root@DocLinux-17-22 10.20.17.198]#
```

g. Wait! Do not press Enter. Was the installation successful? Use the error messages below to evaluate the screen output.

- If yes, exit the script.
- If no, press `Enter` to launch the installer UI again. Correct the problem, then repeat Step e through Step g.

Table 3: (Agent-based Linux PNs) Problems *Before* Enrollment

`Completed Successfully`
`The iptables firewall is enabled on this system....`
	Message appears in the shell, after the GUI curser exits. In addition, you'll be instructed to open up ports.

`Incorrect/invalid values entered`	Install utility stops if you type incorrect/invalid values. Correct the problem and **Save** again or **Cancel**.
`not authorized`	You either typed the credentials incorrectly or the user account does not have root privileges.

5. **Install the Netcat (`nc`) utility**, if not already installed. On your yum-enabled PN, run the following command, then verify that the package was installed. This utility reads and writes data across network connections using TCP or UDP. onQ depends on this utility for FLR restores.

```
# yum install nc
# which nc
nc is /usr/bin/nc
# rpm -qf /usr/bin/nc
nc-1.84-22.el6.x86_64
```

6. **Wait for the RN to build, then perform a self-test.**

Troubleshooting RN Build or Self-test Problems

Mistakes with the grub boot menu enforcement can prevent the RN from booting. The following list represents the most common errors.

- Kernel parameters are not on one single line. Some file editors wrap long parameters.
- You have a typo in `grub.con` or `grub.conf.xvf5` file name.
- You have a typo in the kernel file name or the initramfs file name, or these files don't exist.

- There is a mismatch, on the boot menu, between the kernel versions and the initramfs version. If the kernel's version does not match the contents of initramfs, the RN won't boot.The system could have more than one kernel installed:

  7.0:

  ```
  vmlinuz-3.10.0-123.13.2.el7.x86_64
  ```

  should match

  ```
  initramfs-3.10.0-123.13.2.el7xen.x86_64.img
  ```

  6.x:

  ```
  vmlinuz-2.6.32-279.el6.x86_64
  ```

  should match

  ```
  initramfs-2.6.32-279.el6.x86_64.img
  ```

  5.x:

  ```
  vmlinuz-2.6.18-371.el5xen
  ```

  should match

  ```
  initrd-2.6.18-371.el5xen.img.5
  ```

  To find the driver versions packed inside the init ram file system (`initramfs`) of the boot menu: Locate the initramfs and kernel name from the boot menu prepared for the RN (you'll find it under `/boot)`, then use the following command to peek the contents of initramfs. For example:

RHEL 6.x or 7.0:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-3.10.0-123.el7.x86_64  ro
root=UUID=9002ec24-fb30-4d16-8a78-b352a807e82b
plymouth.enable=0 console=hvc0 loglvl=all
cgroup_disable=memory sync_console
console_to_ring earlyprintk=xen nomodeset net.if-
names=0 biosdevname=0 LANG=en_US.UTF-8
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initramfs-3.10.0-123.el7xen.x86_64.img
# lsinitrd /boot/initramfs-3.10.0-
123.el7xen.x86_64.img|grep modules
rw-r--r--   1 root     root         1446 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep
-rw-r--r--   1 root     root         2450 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep.bin
-rw-r--r--   1 root     root           52 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.devname
-rw-r--r--   1 root     root        82512 Jun 30
2014 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.order
-rw-r--r--   1 root     root          165 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.softdep
-rw-r--r--   1 root     root        28132 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols
-rw-r--r--   1 root     root        34833 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols.bin
```

RHEL 5.x:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-2.6.18-371.el5xen ro
root=/dev/xvda1 rd_NO_LUKS rd_NO_MD rhgb crashker-
nel=auto rd_NO_LVM
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initrd-2.6.18-371.el5xen.img.5
# zcat /tmp/initrd-2.6.18-371.el5xen.img.5|cpio
-t|grep -E "xen|ext"
16524 blocks
lib/ext3.ko
lib/xennet.ko
lib/xenblk.ko
```

7.

8. **(Recommended) Disable the Network Manager service**, if installed, for self-tests to work correctly. This service is not useful in a server environment.

```
# service NetworkManager stop
# service NetworkManager status
# chkconfig NetworkManager off
# chkconfig --list NetworkManager
NetworkManager  0:off   1:off   2:off   3:off
4:off   5:off   6:off
```

9. **Log on to the PN and open the** following ports on the firewall in order for onQ to communicate with the PN.
   - UDP port `5990`
   - TCP ports `5000` and `5990`

10.

iptables:

a. Verify that udp 5990 and tcp 5000 and 5990 ports are open and above the `REJECT` line:

```
# iptables -L -n | grep -E "5900|5000"
ACCEPT   udp -- 0.0.0.0/0       0.0.0.0/0
udp dpt:5990
ACCEPT   tcp -- 0.0.0.0/0       0.0.0.0/0
state NEW tcp dpt:5000
ACCEPT   tcp -- 0.0.0.0/0       0.0.0.0/0
state NEW tcp dpt:5990
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with
icmp-host-prohibited
```

b. If these ports are not open, open them.

Find the input chain name, which is reported in the line that appears after `INPUT`:

```
# iptables -L -line numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 RH-Firewall-1-INPUT all -- anywhere anywhere
...
10 REJECT all -- anywhere anywhere reject-with
icmp-host-prohibited
```

Using the line number of the `REJECT` line and the chain name (line `10` and line `1`, respectively, in the step above), insert the onQ ports:

```
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5990 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5000 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -p udp --
dport 5990 -j ACCEPT
```

c. Save and restart iptables.

Afterward, verify that the ports are open and above the `REJECT` line as outlined earlier.

```
# service iptables save
Saving firewall rules to /etc/sysconfig/iptables:
[ OK ]
# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules:
ip_conntrack_netbios_n [ OK ]
```

11. **(Oracle database) Install `RMAN` scripts**.

    If the PN has an Oracle database, install the `RMAN` scripts so that onQ can execute a hot backup of your database as outlined in Back up and restore Oracle 11g database on Linux.

12.

(RHEL 5.x) To enroll an agent-based Linux PN:

Use this procedure to enroll an agent-based Linux PN running RHEL 5.x.

1. (Important!) If any of your PNs were previously enrolled, search for and delete all orphan data for those PNs on both the HA and the DR.

   If you remove orphan data for a given PN from the HA—but not from the DR, then later re-enroll that same PN on the same HA, the DR fails to add the future snapshots for this PN thereby compromising disaster recovery.

2. Log on to the HA's onQ Portal as varadmin.
3. SSH to the to the server that you want to enroll as a PN, then log on as `root`.

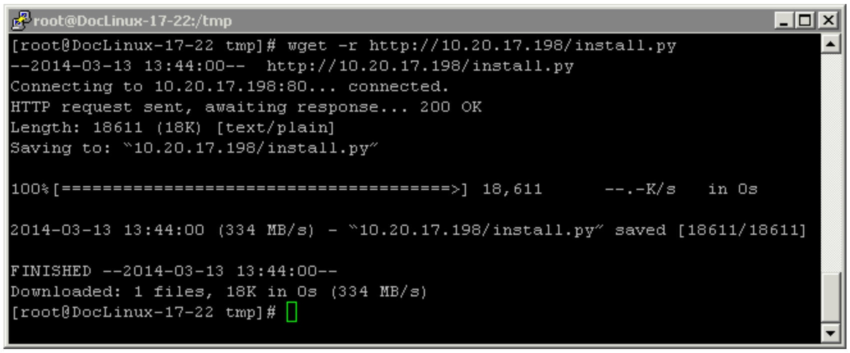
4. Install the agent software:

a. Launch the installer:

> **Note:** By default, wget preserves the original files. Newly retrieved install.py is saved with extensions `.1`, `.2`, etc. Use the `-r` option (see wget man page) to overwrite the existing file.

b. From within a folder (`/tmp`) where you want to save the install script, run the following command:

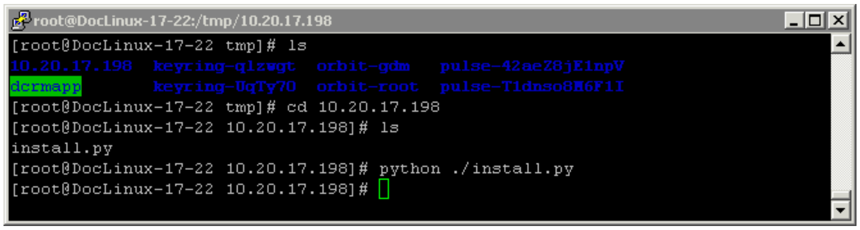
```
# wget -r http://<onQ-IP-address>/install.py
```



```
[root@DocLinux-17-22 tmp]# wget -r http://10.20.17.198/install.py
--2014-03-13 13:44:00--  http://10.20.17.198/install.py
Connecting to 10.20.17.198:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18611 (18K) [text/plain]
Saving to: `10.20.17.198/install.py'

100%[======================================>] 18,611      --.-K/s   in 0s

2014-03-13 13:44:00 (334 MB/s) - `10.20.17.198/install.py' saved [18611/18611]

FINISHED --2014-03-13 13:44:00--
Downloaded: 1 files, 18K in 0s (334 MB/s)
[root@DocLinux-17-22 tmp]# 
```

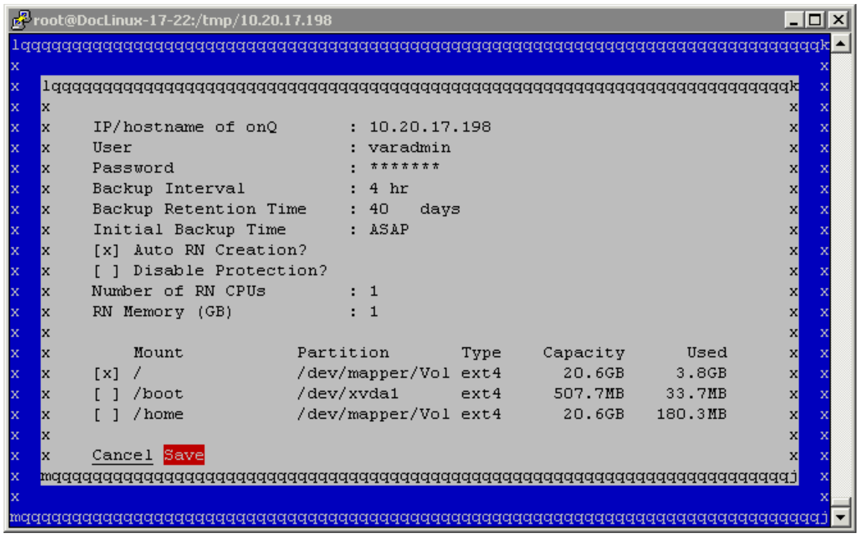
c. Start the installer:

```
# cd <onQ-IP-address>
# python ./install.py
```



```
[root@DocLinux-17-22 tmp]# ls
10.20.17.198  keyring-qlzwgt  orbit-gdm   pulse-42aeZ8jE1npV
dcrmapp       keyring-UqTy7O  orbit-root  pulse-T1dnso8M6F1I
[root@DocLinux-17-22 tmp]# cd 10.20.17.198
[root@DocLinux-17-22 10.20.17.198]# ls
install.py
[root@DocLinux-17-22 10.20.17.198]# python ./install.py
[root@DocLinux-17-22 10.20.17.198]# 
```

d. Type the credentials for either onQ varadmin or admin user.

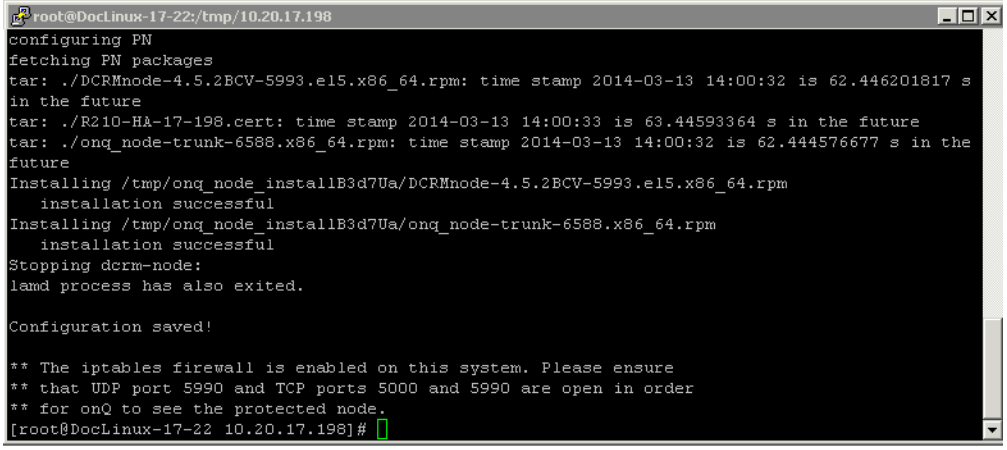


root@DocLinux-17-22:/tmp/10.20.17.198

```
IP/hostname of onQ        : 10.20.17.198
User                      : varadmin
Password                  : *******
Backup Interval           : 4 hr
Backup Retention Time     : 40   days
Initial Backup Time       : ASAP
[x] Auto RN Creation?
[ ] Disable Protection?
Number of RN CPUs         : 1
RN Memory (GB)            : 1

    Mount               Partition        Type      Capacity       Used
[x] /                   /dev/mapper/Vol  ext4        20.6GB      3.8GB
[ ] /boot               /dev/xvda1       ext4       507.7MB     33.7MB
[ ] /home               /dev/mapper/Vol  ext4        20.6GB    180.3MB

Cancel Save
```

e. (Optional) Specify all valid values, excluding file system type and capacity because these values aren’t editable, in the node parameter fields provided and modify defaults as needed. (The install utility lists all available volumes/partitions/mount points and the onQ portal enforces any file system requirements as outlined in Linux Filesystem Format Requirements.) You can make these node changes at any point after enrollment via the **Protection Config** tab in the onQ Portal.

f. Select **Save** to update/install the client node package on the Linux node.



root@DocLinux-17-22:/tmp/10.20.17.198

```
configuring PN
fetching PN packages
tar: ./DCRMnode-4.5.2BCV-5993.el5.x86_64.rpm: time stamp 2014-03-13 14:00:32 is 62.446201817 s
in the future
tar: ./R210-HA-17-198.cert: time stamp 2014-03-13 14:00:33 is 63.44593364 s in the future
tar: ./onq_node-trunk-6588.x86_64.rpm: time stamp 2014-03-13 14:00:32 is 62.444576677 s in the
future
Installing /tmp/onq_node_installB3d7Ua/DCRMnode-4.5.2BCV-5993.el5.x86_64.rpm
   installation successful
Installing /tmp/onq_node_installB3d7Ua/onq_node-trunk-6588.x86_64.rpm
   installation successful
Stopping dcrm-node:
lamd process has also exited.

Configuration saved!

** The iptables firewall is enabled on this system. Please ensure
** that UDP port 5990 and TCP ports 5000 and 5990 are open in order
** for onQ to see the protected node.
[root@DocLinux-17-22 10.20.17.198]#
```

g. Wait! Do not press Enter. Was the installation successful? Use the error messages below to evaluate the screen output.

- If yes, exit the script.
- If no, press `Enter` to launch the installer UI again. Correct the problem, then repeat Step e through Step g.

Table 4: (Agent-based Linux PNs) Problems *Before* Enrollment

`Completed Successfully`
`The iptables firewall is enabled on this system....`
	Message appears in the shell, after the GUI curser exits. In addition, you'll be instructed to open up ports.

`Incorrect/invalid values entered`	Install utility stops if you type incorrect/invalid values. Correct the problem and **Save** again or **Cancel**.
`not authorized`	You either typed the credentials incorrectly or the user account does not have root privileges.

5. Install kernel-xen RPM package.

6. Copy and modify `/boot/grub/menu.lst`:

```
default=0
timeout=5
hiddenmenu
title Red Hat Enterprise Linux Server by Quorum onQ (2.6.18-
371.el5xen)
root (hd0,0)
kernel /vmlinuz-2.6.18-371.el5xen ro root=/dev/xvda1
rd_NO_LUKS rd_NO_MD rhgb crashkernel=auto rd_NO_LVM
initrd /initrd-2.6.18-371.el5xen.img.5
```

7. **Wait for the RN to build, then perform a self-test.**

   Troubleshooting RN Build or Self-test Problems

   Mistakes with the grub boot menu enforcement can prevent the RN from booting. The following list represents the most common errors.

   - Kernel parameters are not on one single line. Some file editors wrap long parameters.

- You have a typo in `grub.con` or `grub.conf.xvf5` file name.
- You have a typo in the kernel file name or the initramfs file name, or these files don’t exist.
- There is a mismatch, on the boot menu, between the kernel versions and the initramfs version. If the kernel's version does not match the contents of initramfs, the RN won't boot.The system could have more than one kernel installed:

  7.0:

  ```
  vmlinuz-3.10.0-123.13.2.el7.x86_64
  ```

  should match

  ```
  initramfs-3.10.0-123.13.2.el7xen.x86_64.img
  ```

  6.x:

  ```
  vmlinuz-2.6.32-279.el6.x86_64
  ```

  should match

  ```
  initramfs-2.6.32-279.el6.x86_64.img
  ```

  5.x:

  ```
  vmlinuz-2.6.18-371.el5xen
  ```

  should match

  ```
  initrd-2.6.18-371.el5xen.img.5
  ```

  To find the driver versions packed inside the init ram file system (`initramfs`) of the boot menu: Locate the initramfs and kernel name from the boot menu prepared for the RN (you’ll find it under `/boot)`, then use the following command to peek the contents of initramfs. For example:

RHEL 6.x or 7.0:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-3.10.0-123.el7.x86_64  ro
root=UUID=9002ec24-fb30-4d16-8a78-b352a807e82b
plymouth.enable=0 console=hvc0 loglvl=all
cgroup_disable=memory sync_console
console_to_ring earlyprintk=xen nomodeset net.if-
names=0 biosdevname=0 LANG=en_US.UTF-8
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initramfs-3.10.0-123.el7xen.x86_64.img
# lsinitrd /boot/initramsfs-3.10.0-
123.el7xen.x86_64.img|grep modules
rw-r--r--   1 root     root         1446 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep
-rw-r--r--   1 root     root         2450 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep.bin
-rw-r--r--   1 root     root           52 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.devname
-rw-r--r--   1 root     root        82512 Jun 30
2014 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.order
-rw-r--r--   1 root     root          165 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.softdep
-rw-r--r--   1 root     root        28132 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols
-rw-r--r--   1 root     root        34833 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols.bin
```

RHEL 5.x:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-2.6.18-371.el5xen ro
root=/dev/xvda1 rd_NO_LUKS rd_NO_MD rhgb crashker-
nel=auto rd_NO_LVM
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initrd-2.6.18-371.el5xen.img.5
# zcat /tmp/initrd-2.6.18-371.el5xen.img.5|cpio
-t|grep -E “xen|ext”
16524 blocks
lib/ext3.ko
lib/xennet.ko
lib/xenblk.ko
```

8.

9. **(Recommended) Disable the Network Manager service and Kudzu services**, if installed, for self-tests to work correctly. This service is not useful in a server environment.

```
# service NetworkManager stop
# service NetworkManager status
# chkconfig NetworkManager off
# chkconfig --list NetworkManager
NetworkManager  0:off   1:off   2:off   3:off
4:off   5:off   6:off
# service kudzu stop
# service kudzu status
# chkconfig kudzu off
# chkconfig --list kudzu
kudzu        0:off  1:off  2:off  3:off  4:off
5:off   6:off
```

10. **Log on to the PN and open the** following ports on the firewall in order for onQ to communicate with the PN.
    - UDP port `5990`
    - TCP ports `5000` and `5990`

11.

iptables:

a. Verify that udp 5990 and tcp 5000 and 5990 ports are open and above the `REJECT` line:

```
# iptables -L -n | grep -E "5900|5000"
ACCEPT   udp -- 0.0.0.0/0       0.0.0.0/0
udp dpt:5990
ACCEPT   tcp -- 0.0.0.0/0       0.0.0.0/0
state NEW tcp dpt:5000
ACCEPT   tcp -- 0.0.0.0/0       0.0.0.0/0
state NEW tcp dpt:5990
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with
icmp-host-prohibited
```

b. If these ports are not open, open them.

Find the input chain name, which is reported in the line that appears after `INPUT`:

```
# iptables -L -line numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 RH-Firewall-1-INPUT all -- anywhere anywhere
...
10 REJECT all -- anywhere anywhere reject-with
icmp-host-prohibited
```

Using the line number of the `REJECT` line and the chain name (line `10` and line `1`, respectively, in the step above), insert the onQ ports:

```
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5990 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5000 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -p udp --
dport 5990 -j ACCEPT
```

c. Save and restart iptables.

Afterward, verify that the ports are open and above the `REJECT` line as outlined earlier.

```
# service iptables save
Saving firewall rules to /etc/sysconfig/iptables:
[ OK ]
# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules:
ip_conntrack_netbios_n [ OK ]
```

12. **(Oracle database) Install `RMAN` scripts**.

    If the PN has an Oracle database, install the `RMAN` scripts so that onQ can execute a hot backup of your database as outlined in Back up and restore Oracle 11g database on Linux.

13.

(Optional) To enforce a network setting:

Unlike with Windows RNs, Linux RNs cannot be assigned to networks as outlined in Assign RNs to Networks. However, you can still enforce network settings for RN self-tests.

The Linux RN build should have a working NIC. If you have special need to set the RN’s NIC to a different IP, you can place a file, `/opt/quorum/bin/xvf.dat`, to generate `/etc/sysconfig/network-scripts/ifcfg-eth0`.

For example:

```
# cat /opt/quorum/bin/xvf.dat
@@XV_PN_IP
10.20.16.74
@@XV_PN_MASK
255.255.248.0
@@XV_PN_GW
10.20.16.1
```

Related Topics

(Agent-based Linux PNs) Update node software
(Agent-based Windows PNs) Enroll protected nodes
(Agent-less Linux/Windows PNs) Enroll protected nodes
(Agent-based PNs) Connection Problems

5.3 (Agent-based Centralized PNs) Enroll protected nodes

If you have a large number of PNs to enroll, consider using the onQ centralized installation manager for the platforms specified in Centralized Enrollment Support thereby eliminating repetitive tasks. With the onQ centralized installation manager, you do not need to log on to each PN separately to install the onQ Service.

Instead, simply configure the onQ Portal with your Windows Domain Controller account credentials. onQ centralized installation manager will then use an Active Directory GPO (Group Policy Object) to push the onQ Service software to the specified PNs and execute the install wizard for each PN. You only need to run the wizard once! This process also enrolls the Domain Controller itself.

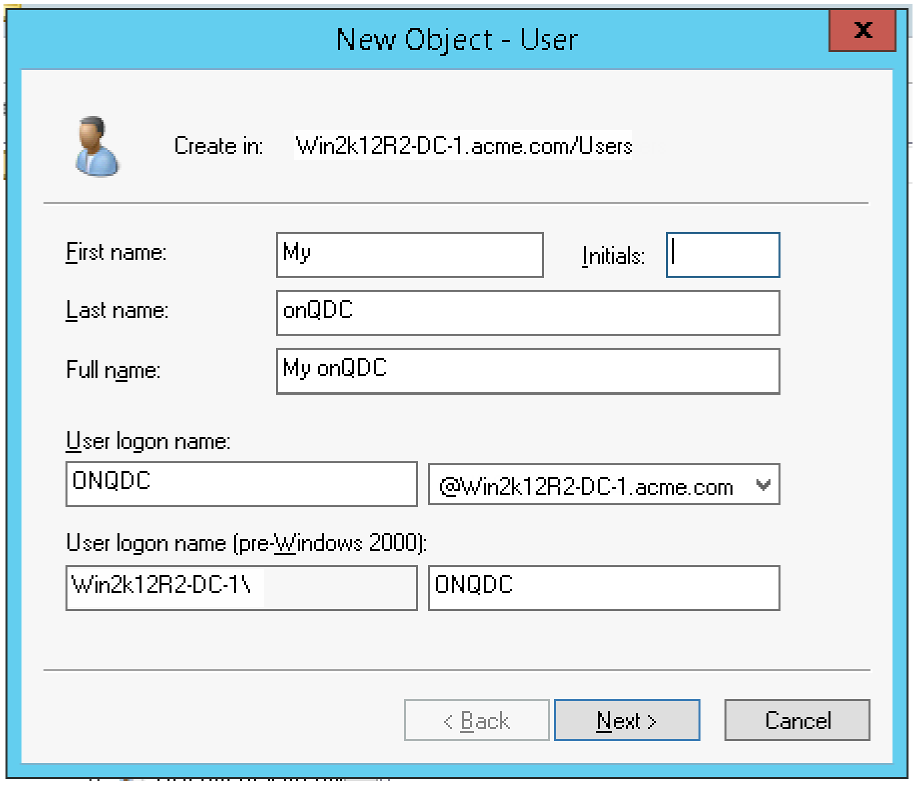
The onQ centralized installation manager sets the node configuration parameters to reasonable defaults that will protect your PNs, but you can customize these parameters globally during enrollment or individually after enrollment.

To enroll multiple agent-based PNs and DC simultaneously:

1. Verify that your platform is supported. Go to Centralized Enrollment Support.
2. (Important!) If any of your PNs were previously enrolled, search for and delete all orphan data for those PNs on both the HA and the DR.

   If you remove orphan data for a given PN from the HA—but not from the DR, then later re-enroll that same PN on the same HA, the DR fails to add the future snapshots for this PN thereby compromising disaster recovery.
3. Log on to the *primary* Windows Domain Controller and create a new account to be used exclusively by onQ. This account must have root privileges:

a. Specify an intuitive user name such as `ONQDC`. The first and last name entries aren’t important.



New Object - User

Create in: Win2k12R2-DC-1.acme.com/Users

First name: My

Initials:

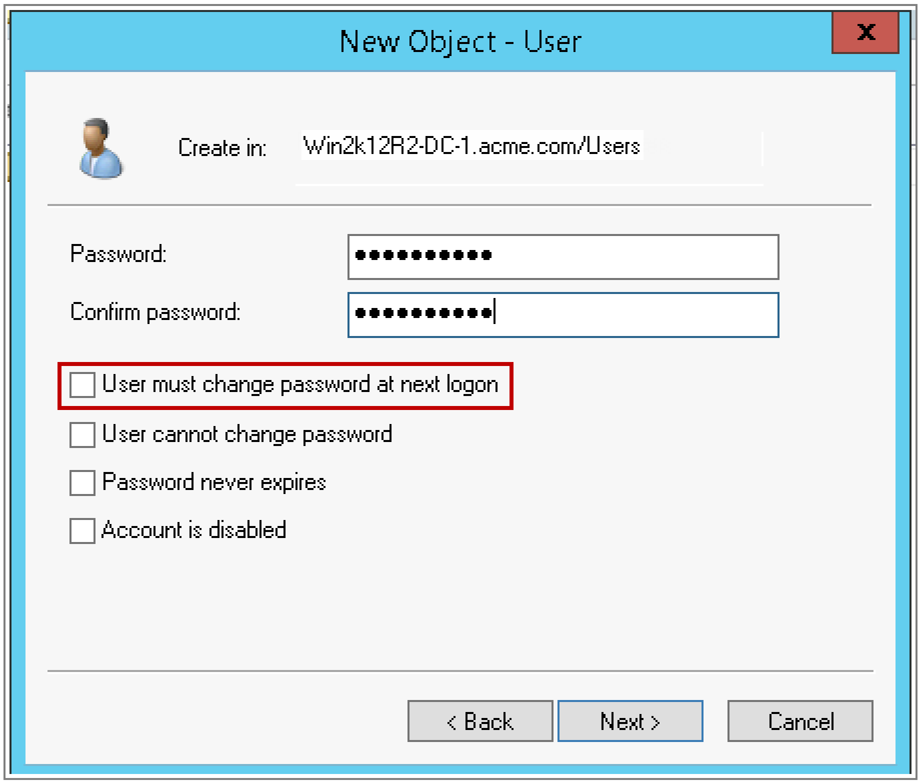
Last name: onQDC

Full name: My onQDC

User logon name: ONQDC @Win2k12R2-DC-1.acme.com

User logon name (pre-Windows 2000): Win2k12R2-DC-1\ ONQDC

b. Clear the **must change password on next login** check box.



New Object - User

Create in: Win2k12R2-DC-1.acme.com/Users

Password: ●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●

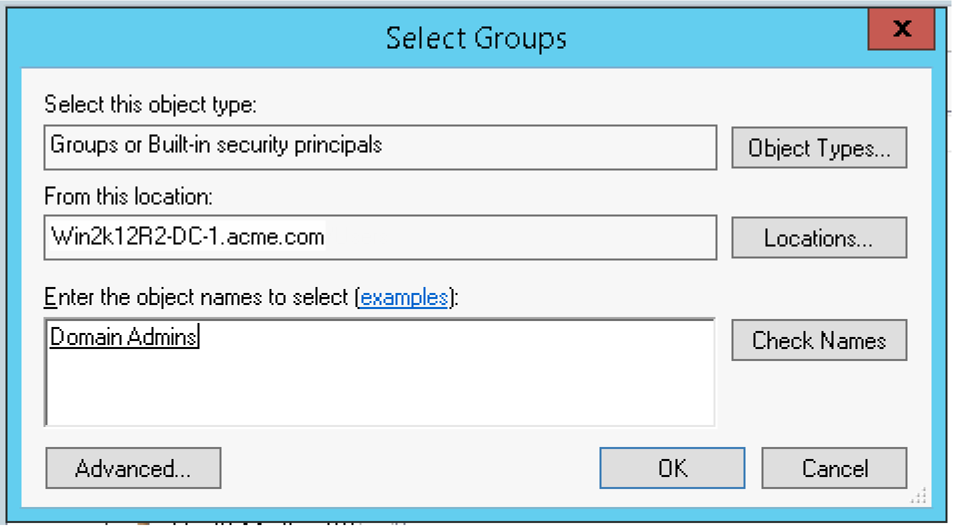
□ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

c. Right-click on the newly created user and **add to group**, specify **Domain Admins**, then click **Check Names** button.



Select Groups

Select this object type:
Groups or Built-in security principals

From this location:
Win2k12R2-DC-1.acme.com

Enter the object names to select (examples):
Domain Admins

4. Configure onQ to join the domain:

a. Log on to the HA’s onQ Portal.

b. Click the **PROTECTION CONFIG** tab.

c. Click the double-plus button (**++**).

d. The **Add Protected Nodes via Host** dialog appears.

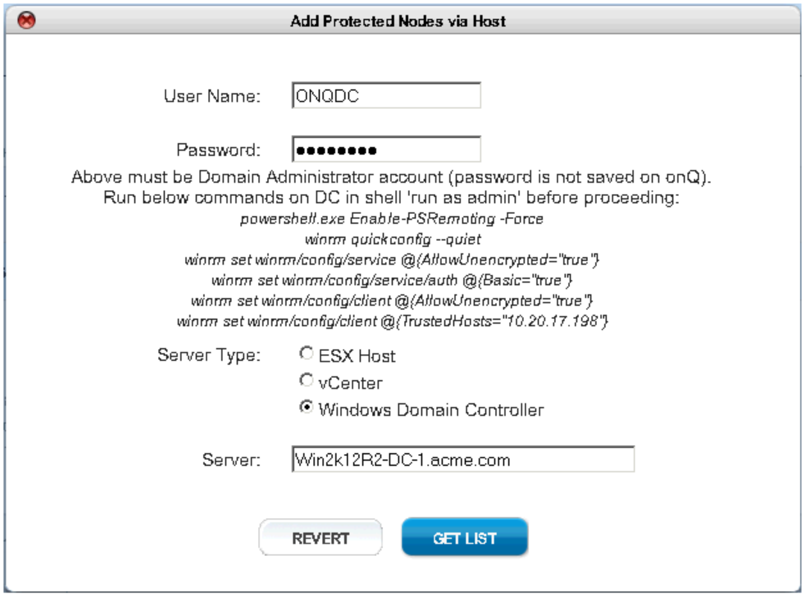
e. In the **Server Type** field, select the **Windows Domain Controller** radio button.

f. In the **User Name** and **Password** fields, provide the primary DC’s hostname or IP address and account credentials for the account that you created in Step 3. For security purposes, the username and password will not be saved.

g. Run the list of winrm (Windows Remote Management) commands that appear in the dialog. These commands enable the onQ Portal to retrieve a list of PNs registered with the Domain Controller and authorizes onQ to install packages on the PNs that you specify.

   After enrollment, you can disable winrm. For specific instructions, contact Quorum Support.

h. Click **GET LIST**.



Add Protected Nodes via Host

User Name: ONQDC

Password: ●●●●●●●●●

Above must be Domain Administrator account (password is not saved on onQ).
Run below commands on DC in shell 'run as admin' before proceeding:

```
powershell.exe Enable-PSRemoting -Force
winrm quickconfig --quiet
winrm set winrm/config/service @{AllowUnencrypted="true"}
winrm set winrm/config/service/auth @{Basic="true"}
winrm set winrm/config/client @{AllowUnencrypted="true"}
winrm set winrm/config/client @{TrustedHosts="10.20.17.198"}
```

Server Type: ○ ESX Host ○ vCenter ● Windows Domain Controller

Server: Win2k12R2-DC-1.acme.com

The onQ Portal retrieves a list of machines from Active Directory, then displays the inventory. You’re now ready to enroll them. Proceed to the next step.

5. Enroll the PNs:

a. Select the check boxes (or **ALL** button) for the PNs that you want to enroll.

   If a host does not appear in the list, make sure that (1) it is joined to the domain that you specified, and (2) its operating system is supported (see Centralized Enrollment Support).

   If a host appears, but is greyed out, it’s already enrolled on this onQ. If you want to enroll a previously enrolled agent-based PN on a different onQ using Centralized Enrollment, you must first delete the certificate on that PN; for instructions, go to Create secure connection to PNs.

b. Click **Enroll** to push the onQ Service to the PNs that you specified.

6. (Optional) Make global changes to the node configuration parameters. You can always customize these parameters after enrollment.
7. Verify enrollment. If onQ is unable to enroll a PN or the DC, see (Centralized Enrollment) Protected Node Enrollment Problems.
8. Activate the PNs. Go to **PROTECTION CONFIG** tab > **MODIFY** button > **SAVE** button.

   That’s it!

Related Topics

(Agent-based Linux PNs) Enroll protected nodes

(Agent-based Windows PNs) Enroll protected nodes

(Agent-less Linux/Windows PNs) Enroll protected nodes

(Agent-based PNs) Connection Problems

5.4 (Agent-less Linux/Windows PNs) Enroll protected nodes

onQ supports both agent-based and agent-less PNs. onQ’s VMware Real Agentless protection provides the following benefits:

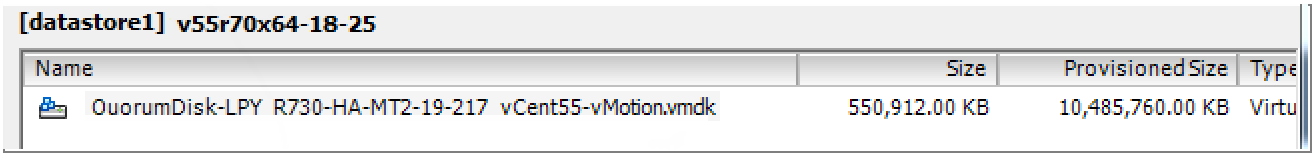
- No PN CPU utilization.
- Easier deployment in a VMware environment.
- No need to test or revalidate servers due to the introduction of new software.
- No need to worry about voiding vendor contracts or support due to installing agent-based software.

However, before you deploy agent-less PNs, consider the trade-offs outlined in “Agent-less PN Enrollment Limitations” in onQ Release Notes.

To protect agent-less PNs, you must indirectly enroll PNs by enrolling one of the following hosts:

- **vCenter Server**. Choose this option if your virtual machines are being hosted by multiple ESXi hosts and managed by vCenter; in this case, a vCenter enrollment provides the quickest deployment possible. This option is also advantageous if you want the ability to migrate those virtual machines to a different ESXi host using vSphere vMotion live migration; after a vMotion migration, onQ continues to back up those PNs, provided that you take into account the following requirements:
  - **Proxy installation**. Every ESXi host in a vMotion cluster must have a proxy installed from the onQ where the PN is enrolled. If you vMotion a PN on to an ESXi host that doesn't have a proxy installed, onQ cannot back up that PN and cannot notify you of this failure because onQ is unaware of that host.
  - **Shared datastore**. During a vMotion migration, virtual machines aren’t running. As a best practice, virtual machines should use a shared datastore, not a local datastore, so that they are available as soon as possible (and, therefore, available to be backed up by onQ), especially virtual machines with multi-terabytes of data. Moreover, if you don’t use shared storage, `QuorumDisk.vmdk`, which onQ creates for agent-less PNs to have persistent backup records in terms of scan and blocksums folders, doesn’t get automatically migrated by vMotion; therefore, onQ

must perform a full scan, not a delta, after the migration. (`QuorumDisk.vmdk` is created in the VM folder, but isn't part of the VM itself.) If you prefer local storage, manually migrate `QuorumDisk.vmdk` to the destination datastore *before* you perform the vMotion migration.



[datastore1] v55r70x64-18-25

Name	Size	Provisioned Size	Type
QuorumDisk-LPY_R730-HA-MT2-19-217_vCent55-vMotion.vmdk	550,912.00 KB	10,485,760.00 KB	Virtu

- **ESX/ESXi Server**. Choose this option if your virtual machines are being hosted by a *single* ESXi host.

VMware-hosted nodes, whether Windows or Linux, do not require that an agent (onQ Service) be installed on the PN. Instead, on *each* ESX/ESXi server (aka *Proxy Host*) that you enroll, the installer deploys 1 to 3 proxies per operating system type (Linux or Windows), per ESX/ESXi server, and per onQ. If all the PNs that you enroll have the same operating system, onQ doesn't deploy any PN proxies for the extraneous operating system. All PNs on a given ESX/ESXi server and having the same operating system (Linux or Windows) share the same PN proxies.

Using these proxies, the onQ's backup utility works with VMware Snapshot to back up the PNs to the HA.

Note: If you need to rename the onQ host name, you will need to perform the steps outlined in Configure Appliance's network settings.

Note the following:

- Whether you enroll using vCenter Server or ESX/ESXi Server, you can configure 1 to 3 proxies per operating system type per onQ, though you must configure *at least one* proxy per ESXi server and per onQ if the ESXi server is part of a vSphere cluster. The onQ enrollment process simply deploys the requested proxy type and number of proxies that you configure. Quorum recommends that you configure the maximum to realize onQ's ability to perform three concurrent backups and to facilitate timely backups (see Stop in-progress backups).
- Whether you enroll using vCenter Server or ESX/ESXi Server, all proxies deployed from a specific onQ are removed only upon deletion of the last PN from that onQ and will be reflected in the onQ's configuration after such deletion occurs.

For information about how onQ upgrades these proxies, go to Update Appliance software.

(Windows/vCenter) To enroll an agent-less Windows PN:

Use this procedure to enroll an agent-less Windows PN that's being managed by vCenter.

Warning: If your Windows 2012 PN is running on the VMware host and uses the VMware E1000E network interface adapter, squirt-server might receive a corrupted `source.info` from squirtcopy due to a problem with VMware's NIC, as outlined in VMware KB 2058692. To prevent this problem, on the VMware-hosted PNs, switch the NIC type from E1000E to E1000.

1. **Install the PN proxies**:

   a. Enable `ssh` on each ESXi/ESX server in the vMotion cluster.

   b. Reserve 1 to 3 unique static IP addresses for each PN proxy type (Linux and Windows). The more proxies you configure, the more concurrent backups onQ can perform.

   c. Log on to the HA's onQ Portal.

   d. Click the **PROTECTION CONFIG** tab > double-plus button (**++**).

      The **Add Protected Nodes via Host** dialog appears.

   e. In the **Server Type** field, select the **vCenter** radio button.

   f. Provide the vCenter credentials for any user with root privileges and either the hostname or the IP address for vCenter, then **GET LIST**. The **Add Protected Nodes via vCenter** dialog appears.

      The onQ Portal queries the virtual machines managed by vCenter, then displays the inventory.

   g. Provide ESXi host credentials for any user with root privileges, specify proxy information for each proxy type, and select the check boxes for the PNs that you want to enroll.

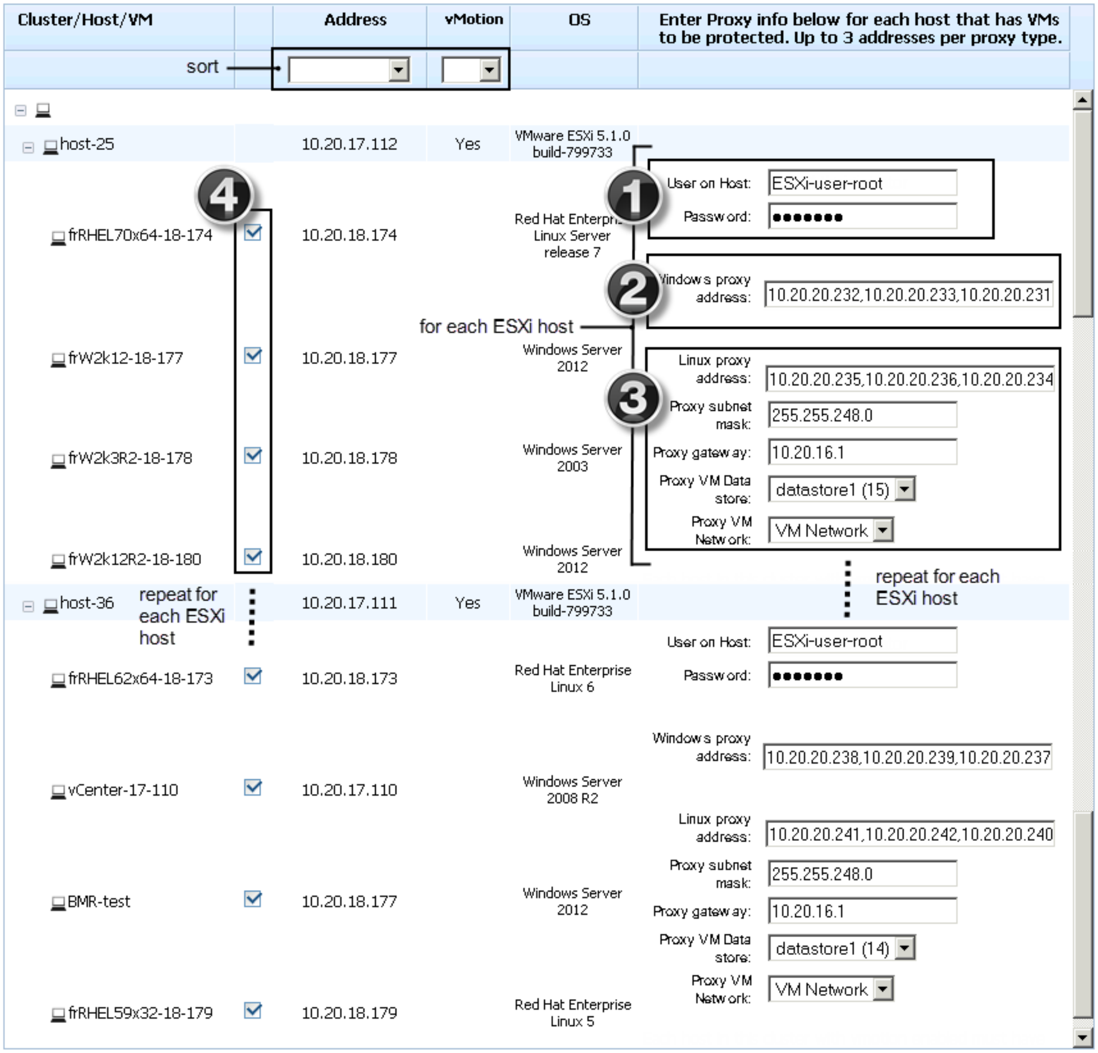
      If an expected virtual machine does not appear in the list, it's likely that the virtual machine does not have VMware Tools installed.

      Provide the network properties for each proxy. Use the unique IP address(es) that you reserved above. If more than one IP per proxy type, provide a comma-separated list.

      - **Windows proxy address**. The static IP address that you reserved for the Windows PN proxy.

- **Linux proxy address**. The static IP address that you reserved for the Linux PN proxy.
- **Proxy subnet mask**. The PN proxy's subnet mask.
- **Proxy gateway**. The PN proxy's gateway.
- **Proxy VM Data store**. The directory in which the vm's files are stored.
- **Proxy VM Network**. Your network configuration can include a vCenter-level Distributed Virtual Switches (DVS) or an ESXi host-level virtual switch. When you enroll an ESXi host, all available networks that are visible to that host are listed and available for selection.

In the following example, all PNs on all ESXi hosts in the vMotion cluster are being enrolled and using the maximum number of proxies allowed for each proxy type:



Cluster/Host/VM		Address	vMotion	OS
host-25		10.20.17.112	Yes	VMware ESXi 5.1.0 build-799733
frRHEL70x64-18-174	☑	10.20.18.174		Red Hat Enterpr Linux Server release 7
frW2k12-18-177	☑	10.20.18.177		Windows Server 2012
frW2k3R2-18-178	☑	10.20.18.178		Windows Server 2003
frW2k12R2-18-180	☑	10.20.18.180		Windows Server 2012
host-36		10.20.17.111	Yes	VMware ESXi 5.1.0 build-799733
frRHEL62x64-18-173	☑	10.20.18.173		Red Hat Enterprise Linux 6
vCenter-17-110	☑	10.20.17.110		Windows Server 2008 R2
BMR-test	☑	10.20.18.177		Windows Server 2012
frRHEL59x32-18-179	☑	10.20.18.179		Red Hat Enterprise Linux 5

Enter Proxy info below for each host that has VMs to be protected. Up to 3 addresses per proxy type.

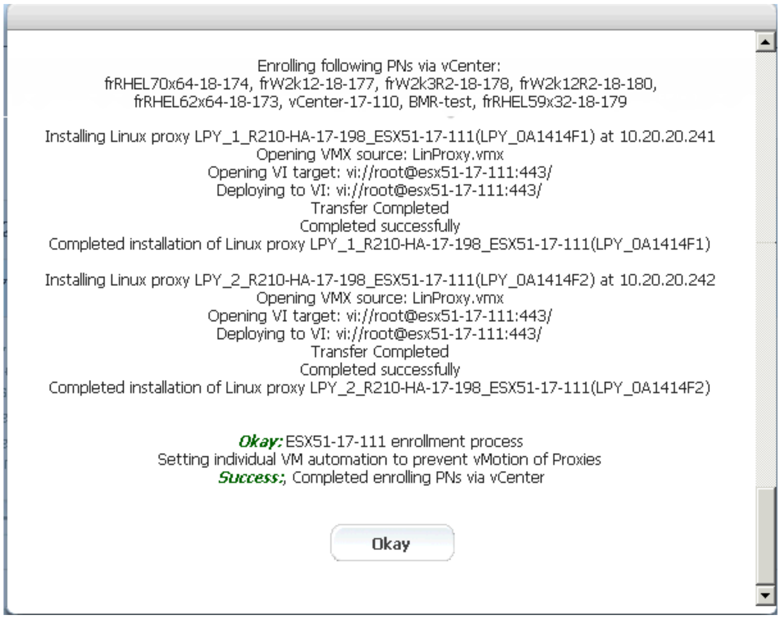
host-25:

User on Host: ESXi-user-root
Password: •••••••
Windows proxy address: 10.20.20.232,10.20.20.233,10.20.20.231
Linux proxy address: 10.20.20.235,10.20.20.236,10.20.20.234
Proxy subnet mask: 255.255.248.0
Proxy gateway: 10.20.16.1
Proxy VM Data store: datastore1 (15)
Proxy VM Network: VM Network

host-36:

User on Host: ESXi-user-root
Password: •••••••
Windows proxy address: 10.20.20.238,10.20.20.239,10.20.20.237
Linux proxy address: 10.20.20.241,10.20.20.242,10.20.20.240
Proxy subnet mask: 255.255.248.0
Proxy gateway: 10.20.16.1
Proxy VM Data store: datastore1 (14)
Proxy VM Network: VM Network

Click the **ENROLL** button, then **OKAY**.



```
Enrolling following PNs via vCenter:
frRHEL70x64-18-174, frW2k12-18-177, frW2k3R2-18-178, frW2k12R2-18-180,
frRHEL62x64-18-173, vCenter-17-110, BMR-test, frRHEL59x32-18-179

Installing Linux proxy LPY_1_R210-HA-17-198_ESX51-17-111(LPY_0A1414F1) at 10.20.20.241
Opening VMX source: LinProxy.vmx
Opening VI target: vi://root@esx51-17-111:443/
Deploying to VI: vi://root@esx51-17-111:443/
Transfer Completed
Completed successfully
Completed installation of Linux proxy LPY_1_R210-HA-17-198_ESX51-17-111(LPY_0A1414F1)

Installing Linux proxy LPY_2_R210-HA-17-198_ESX51-17-111(LPY_0A1414F2) at 10.20.20.242
Opening VMX source: LinProxy.vmx
Opening VI target: vi://root@esx51-17-111:443/
Deploying to VI: vi://root@esx51-17-111:443/
Transfer Completed
Completed successfully
Completed installation of Linux proxy LPY_2_R210-HA-17-198_ESX51-17-111(LPY_0A1414F2)

Okay: ESX51-17-111 enrollment process
Setting individual VM automation to prevent vMotion of Proxies
Success:, Completed enrolling PNs via vCenter
```

The PNs that you selected appear in the Protected Nodes list; however, they are `unverified` as evidenced by the status in the **PROTECTED NODES** page > **Protection Disabled** column.

h. From the ESXi/ESX host, power on the PN proxies.

i. Activate (aka *verify*) the PNs so that onQ can protect them.

Go to **PROTECTION CONFIG** tab, select the PN, then click the **MODIFY** button.

Specify values for the node parameters, then **SAVE**. The act of saving a PN’s configuration instructs onQ to activate that PN’s configuration. If the PN is a Linux PN, onQ cannot enroll these XFS mount points automatically, so you must do so now. See Linux Filesystem Format Requirements.

The onQ Portal groups the PNs by ESXi server. If you do not want these PNs in such a group, clear the default **Group Name** field to remove the PNs from this group and place them in the shared pool.

2. **Log on to the PN and open the** following ports on the firewall in order for onQ to communicate with the PN.
    - UDP port `5990`
    - TCP ports `5000` and `5990`

3.

4. (Oracle database) Install `RMAN` scripts.

   If the PN has an Oracle database, install the `RMAN` scripts so that onQ can execute a hot backup of your database as outlined in Back up and restore Oracle 10g+ database on Windows.

(Windows/ESXi) To enroll an agent-less Windows PN:

Use this procedure to enroll an agent-less Windows PN that's being hosted my an ESXi server.

Warning: If your Windows 2012 PN is running on the VMware host and uses the VMware E1000E network interface adapter, squirt-server might receive a corrupted `source.info` from squirtcopy due to a problem with VMware's NIC, as outlined in VMware KB 2058692. To prevent this problem, on the VMware-hosted PNs, switch the NIC type from E1000E to E1000.

1. **Install the PN proxies**:

   a. Enable `ssh` on the ESXi/ESX server.

   b. Reserve 1 to 3 unique static IP addresses for each PN proxy type (Linux and Windows). The more proxies you configure, the more concurrent backups onQ can perform.

   c. Log on to the HA's onQ Portal.

   d. Click the **PROTECTION CONFIG** tab > double-plus button (**++**).

      The **Add Protected Nodes via Host** dialog appears.

   e. In the **Server Type** field, select the **ESX Host** radio button.

   f. In the **User Name** and **Password** fields, provide the ESXi/ESX host credentials for any user with root privileges.

   g. In the Server field, provide either the hostname or the IP address for the ESXi/ESX host, then **GET LIST**.

      The onQ Portal queries the virtual machines hosted by the ESXi/ESX server, then displays the inventory.

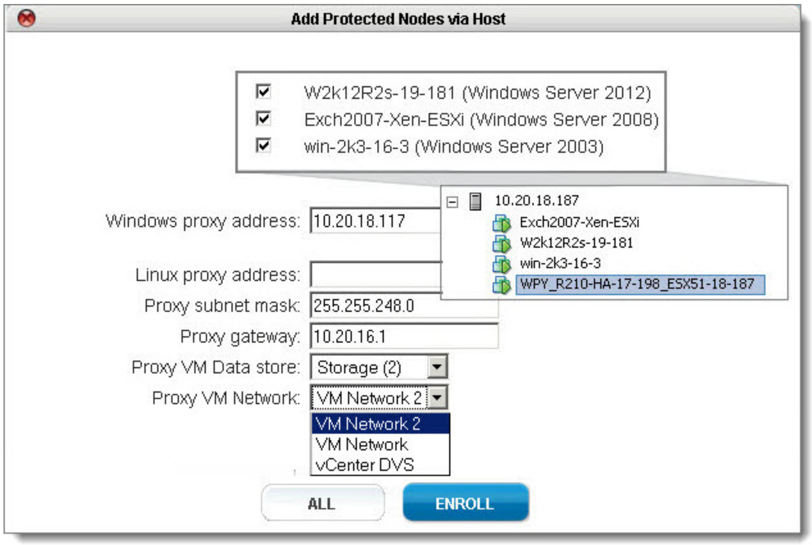
   h. In the virtual machine list, select the check boxes (or **ALL** button) for the PNs that you want to enroll.

If an expected virtual machine does not appear in the list, it's likely that the virtual machine does not have VMware Tools installed.

Provide the network properties for each proxy. Use the unique IP addresses that you reserved above.

- **Windows proxy address**. The static IP address that you reserved for the Windows PN proxy.
- **Linux proxy address**. The static IP address that you reserved for the Linux PN proxy.
- **Proxy subnet mask**. The PN proxy's subnet mask.
- **Proxy gateway**. The PN proxy's gateway.
- **Proxy VM Data store**. The directory in which the vm's files are stored.
- **Proxy VM Network**. Your network configuration can include a vCenter-level Distributed Virtual Switches (DVS) or an ESXi host-level virtual switch. When you enroll an ESXi host, all available networks that are visible to that host are listed and available for selection.

In the following example, three Windows PN are being enrolled, so only one static IP address (for the Windows PN proxy `WPY_`<onQhostname>_<ESXhostname>) is needed:

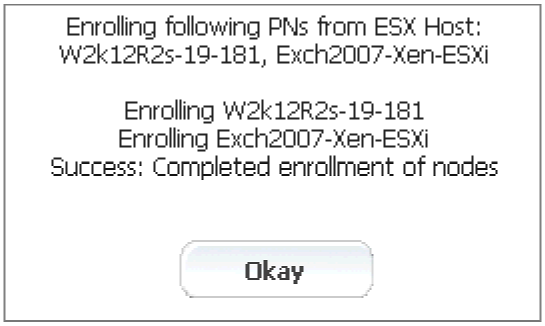


Add Protected Nodes via Host

☑ W2k12R2s-19-181 (Windows Server 2012)
☑ Exch2007-Xen-ESXi (Windows Server 2008)
☑ win-2k3-16-3 (Windows Server 2003)

Windows proxy address: 10.20.18.117
Linux proxy address:
Proxy subnet mask: 255.255.248.0
Proxy gateway: 10.20.16.1
Proxy VM Data store: Storage (2)
Proxy VM Network: VM Network 2

Click the **ENROLL** button, then **OKAY**.



Enrolling following PNs from ESX Host:
W2k12R2s-19-181, Exch2007-Xen-ESXi

Enrolling W2k12R2s-19-181
Enrolling Exch2007-Xen-ESXi
Success: Completed enrollment of nodes

The PNs that you selected appear in the Protected Nodes list; however, they are `unverified` as evidenced by the status in the **PROTECTED NODES** page > **Protection Disabled** column.

i. From the ESXi/ESX host, power on the PN proxies.

j. Activate (aka *verify*) the PNs so that onQ can protect them.

Go to **PROTECTION CONFIG** tab, select the PN, then click the **MODIFY** button.

Specify values for the node parameters, then **SAVE**. The act of saving a PN's configuration instructs onQ to activate that PN's configuration. If the PN is a Linux PN, onQ cannot enroll these XFS mount points automatically, so you must do so now. See Linux Filesystem Format Requirements.

The onQ Portal groups the PNs by ESXi server. If you do not want these PNs in such a group, clear the default **Group Name** field to remove the PNs from this group and place them in the shared pool.

2. **Log on to the PN and open the** following ports on the firewall in order for onQ to communicate with the PN.
   - UDP port `5990`
   - TCP ports `5000` and `5990`

3. (Oracle database) Install `RMAN` scripts.

   If the PN has an Oracle database, install the `RMAN` scripts so that onQ can execute a hot backup of your database as outlined in Back up and restore Oracle 10g+ database on Windows.

(RHEL 7.0/vCenter) To enroll an agent-less Linux PN:

Use this procedure to enroll an agent-less Linux PN running RHEL 7.0 and that's being managed by vCenter.

1. **Install the PN proxies**:
   - **a.** Enable `ssh` on each ESXi/ESX server in the vMotion cluster.
   - **b.** Reserve 1 to 3 unique static IP addresses for each PN proxy type (Linux and Windows). The more proxies you configure, the more concurrent backups onQ can perform.
   - **c.** Log on to the HA's onQ Portal.
   - **d.** Click the **PROTECTION CONFIG** tab > double-plus button (**++**).

     The **Add Protected Nodes via Host** dialog appears.
   - **e.** In the **Server Type** field, select the **vCenter** radio button.
   - **f.** Provide the vCenter credentials for any user with root privileges and either the hostname or the IP address for vCenter, then **GET LIST**. The **Add Protected Nodes via vCenter** dialog appears.

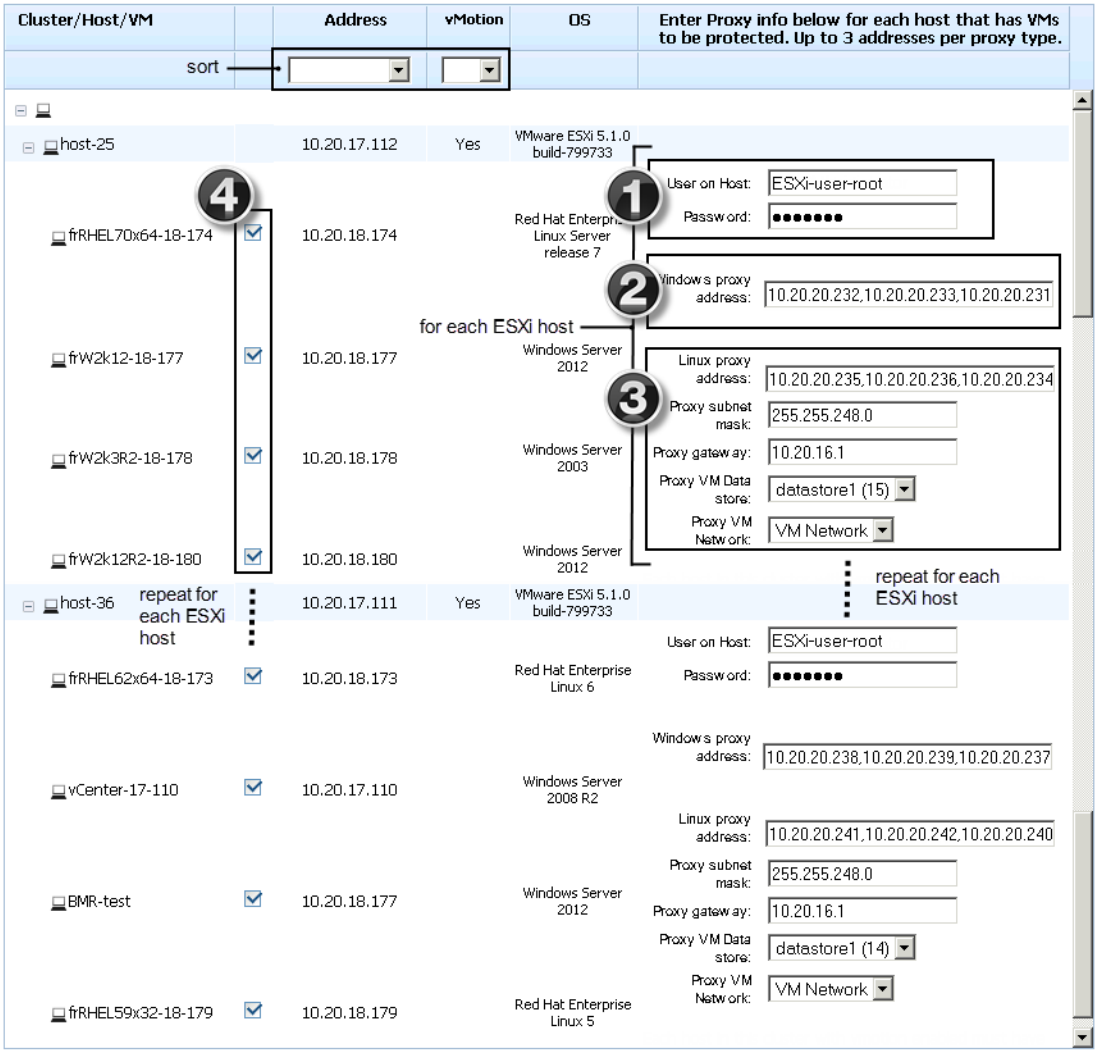
     The onQ Portal queries the virtual machines managed by vCenter, then displays the inventory.
   - **g.** Provide ESXi host credentials for any user with root privileges, specify proxy information for each proxy type, and select the check boxes for the PNs that you want to enroll.

     If an expected virtual machine does not appear in the list, it's likely that the virtual machine does not have VMware Tools installed.

     Provide the network properties for each proxy. Use the unique IP address(es) that you reserved above. If more than one IP per proxy type, provide a comma-separated list.
     - **Windows proxy address**. The static IP address that you reserved for the Windows PN proxy.
     - **Linux proxy address**. The static IP address that you reserved for the Linux PN proxy.
     - **Proxy subnet mask**. The PN proxy's subnet mask.
     - **Proxy gateway**. The PN proxy's gateway.
     - **Proxy VM Data store**. The directory in which the vm's files are stored.
     - **Proxy VM Network**. Your network configuration can include a

vCenter-level Distributed Virtual Switches (DVS) or an ESXi host-level virtual switch. When you enroll an ESXi host, all available networks that are visible to that host are listed and available for selection.

In the following example, all PNs on all ESXi hosts in the vMotion cluster are being enrolled and using the maximum number of proxies allowed for each proxy type:



Cluster/Host/VM		Address	vMotion	OS
host-25		10.20.17.112	Yes	VMware ESXi 5.1.0 build-799733
frRHEL70x64-18-174	☑	10.20.18.174		Red Hat Enterpri Linux Server release 7
frW2k12-18-177	☑	10.20.18.177		Windows Server 2012
frW2k3R2-18-178	☑	10.20.18.178		Windows Server 2003
frW2k12R2-18-180	☑	10.20.18.180		Windows Server 2012
host-36		10.20.17.111	Yes	VMware ESXi 5.1.0 build-799733
frRHEL62x64-18-173	☑	10.20.18.173		Red Hat Enterprise Linux 6
vCenter-17-110	☑	10.20.17.110		Windows Server 2008 R2
BMR-test	☑	10.20.18.177		Windows Server 2012
frRHEL59x32-18-179	☑	10.20.18.179		Red Hat Enterprise Linux 5

Enter Proxy info below for each host that has VMs to be protected. Up to 3 addresses per proxy type.

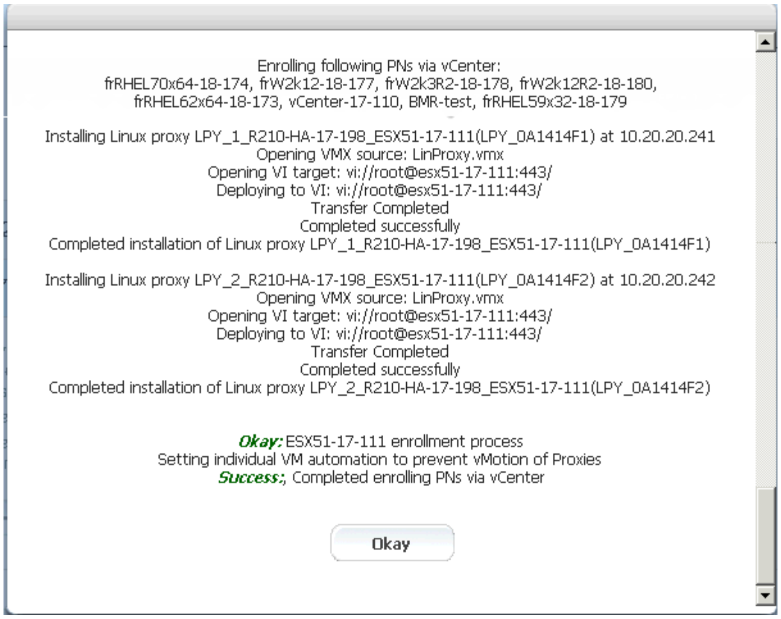
host-25:

User on Host: ESXi-user-root
Password: ●●●●●●●
Windows proxy address: 10.20.20.232,10.20.20.233,10.20.20.231
Linux proxy address: 10.20.20.235,10.20.20.236,10.20.20.234
Proxy subnet mask: 255.255.248.0
Proxy gateway: 10.20.16.1
Proxy VM Data store: datastore1 (15)
Proxy VM Network: VM Network

host-36:

User on Host: ESXi-user-root
Password: ●●●●●●●
Windows proxy address: 10.20.20.238,10.20.20.239,10.20.20.237
Linux proxy address: 10.20.20.241,10.20.20.242,10.20.20.240
Proxy subnet mask: 255.255.248.0
Proxy gateway: 10.20.16.1
Proxy VM Data store: datastore1 (14)
Proxy VM Network: VM Network

Click the **ENROLL** button, then **OKAY**.



```
Enrolling following PNs via vCenter:
frRHEL70x64-18-174, frW2k12-18-177, frW2k3R2-18-178, frW2k12R2-18-180,
frRHEL62x64-18-173, vCenter-17-110, BMR-test, frRHEL59x32-18-179

Installing Linux proxy LPY_1_R210-HA-17-198_ESX51-17-111(LPY_0A1414F1) at 10.20.20.241
Opening VMX source: LinProxy.vmx
Opening VI target: vi://root@esx51-17-111:443/
Deploying to VI: vi://root@esx51-17-111:443/
Transfer Completed
Completed successfully
Completed installation of Linux proxy LPY_1_R210-HA-17-198_ESX51-17-111(LPY_0A1414F1)

Installing Linux proxy LPY_2_R210-HA-17-198_ESX51-17-111(LPY_0A1414F2) at 10.20.20.242
Opening VMX source: LinProxy.vmx
Opening VI target: vi://root@esx51-17-111:443/
Deploying to VI: vi://root@esx51-17-111:443/
Transfer Completed
Completed successfully
Completed installation of Linux proxy LPY_2_R210-HA-17-198_ESX51-17-111(LPY_0A1414F2)


Okay: ESX51-17-111 enrollment process
Setting individual VM automation to prevent vMotion of Proxies
Success:; Completed enrolling PNs via vCenter
```

The PNs that you selected appear in the Protected Nodes list; however, they are `unverified` as evidenced by the status in the **PROTECTED NODES** page > **Protection Disabled** column.

h. From the ESXi/ESX host, power on the PN proxies.

i. Activate (aka *verify*) the PNs so that onQ can protect them.

Go to **PROTECTION CONFIG** tab, select the PN, then click the **MODIFY** button.

Specify values for the node parameters, then **SAVE**. The act of saving a PN’s configuration instructs onQ to activate that PN’s configuration. If the PN is a Linux PN, onQ cannot enroll these XFS mount points automatically, so you must do so now. See Linux Filesystem Format Requirements.

The onQ Portal groups the PNs by ESXi server. If you do not want these PNs in such a group, clear the default **Group Name** field to remove the PNs from this group and place them in the shared pool.

2. **Create the grub boot menu**. In order to boot the RN successfully, the PN needs to prepare the init ram disk image with the required drivers and legacy grub boot menu.

a. Verify OS version:

```
# cat /etc/redhat-release

Red Hat Enterprise Linux Server release 7.0
(Maipo)
```

b. Make sure `ext2`/`ext3`/`ext4` file systems utilities are installed.

```
# rpm -qa | grep e2fsprogs

e2fsprogs-libs-1.42.9-4.el7.x86_64

e2fsprogs-1.42.9-4.el7.x86_64
```

If not installed, do so now:

```
# yum install e2fsprogs
```

c. Generate the init ram disk with xen drivers and `ext4` file system modules.

Print the kernel release:

```
# uname -r
3.10.0-123.13.2.el7.x86_64
```

Where the `3.10.0-123.13.2.el7.x86_64` is the kernel release by default, change it to match PN's kernel release:

```
# cd /boot
# mkdir -p /boot/grub
# dracut --force --filesystems "ext4 ext3"  \
--add-drivers  "xen:vbd xen:vif" \
initramfs-3.10.0-123.13.2.el7xen.x86_64.img
```

d. Verify the legacy grub boot loader:

```
# vi /boot/grub/grub.conf.xvf5
```

Where the `3.10.0-123.13.2.el7.x86_64` is the kernel release by default, change `vmlinuz` and `initramfs` to match PN's kernel release. The kernel parameters are on a single line. Simply copy and paste from following screen.

Where the `root=UUID=855cd484-3852-4984-b568-ee0408c6b590`, the `855cd`... (UUID) is a temporary placeholder and will be replaced by read "`/`"'s UUID during the RN build. Do not make any changes to this parameter.

For example: The contents of `/boot/grub/grub.conf.xvf5`:

```
default=0
timeout=5
title onQ Red Hat Enterprise Linux (3.10.0-123.13.2.el7.x86_64)
root (hd0,0)
kernel /vmlinuz-3.10.0-123.13.2.el7.x86_64 ro root=UUID=855cd484-3852-
4984-b568-ee0408c6b590 plymouth.enable=0 console=hvc0 loglvl=all
cgroup_disable=memory sync_console console_to_ring earlyprintk=xen
nomodeset net.ifnames=0 biosdevname=0 LANG=en_US.UTF-8
initrd /initramfs-3.10.0-123.13.2el7xen.x86_64.img
```

From `/boot`, validate that `vmlinuz-3.10.0-123.13.2.el7.x86_64` and `initramfs-3.10.0-123.13.2.el7xen.x86_64.img` exist in `/boot` folder as shown in the example below:

```
# ls /boot/vmlinuz-3.10.0-123.13.2.el7.x86_64
/boot/vmlinuz-3.10.0-123.13.2.el7.x86_64
# ls /boot/initramfs-3.10.0-
123.13.2.el7xen.x86_64.img
/boot/initramfs-3.10.0-123.13.2.el7xen.x86_64.img
```

3. **Wait for the RN to build, then perform a self-test**.

   Troubleshooting RN Build or Self-test Problems

   Mistakes with the grub boot menu enforcement can prevent the RN from booting. The following list represents the most common errors.

   - Kernel parameters are not on one single line. Some file editors wrap long parameters.
   - You have a typo in `grub.con` or `grub.conf.xvf5` file name.
   - You have a typo in the kernel file name or the initramfs file name, or these files don't exist.
   - There is a mismatch, on the boot menu, between the kernel versions and the initramfs version. If the kernel's version does not match the contents of initramfs, the RN won't boot.The system could have more than one kernel installed:

7.0:

`vmlinuz-3.10.0-123.13.2.el7.x86_64`

should match

`initramfs-3.10.0-123.13.2.el7xen.x86_64.img`

6.x:

`vmlinuz-2.6.32-279.el6.x86_64`

should match

`initramfs-2.6.32-279.el6.x86_64.img`

5.x:

`vmlinuz-2.6.18-371.el5xen`

should match

`initrd-2.6.18-371.el5xen.img.5`

To find the driver versions packed inside the init ram file system (`initramfs`) of the boot menu: Locate the initramfs and kernel name from the boot menu prepared for the RN (you'll find it under `/boot)`, then use the following command to peek the contents of initramfs. For example:

RHEL 6.x or 7.0:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-3.10.0-123.el7.x86_64  ro
root=UUID=9002ec24-fb30-4d16-8a78-b352a807e82b
plymouth.enable=0 console=hvc0 loglvl=all
cgroup_disable=memory sync_console
console_to_ring earlyprintk=xen nomodeset net.if-
names=0 biosdevname=0 LANG=en_US.UTF-8
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initramfs-3.10.0-123.el7xen.x86_64.img
# lsinitrd /boot/initramsfs-3.10.0-
123.el7xen.x86_64.img|grep modules
rw-r--r--   1 root     root         1446 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep
-rw-r--r--   1 root     root         2450 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep.bin
-rw-r--r--   1 root     root           52 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.devname
-rw-r--r--   1 root     root        82512 Jun 30
2014 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.order
-rw-r--r--   1 root     root          165 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.softdep
-rw-r--r--   1 root     root        28132 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols
-rw-r--r--   1 root     root        34833 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols.bin
```

RHEL 5.x:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-2.6.18-371.el5xen ro
root=/dev/xvda1 rd_NO_LUKS rd_NO_MD rhgb crashkernel=auto rd_NO_LVM
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initrd-2.6.18-371.el5xen.img.5
# zcat /tmp/initrd-2.6.18-371.el5xen.img.5|cpio
-t|grep -E “xen|ext”
16524 blocks
lib/ext3.ko
lib/xennet.ko
lib/xenblk.ko
```

4. **Log on to the PN and open the** following ports on the firewall in order for onQ to communicate with the PN.
   - UDP port `5990`
   - TCP ports `5000` and `5990`

   Firewalld:

   By default, RHEL 7.0 has introduced a new firewall service, a dynamic firewall daemon known as `firewalld`, instead of iptables service by default; however, the traditional iptables service is supported if installed. For details, see the Red Hat Linux 7 Security Guide. If you choose to disable firewalld, there is no need to configure firewalld firewall rules: simply skip this procedure.

   `firewalld` daemon and service and iptables service are using iptables commands to configure the netfilter in the kernel to separate and filter the network traffic. `firewalld` stores it in various XML files in `/usr/lib/firewalld/` and `/etc/firewalld/`.

   The firewalld firewall defines how *networks zones* can be used to separate networks into different zones. Based on the level of trust, you can decide to place devices and traffic within a particular network zone. Each mutable network zone can have a different combination of firewall rules.

   a. Verify that firewalld is in a running state.

b. Check the service status:

```
[root@RHEL70x64-17-167 services]# systemctl status
firewalld.service
firewalld.service - firewalld - dynamic firewall
daemon
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled)
Active: inactive (dead)
```

c. Enable the service, if not already enabled:

```
[root@RHEL70x64-17-167 services]# systemctl enable
firewalld
ln -s '/usr/lib/systemd/system/firewalld.service'
'/etc/systemd/system/dbusorg.edoraproject.FirewallD1.service'
ln -s '/usr/lib/systemd/system/firewalld.service'
'/etc/systemd/system
/basic.target.wants/firewalld.service'
```

d. Start the service, if not already running:

```
[root@RHEL70x64-17-167 services]# systemctl start
firewalld
```

e. On the PN, find the network interface that is used to communicate with onQ. In this example, that NIC is `ens32`.

```
[root@RHEL70x64-17-167 services]# ifconfig
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.20.17.167 netmask 255.255.248.0 broadcast 10.20.23.255
inet6 fe80::250:56ff:fe9d:2121 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:9d:21:21 txqueuelen 1000 (Ethernet)
RX packets 7115713 bytes 476287831 (454.2 MiB)
RX errors 0 dropped 149791 overruns 0 frame 0
TX packets 924966 bytes 1305413839 (1.2 GiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 10 bytes 980 (980.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10 bytes 980 (980.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

f. For the network interface that you identified above, find the network interface’s network zone. In this example, the network zone is `work`.

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-zone-of-interface=ens32
work
```

Determine your default zone. In the following example, the default zone is `Public`.

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-default-zone
public
```

g. Associate the zone(s) with the following firewall rules. The same rules can be applied to many zones as needed. In the following example, dcrm-node service is associated with `work` zone for `ens32`. The `dcrm-node.xml` is located at `/usr/lib/firewalld/services`.

```
[root@RHEL70x64-17-167 services]# firewall-cmd --add-service=dcrm-node --permanent --zone=work
success
```

h. Activate the latest firewall rules:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --reload
success
```

Now the PN can communicate with onQ.

i. Set up the rule for RN on the PN site.

The RN will be equipped with `eth0` interface, so apply the rules to `eth0` interface's zone if different from PN's zone. The PN might not have `eth0` interface; in such a case, the RN's `eth0` will be in the default zone.

Find `eth0` network interface's network zone. In this example, it is *not* set:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-zone-of-interface=eth0
no zone
```

Determine your default zone. In this example default zone is `Public`. Since `eth0` has no zone dcm-node is associated with `Public` zone:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-default-zone
public
```

j. Associate the zone(s) with the following firewall rules. The same rules can be applied to many zones as needed:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --add-service=dcrm-node --permanent --zone=public
success
```

k. Active the latest firewall rules:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --reload
success
```

Now the RN can communicate with onQ, mainly for self-tests.

l. Confirm the firewall rules. The public zone and work zone have TCP ports (5000/5990) and UDP port 5990 opened in this case.

```
[root@RHEL70x64-17-167 services]# iptables -L -n
Chain IN_public (2 references)
target prot opt source destination
IN_public_log all -- 0.0.0.0/0 0.0.0.0/0
IN_public_deny all -- 0.0.0.0/0 0.0.0.0/0
IN_public_allow all -- 0.0.0.0/0 0.0.0.0/0
Chain IN_public_allow (1 references)
target prot opt source destination
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5000 ct-
state NEW
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 ct-
state NEW
Chain IN_work (0 references)
target prot opt source destination
IN_work_log all -- 0.0.0.0/0 0.0.0.0/0
IN_work_deny all -- 0.0.0.0/0 0.0.0.0/0
IN_work_allow all -- 0.0.0.0/0 0.0.0.0/0
Chain IN_work_allow (1 references)
target prot opt source destination
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:631 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5000 ct-
state NEW
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 ct-
state NEW
```

iptables:

a. Verify that udp 5990 and tcp 5000 and 5990 ports are open and above the `REJECT` line:

```
# iptables -L -n | grep -E "5900|5000"
ACCEPT    udp -- 0.0.0.0/0        0.0.0.0/0
udp dpt:5990
ACCEPT    tcp -- 0.0.0.0/0        0.0.0.0/0
state NEW tcp dpt:5000
ACCEPT    tcp -- 0.0.0.0/0        0.0.0.0/0
state NEW tcp dpt:5990
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with
icmp-host-prohibited
```

b. If these ports are not open, open them.

Find the input chain name, which is reported in the line that appears after `INPUT`:

```
# iptables -L -line numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 RH-Firewall-1-INPUT all -- anywhere anywhere
...
10 REJECT all -- anywhere anywhere reject-with
icmp-host-prohibited
```

Using the line number of the `REJECT` line and the chain name (line `10` and line `1`, respectively, in the step above), insert the onQ ports:

```
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5990 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5000 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -p udp --
dport 5990 -j ACCEPT
```

c. Save and restart iptables.

Afterward, verify that the ports are open and above the `REJECT` line as outlined earlier.

```
# service iptables save
Saving firewall rules to /etc/sysconfig/iptables:
[ OK ]
# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules:
ip_conntrack_netbios_n [ OK ]
```

5. **(Oracle database) Install `RMAN` scripts**.

   If the PN has an Oracle database, install the `RMAN` scripts so that onQ can execute a hot backup of your database as outlined in Back up and restore Oracle 11g database on Linux.

(RHEL 7.0/ESXi) To enroll an agent-less Linux PN:

Use this procedure to enroll an agent-less Linux PN running RHEL 7.0 and that’s being hosted by an ESXi server.

1. **Install the PN proxies**:

   a. Enable `ssh` on the ESXi/ESX server.

   b. Reserve 1 to 3 unique static IP addresses for each PN proxy type (Linux and Windows). The more proxies you configure, the more concurrent backups onQ can perform.

   c. Log on to the HA’s onQ Portal.

   d. Click the **PROTECTION CONFIG** tab > double-plus button (**++**).

      The **Add Protected Nodes via Host** dialog appears.

   e. In the **Server Type** field, select the **ESX Host** radio button.

f. In the **User Name** and **Password** fields, provide the ESXi/ESX host credentials for any user with root privileges.

g. In the Server field, provide either the hostname or the IP address for the ESXi/ESX host, then **GET LIST**.

The onQ Portal queries the virtual machines hosted by the ESXi/ESX server, then displays the inventory.

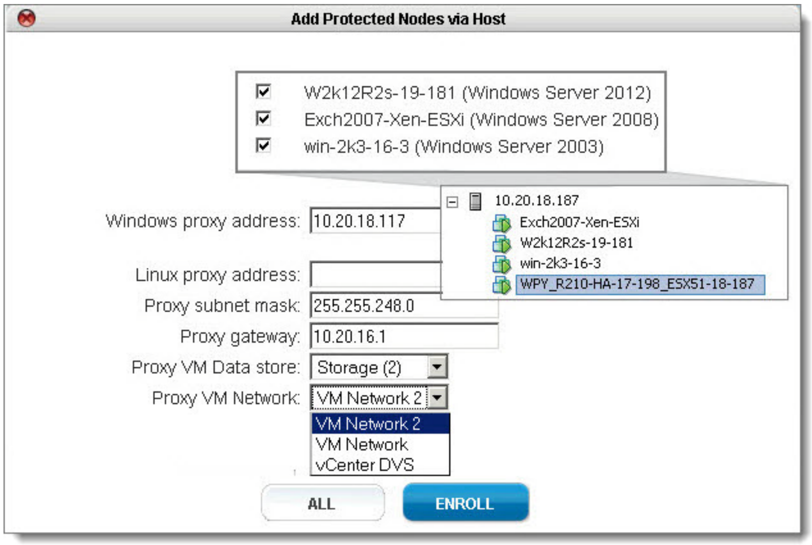
h. In the virtual machine list, select the check boxes (or **ALL** button) for the PNs that you want to enroll.

If an expected virtual machine does not appear in the list, it's likely that the virtual machine does not have VMware Tools installed.

Provide the network properties for each proxy. Use the unique IP addresses that you reserved above.

- **Windows proxy address**. The static IP address that you reserved for the Windows PN proxy.
- **Linux proxy address**. The static IP address that you reserved for the Linux PN proxy.
- **Proxy subnet mask**. The PN proxy's subnet mask.
- **Proxy gateway**. The PN proxy's gateway.
- **Proxy VM Data store**. The directory in which the vm's files are stored.
- **Proxy VM Network**. Your network configuration can include a vCenter-level Distributed Virtual Switches (DVS) or an ESXi host-level virtual switch. When you enroll an ESXi host, all available networks that are visible to that host are listed and available for selection.

In the following example, three Windows PN are being enrolled, so only one static IP address (for the Windows PN proxy `WPY_`<onQhostname>_<ESXhostname>) is needed:



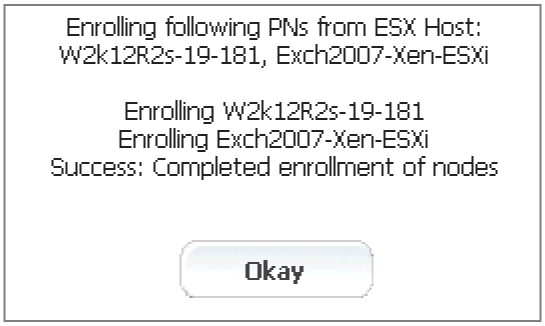
Add Protected Nodes via Host

☑ W2k12R2s-19-181 (Windows Server 2012)
☑ Exch2007-Xen-ESXi (Windows Server 2008)
☑ win-2k3-16-3 (Windows Server 2003)

10.20.18.187
- Exch2007-Xen-ESXi
- W2k12R2s-19-181
- win-2k3-16-3
- WPY_R210-HA-17-198_ESX51-18-187

Windows proxy address: 10.20.18.117
Linux proxy address:
Proxy subnet mask: 255.255.248.0
Proxy gateway: 10.20.16.1
Proxy VM Data store: Storage (2)
Proxy VM Network: VM Network 2

Click the **ENROLL** button, then **OKAY**.



Enrolling following PNs from ESX Host:
W2k12R2s-19-181, Exch2007-Xen-ESXi

Enrolling W2k12R2s-19-181
Enrolling Exch2007-Xen-ESXi
Success: Completed enrollment of nodes

The PNs that you selected appear in the Protected Nodes list; however, they are `unverified` as evidenced by the status in the **PROTECTED NODES** page > **Protection Disabled** column.

i. From the ESXi/ESX host, power on the PN proxies.

j. Activate (aka *verify*) the PNs so that onQ can protect them.

Go to **PROTECTION CONFIG** tab, select the PN, then click the **MODIFY** button.

Specify values for the node parameters, then **SAVE**. The act of saving a PN’s configuration instructs onQ to activate that PN’s configuration. If the PN is a Linux PN, onQ cannot enroll these

XFS mount points automatically, so you must do so now. See Linux Filesystem Format Requirements.

The onQ Portal groups the PNs by ESXi server. If you do not want these PNs in such a group, clear the default **Group Name** field to remove the PNs from this group and place them in the shared pool.

2. **Create the grub boot menu**. In order to boot the RN successfully, the PN needs to prepare the init ram disk image with the required drivers and legacy grub boot menu.

   a. Verify OS version:

   ```
   # cat /etc/redhat-release

   Red Hat Enterprise Linux Server release 7.0
   (Maipo)
   ```

   b. Make sure `ext2`/`ext3`/`ext4` file systems utilities are installed.

   ```
   # rpm -qa | grep e2fsprogs

   e2fsprogs-libs-1.42.9-4.el7.x86_64

   e2fsprogs-1.42.9-4.el7.x86_64
   ```

   If not installed, do so now:

   ```
   # yum install e2fsprogs
   ```

   c. Generate the init ram disk with xen drivers and `ext4` file system modules.

   Print the kernel release:

   ```
   # uname -r
   3.10.0-123.13.2.el7.x86_64
   ```

Where the `3.10.0-123.13.2.el7.x86_64` is the kernel release by default, change it to match PN's kernel release:

```
# cd /boot
# mkdir -p /boot/grub
# dracut --force --filesystems "ext4 ext3"  \
--add-drivers  "xen:vbd xen:vif" \
initramfs-3.10.0-123.13.2.el7xen.x86_64.img
```

d. Verify the legacy grub boot loader:

```
# vi /boot/grub/grub.conf.xvf5
```

Where the `3.10.0-123.13.2.el7.x86_64` is the kernel release by default, change `vmlinuz` and `initramfs` to match PN's kernel release. The kernel parameters are on a single line. Simply copy and paste from following screen.

Where the `root=UUID=855cd484-3852-ee0408c6b590`, the `855cd`... (UUID) is a temporary placeholder and will be replaced by read “`/`”'s UUID during the RN build. Do not make any changes to this parameter.

For example: The contents of `/boot/grub/grub.conf.xvf5`:

```
default=0
timeout=5
title onQ Red Hat Enterprise Linux (3.10.0-123.13.2.el7.x86_64)
root (hd0,0)
kernel /vmlinuz-3.10.0-123.13.2.el7.x86_64 ro root=UUID=855cd484-3852-
4984-b568-ee0408c6b590 plymouth.enable=0 console=hvc0 loglvl=all
cgroup_disable=memory sync_console console_to_ring earlyprintk=xen
nomodeset net.ifnames=0 biosdevname=0 LANG=en_US.UTF-8
initrd /initramfs-3.10.0-123.13.2el7xen.x86_64.img
```

From `/boot`, validate that `vmlinuz-3.10.0-123.13.2.el7.x86_64` and `initramfs-3.10.0-`

`123.13.2.el7xen.x86_64.img` exist in `/boot` folder as shown in the example below:

```
# ls /boot/vmlinuz-3.10.0-123.13.2.el7.x86_64
/boot/vmlinuz-3.10.0-123.13.2.el7.x86_64
# ls /boot/initramfs-3.10.0-
123.13.2.el7xen.x86_64.img
/boot/initramfs-3.10.0-123.13.2.el7xen.x86_64.img
```

3. **Wait for the RN to build, then perform a self-test**.

   Troubleshooting RN Build or Self-test Problems

   Mistakes with the grub boot menu enforcement can prevent the RN from booting. The following list represents the most common errors.

   - Kernel parameters are not on one single line. Some file editors wrap long parameters.
   - You have a typo in `grub.con` or `grub.conf.xvf5` file name.
   - You have a typo in the kernel file name or the initramfs file name, or these files don’t exist.
   - There is a mismatch, on the boot menu, between the kernel versions and the initramfs version. If the kernel's version does not match the contents of initramfs, the RN won't boot.The system could have more than one kernel installed:

     7.0:

     `vmlinuz-3.10.0-123.13.2.el7.x86_64`

     should match

     `initramfs-3.10.0-123.13.2.el7xen.x86_64.img`

     6.x:

     `vmlinuz-2.6.32-279.el6.x86_64`

     should match

     `initramfs-2.6.32-279.el6.x86_64.img`

     5.x:

     `vmlinuz-2.6.18-371.el5xen`

     should match

     `initrd-2.6.18-371.el5xen.img.5`

To find the driver versions packed inside the init ram file system (`initramfs`) of the boot menu: Locate the initramfs and kernel name from the boot menu prepared for the RN (you’ll find it under `/boot)`, then use the following command to peek the contents of initramfs. For example:

RHEL 6.x or 7.0:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-3.10.0-123.el7.x86_64  ro
root=UUID=9002ec24-fb30-4d16-8a78-b352a807e82b
plymouth.enable=0 console=hvc0 loglvl=all
cgroup_disable=memory sync_console
console_to_ring earlyprintk=xen nomodeset net.if-
names=0 biosdevname=0 LANG=en_US.UTF-8
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initramfs-3.10.0-123.el7xen.x86_64.img
# lsinitrd /boot/initramsfs-3.10.0-
123.el7xen.x86_64.img|grep modules
rw-r--r--   1 root     root         1446 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep
-rw-r--r--   1 root     root         2450 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep.bin
-rw-r--r--   1 root     root           52 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.devname
-rw-r--r--   1 root     root        82512 Jun 30
2014 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.order
-rw-r--r--   1 root     root          165 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.softdep
-rw-r--r--   1 root     root        28132 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols
-rw-r--r--   1 root     root        34833 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols.bin
```

RHEL 5.x:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-2.6.18-371.el5xen ro
root=/dev/xvda1 rd_NO_LUKS rd_NO_MD rhgb crashker-
nel=auto rd_NO_LVM
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initrd-2.6.18-371.el5xen.img.5
# zcat /tmp/initrd-2.6.18-371.el5xen.img.5|cpio
-t|grep -E “xen|ext”
16524 blocks
lib/ext3.ko
lib/xennet.ko
lib/xenblk.ko
```

4. **Log on to the PN and open the** following ports on the firewall in order for onQ to communicate with the PN.
   - UDP port `5990`
   - TCP ports `5000` and `5990`

   Firewalld:

   By default, RHEL 7.0 has introduced a new firewall service, a dynamic firewall daemon known as `firewalld`, instead of iptables service by default; however, the traditional iptables service is supported if installed. For details, see the Red Hat Linux 7 Security Guide. If you choose to disable firewalld, there is no need to configure firewalld firewall rules: simply skip this procedure.

   `firewalld` daemon and service and iptables service are using iptables commands to configure the netfilter in the kernel to separate and filter the network traffic. `firewalld` stores it in various XML files in `/usr/lib/firewalld/` and `/etc/firewalld/`.

   The firewalld firewall defines how *networks zones* can be used to separate networks into different zones. Based on the level of trust, you can decide to place devices and traffic within a particular network zone. Each mutable network zone can have a different combination of firewall rules.

   a. Verify that firewalld is in a running state.

b. Check the service status:

```
[root@RHEL70x64-17-167 services]# systemctl status
firewalld.service
firewalld.service - firewalld - dynamic firewall
daemon
Loaded: loaded (/usr/lib/systemd/system/fire-
walld.service; disabled)
Active: inactive (dead)
```

c. Enable the service, if not already enabled:

```
[root@RHEL70x64-17-167 services]# systemctl enable
firewalld
ln -s '/usr/lib/systemd/system/firewalld.service'
'/etc/systemd/system/dbusorg.edorapro-
ject.FirewallD1.service'
ln -s '/usr/lib/systemd/system/firewalld.service'
'/etc/systemd/system
/basic.target.wants/firewalld.service'
```

d. Start the service, if not already running:

```
[root@RHEL70x64-17-167 services]# systemctl start
firewalld
```

e. On the PN, find the network interface that is used to communicate with onQ. In this example, that NIC is `ens32`.

```
[root@RHEL70x64-17-167 services]# ifconfig
ens32: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.20.17.167 netmask 255.255.248.0 broadcast 10.20.23.255
inet6 fe80::250:56ff:fe9d:2121 prefixlen 64 scopeid 0x20<link>
ether 00:50:56:9d:21:21 txqueuelen 1000 (Ethernet)
RX packets 7115713 bytes 476287831 (454.2 MiB)
RX errors 0 dropped 149791 overruns 0 frame 0
TX packets 924966 bytes 1305413839 (1.2 GiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 0 (Local Loopback)
RX packets 10 bytes 980 (980.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 10 bytes 980 (980.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

f. For the network interface that you identified above, find the network interface's network zone. In this example, the network zone is `work`.

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-zone-of-interface=ens32
work
```

Determine your default zone. In the following example, the default zone is `Public`.

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-default-zone
public
```

g. Associate the zone(s) with the following firewall rules. The same rules can be applied to many zones as needed. In the following example, dcrm-node service is associated with `work` zone for `ens32`. The `dcrm-node.xml` is located at `/usr/lib/firewalld/services`.

```
[root@RHEL70x64-17-167 services]# firewall-cmd --add-service=dcrm-node --permanent --zone=work
success
```

h. Activate the latest firewall rules:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --reload
success
```

Now the PN can communicate with onQ.

i. Set up the rule for RN on the PN site.

The RN will be equipped with `eth0` interface, so apply the rules to `eth0` interface's zone if different from PN's zone. The PN might not have `eth0` interface; in such a case, the RN's `eth0` will be in the default zone.

Find `eth0` network interface's network zone. In this example, it is *not* set:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-zone-of-interface=eth0
no zone
```

Determine your default zone. In this example default zone is `Public`. Since `eth0` has no zone dcm-node is associated with `Public` zone:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --get-default-zone
public
```

j. Associate the zone(s) with the following firewall rules. The same rules can be applied to many zones as needed:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --add-service=dcrm-node --permanent --zone=public
success
```

k. Active the latest firewall rules:

```
[root@RHEL70x64-17-167 services]# firewall-cmd --reload
success
```

Now the RN can communicate with onQ, mainly for self-tests.

l. Confirm the firewall rules. The public zone and work zone have TCP ports (5000/5990) and UDP port 5990 opened in this case.

```
[root@RHEL70x64-17-167 services]# iptables -L -n
Chain IN_public (2 references)
target prot opt source destination
IN_public_log all -- 0.0.0.0/0 0.0.0.0/0
IN_public_deny all -- 0.0.0.0/0 0.0.0.0/0
IN_public_allow all -- 0.0.0.0/0 0.0.0.0/0
Chain IN_public_allow (1 references)
target prot opt source destination
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5000 ct-
state NEW
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 ct-
state NEW
Chain IN_work (0 references)
target prot opt source destination
IN_work_log all -- 0.0.0.0/0 0.0.0.0/0
IN_work_deny all -- 0.0.0.0/0 0.0.0.0/0
IN_work_allow all -- 0.0.0.0/0 0.0.0.0/0
Chain IN_work_allow (1 references)
target prot opt source destination
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:631 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5000 ct-
state NEW
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:5990 ct-
state NEW
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:22 ct-
state NEW
```

iptables:

a. Verify that udp 5990 and tcp 5000 and 5990 ports are open and above the `REJECT` line:

```
# iptables -L -n | grep -E "5900|5000"
ACCEPT   udp -- 0.0.0.0/0        0.0.0.0/0
udp dpt:5990
ACCEPT   tcp -- 0.0.0.0/0        0.0.0.0/0
state NEW tcp dpt:5000
ACCEPT   tcp -- 0.0.0.0/0        0.0.0.0/0
state NEW tcp dpt:5990
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with
icmp-host-prohibited
```

b. If these ports are not open, open them.

Find the input chain name, which is reported in the line that appears after `INPUT`:

```
# iptables -L -line numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 RH-Firewall-1-INPUT all -- anywhere anywhere
...
10 REJECT all -- anywhere anywhere reject-with
icmp-host-prohibited
```

Using the line number of the `REJECT` line and the chain name (line `10` and line `1`, respectively, in the step above), insert the onQ ports:

```
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5990 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5000 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -p udp --
dport 5990 -j ACCEPT
```

c. Save and restart iptables.

Afterward, verify that the ports are open and above the `REJECT` line as outlined earlier.

```
# service iptables save
Saving firewall rules to /etc/sysconfig/iptables:
[ OK ]
# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules:
ip_conntrack_netbios_n [ OK ]
```

5. **(Oracle database) Install `RMAN` scripts**.

   If the PN has an Oracle database, install the `RMAN` scripts so that onQ can execute a hot backup of your database as outlined in Back up and restore Oracle 11g database on Linux.

(RHEL 6.x/vCenter) To enroll an agent-less Linux PN:

Use this procedure to enroll an agent-less Linux PN running RHEL 6.x and that’s being managed by vCenter.

1. **Install the PN proxies**:

   a. Enable `ssh` on each ESXi/ESX server in the vMotion cluster.

   b. Reserve 1 to 3 unique static IP addresses for each PN proxy type (Linux and Windows). The more proxies you configure, the more concurrent backups onQ can perform.

   c. Log on to the HA’s onQ Portal.

   d. Click the **PROTECTION CONFIG** tab > double-plus button (**++**).

      The **Add Protected Nodes via Host** dialog appears.

   e. In the **Server Type** field, select the **vCenter** radio button.

f. Provide the vCenter credentials for any user with root privileges and either the hostname or the IP address for vCenter, then **GET LIST**. The **Add Protected Nodes via vCenter** dialog appears.

The onQ Portal queries the virtual machines managed by vCenter, then displays the inventory.

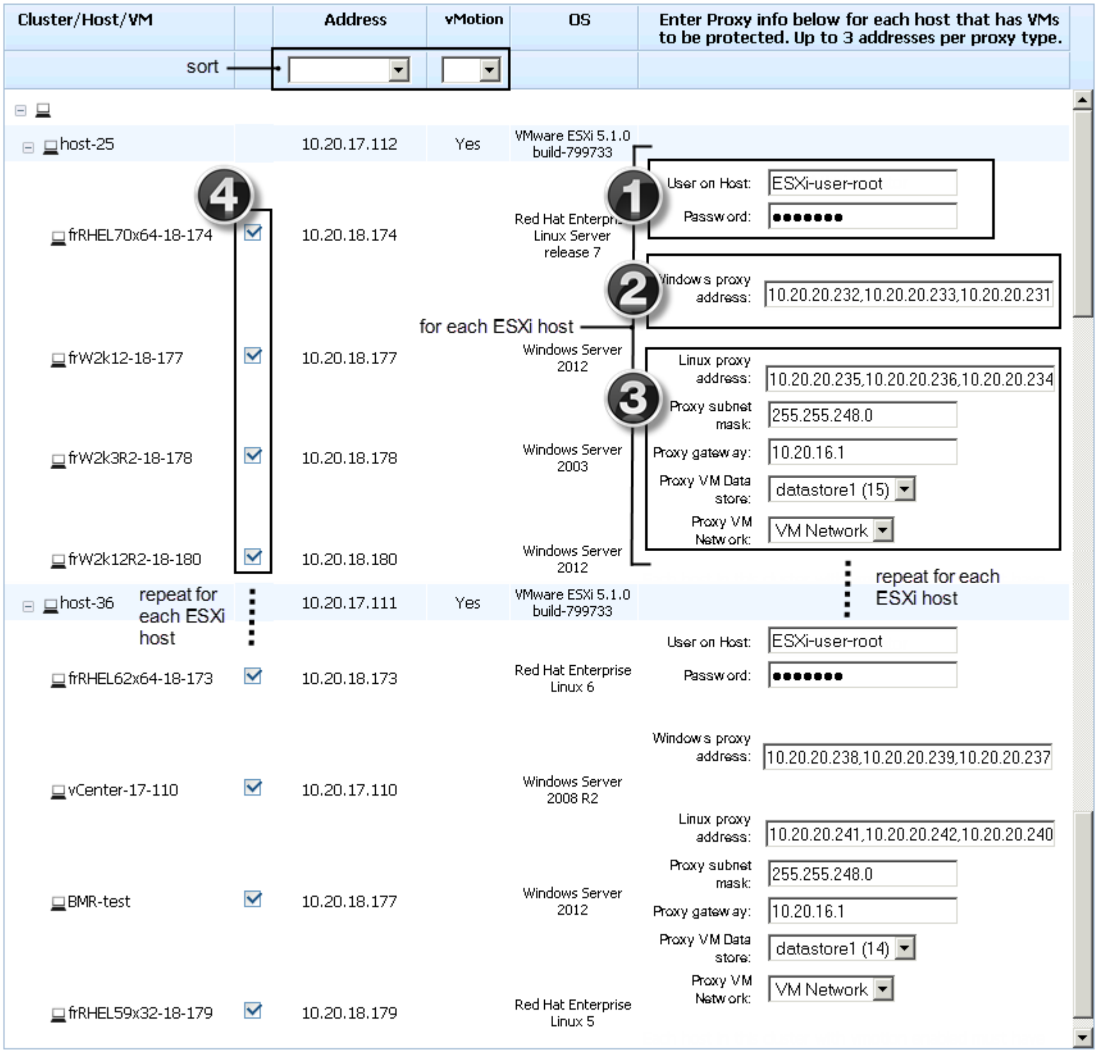
g. Provide ESXi host credentials for any user with root privileges, specify proxy information for each proxy type, and select the check boxes for the PNs that you want to enroll.

If an expected virtual machine does not appear in the list, it’s likely that the virtual machine does not have VMware Tools installed.

Provide the network properties for each proxy. Use the unique IP address(es) that you reserved above. If more than one IP per proxy type, provide a comma-separated list.

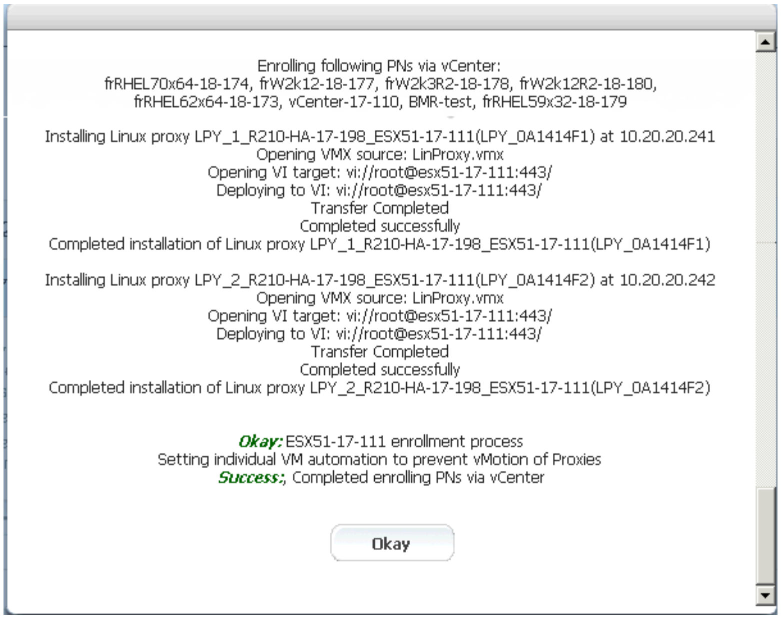
- **Windows proxy address**. The static IP address that you reserved for the Windows PN proxy.
- **Linux proxy address**. The static IP address that you reserved for the Linux PN proxy.
- **Proxy subnet mask**. The PN proxy’s subnet mask.
- **Proxy gateway**. The PN proxy’s gateway.
- **Proxy VM Data store**. The directory in which the vm’s files are stored.
- **Proxy VM Network**. Your network configuration can include a vCenter-level Distributed Virtual Switches (DVS) or an ESXi host-level virtual switch. When you enroll an ESXi host, all available networks that are visible to that host are listed and available for selection.

In the following example, all PNs on all ESXi hosts in the vMotion cluster are being enrolled and using the maximum number of proxies allowed for each proxy type:



Cluster/Host/VM		Address	vMotion	OS	Enter Proxy info below for each host that has VMs to be protected. Up to 3 addresses per proxy type.
host-25		10.20.17.112	Yes	VMware ESXi 5.1.0 build-799733	User on Host: ESXi-user-root Password: ●●●●●●● Windows proxy address: 10.20.20.232,10.20.20.233,10.20.20.231 Linux proxy address: 10.20.20.235,10.20.20.236,10.20.20.234 Proxy subnet mask: 255.255.248.0 Proxy gateway: 10.20.16.1 Proxy VM Data store: datastore1 (15) Proxy VM Network: VM Network
frRHEL70x64-18-174	☑	10.20.18.174		Red Hat Enterpr Linux Server release 7	
frW2k12-18-177	☑	10.20.18.177		Windows Server 2012	
frW2k3R2-18-178	☑	10.20.18.178		Windows Server 2003	
frW2k12R2-18-180	☑	10.20.18.180		Windows Server 2012	
host-36		10.20.17.111	Yes	VMware ESXi 5.1.0 build-799733	User on Host: ESXi-user-root Password: ●●●●●●● Windows proxy address: 10.20.20.238,10.20.20.239,10.20.20.237 Linux proxy address: 10.20.20.241,10.20.20.242,10.20.20.240 Proxy subnet mask: 255.255.248.0 Proxy gateway: 10.20.16.1 Proxy VM Data store: datastore1 (14) Proxy VM Network: VM Network
frRHEL62x64-18-173	☑	10.20.18.173		Red Hat Enterprise Linux 6	
vCenter-17-110	☑	10.20.17.110		Windows Server 2008 R2	
BMR-test	☑	10.20.18.177		Windows Server 2012	
frRHEL59x32-18-179	☑	10.20.18.179		Red Hat Enterprise Linux 5	

Click the **ENROLL** button, then **OKAY**.



```
Enrolling following PNs via vCenter:
frRHEL70x64-18-174, frW2k12-18-177, frW2k3R2-18-178, frW2k12R2-18-180,
frRHEL62x64-18-173, vCenter-17-110, BMR-test, frRHEL59x32-18-179

Installing Linux proxy LPY_1_R210-HA-17-198_ESX51-17-111(LPY_0A1414F1) at 10.20.20.241
Opening VMX source: LinProxy.vmx
Opening VI target: vi://root@esx51-17-111:443/
Deploying to VI: vi://root@esx51-17-111:443/
Transfer Completed
Completed successfully
Completed installation of Linux proxy LPY_1_R210-HA-17-198_ESX51-17-111(LPY_0A1414F1)

Installing Linux proxy LPY_2_R210-HA-17-198_ESX51-17-111(LPY_0A1414F2) at 10.20.20.242
Opening VMX source: LinProxy.vmx
Opening VI target: vi://root@esx51-17-111:443/
Deploying to VI: vi://root@esx51-17-111:443/
Transfer Completed
Completed successfully
Completed installation of Linux proxy LPY_2_R210-HA-17-198_ESX51-17-111(LPY_0A1414F2)


Okay: ESX51-17-111 enrollment process
Setting individual VM automation to prevent vMotion of Proxies
Success:; Completed enrolling PNs via vCenter
```

The PNs that you selected appear in the Protected Nodes list; however, they are `unverified` as evidenced by the status in the **PROTECTED NODES** page > **Protection Disabled** column.

h. From the ESXi/ESX host, power on the PN proxies.

i. Activate (aka *verify*) the PNs so that onQ can protect them.

Go to **PROTECTION CONFIG** tab, select the PN, then click the **MODIFY** button.

Specify values for the node parameters, then **SAVE**. The act of saving a PN's configuration instructs onQ to activate that PN's configuration. If the PN is a Linux PN, onQ cannot enroll these XFS mount points automatically, so you must do so now. See Linux Filesystem Format Requirements.

The onQ Portal groups the PNs by ESXi server. If you do not want these PNs in such a group, clear the default **Group Name** field to remove the PNs from this group and place them in the shared pool.

1.

2. Copy and modify `/boot/grub/menu.lst`:

```
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux (2.6.32-279.el6.x86_64)
    root (hd0,0)
    kernel /vmlinuz-2.6.32-279.el6.x86_64 ro
root=/dev/mapper/VolGroup-lv_root rd_NO_LUKS
LANG=en_US.UTF-8 rd_NO_MD rd_LVM_LV=VolGroup/lv_swap
SYSFONT=latarcyrheb-sun16 crashkernel=auto
rd_LVM_LV=VolGroup/lv_root  KEYBOARDTYPE=pc KEYTABLE=us
rd_NO_DM rhgb quiet
    initrd /initramfs-2.6.32-279.el6.x86_64.img
```

Note: If you want a custom boot menu, create a `/boot/grub/grub.conf.xvf5` file. If `.xvf1` thru `.xvf4` exist, delete them because those files have a higher priority than `.xvf5`.

3. **Wait for the RN to build, then perform a self-test**.

   Troubleshooting RN Build or Self-test Problems

   Mistakes with the grub boot menu enforcement can prevent the RN from booting. The following list represents the most common errors.

   - Kernel parameters are not on one single line. Some file editors wrap long parameters.
   - You have a typo in `grub.con` or `grub.conf.xvf5` file name.
   - You have a typo in the kernel file name or the initramfs file name, or these files don't exist.
   - There is a mismatch, on the boot menu, between the kernel versions and the initramfs version. If the kernel's version does not match the contents of initramfs, the RN won't boot.The system could have more than one kernel installed:

     7.0:

     `vmlinuz-3.10.0-123.13.2.el7.x86_64`

     should match

     `initramfs-3.10.0-123.13.2.el7xen.x86_64.img`

6.x:

```
vmlinuz-2.6.32-279.el6.x86_64
```

should match

```
initramfs-2.6.32-279.el6.x86_64.img
```

5.x:

```
vmlinuz-2.6.18-371.el5xen
```

should match

```
initrd-2.6.18-371.el5xen.img.5
```

To find the driver versions packed inside the init ram file system (`initramfs`) of the boot menu: Locate the initramfs and kernel name from the boot menu prepared for the RN (you'll find it under `/boot)`, then use the following command to peek the contents of initramfs. For example:

RHEL 6.x or 7.0:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-3.10.0-123.el7.x86_64  ro
root=UUID=9002ec24-fb30-4d16-8a78-b352a807e82b
plymouth.enable=0 console=hvc0 loglvl=all
cgroup_disable=memory sync_console
console_to_ring earlyprintk=xen nomodeset net.if-
names=0 biosdevname=0 LANG=en_US.UTF-8
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initramfs-3.10.0-123.el7xen.x86_64.img
# lsinitrd /boot/initramsfs-3.10.0-
123.el7xen.x86_64.img|grep modules
rw-r--r--   1 root     root         1446 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep
-rw-r--r--   1 root     root         2450 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep.bin
-rw-r--r--   1 root     root           52 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.devname
-rw-r--r--   1 root     root        82512 Jun 30
2014 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.order
-rw-r--r--   1 root     root          165 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.softdep
-rw-r--r--   1 root     root        28132 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols
-rw-r--r--   1 root     root        34833 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols.bin
```

RHEL 5.x:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-2.6.18-371.el5xen ro
root=/dev/xvda1 rd_NO_LUKS rd_NO_MD rhgb crashker-
nel=auto rd_NO_LVM
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initrd-2.6.18-371.el5xen.img.5
# zcat /tmp/initrd-2.6.18-371.el5xen.img.5|cpio
-t|grep -E “xen|ext”
16524 blocks
lib/ext3.ko
lib/xennet.ko
lib/xenblk.ko
```

4. **Log on to the PN and open the** following ports on the firewall in order for onQ to communicate with the PN.
   - UDP port `5990`
   - TCP ports `5000` and `5990`

1.

   iptables:

   a. Verify that udp 5990 and tcp 5000 and 5990 ports are open and above the `REJECT` line:

```
# iptables -L -n | grep -E "5900|5000"
ACCEPT   udp -- 0.0.0.0/0       0.0.0.0/0
udp dpt:5990
ACCEPT   tcp -- 0.0.0.0/0       0.0.0.0/0
state NEW tcp dpt:5000
ACCEPT   tcp -- 0.0.0.0/0       0.0.0.0/0
state NEW tcp dpt:5990
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with
icmp-host-prohibited
```

   b. If these ports are not open, open them.

Find the input chain name, which is reported in the line that appears after `INPUT`:

```
# iptables -L -line numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 RH-Firewall-1-INPUT all -- anywhere anywhere
...
10 REJECT all -- anywhere anywhere reject-with
icmp-host-prohibited
```

Using the line number of the `REJECT` line and the chain name (line `10` and line `1`, respectively, in the step above), insert the onQ ports:

```
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5990 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5000 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -p udp --
dport 5990 -j ACCEPT
```

c. Save and restart iptables.

Afterward, verify that the ports are open and above the `REJECT` line as outlined earlier.

```
# service iptables save
Saving firewall rules to /etc/sysconfig/iptables:
[ OK ]
# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules:
ip_conntrack_netbios_n [ OK ]
```

2. (Oracle database) Install `RMAN` scripts.

If the PN has an Oracle database, install the RMAN scripts so that onQ can execute a hot backup of your database as outlined in Back up and restore Oracle 11g database on Linux.

1.

(RHEL 6.x/ESXi) To enroll an agent-less Linux PN:

Use this procedure to enroll an agent-less Linux PN running RHEL 6.x and that's being hosted by an ESXi server.

1. **Install the PN proxies**:
   a. Enable `ssh` on the ESXi/ESX server.
   b. Reserve 1 to 3 unique static IP addresses for each PN proxy type (Linux and Windows). The more proxies you configure, the more concurrent backups onQ can perform.
   c. Log on to the HA's onQ Portal.
   d. Click the **PROTECTION CONFIG** tab > double-plus button (**++**).

      The **Add Protected Nodes via Host** dialog appears.
   e. In the **Server Type** field, select the **ESX Host** radio button.
   f. In the **User Name** and **Password** fields, provide the ESXi/ESX host credentials for any user with root privileges.
   g. In the Server field, provide either the hostname or the IP address for the ESXi/ESX host, then **GET LIST**.

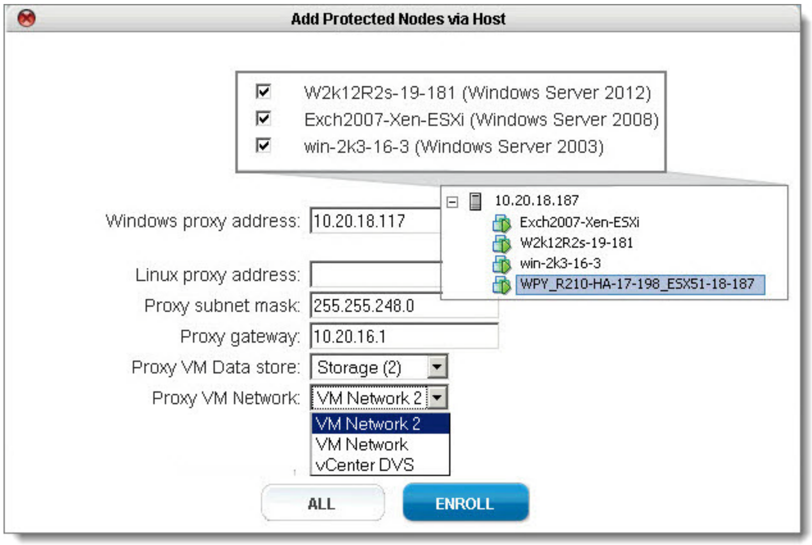
      The onQ Portal queries the virtual machines hosted by the ESXi/ESX server, then displays the inventory.
   h. In the virtual machine list, select the check boxes (or **ALL** button) for the PNs that you want to enroll.

      If an expected virtual machine does not appear in the list, it's likely that the virtual machine does not have VMware Tools installed.

      Provide the network properties for each proxy. Use the unique IP addresses that you reserved above.
      - **Windows proxy address**. The static IP address that you reserved for the Windows PN proxy.
      - **Linux proxy address**. The static IP address that you reserved for the Linux PN proxy.

- **Proxy subnet mask**. The PN proxy's subnet mask.
- **Proxy gateway**. The PN proxy's gateway.
- **Proxy VM Data store**. The directory in which the vm's files are stored.
- **Proxy VM Network**. Your network configuration can include a vCenter-level Distributed Virtual Switches (DVS) or an ESXi host-level virtual switch. When you enroll an ESXi host, all available networks that are visible to that host are listed and available for selection.

In the following example, three Windows PN are being enrolled, so only one static IP address (for the Windows PN proxy `WPY_`<onQhostname>_<ESXhostname>) is needed:



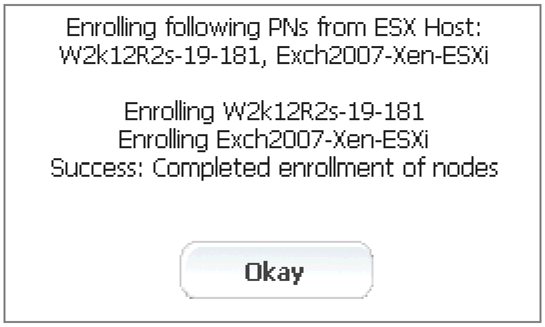
Add Protected Nodes via Host

☑ W2k12R2s-19-181 (Windows Server 2012)
☑ Exch2007-Xen-ESXi (Windows Server 2008)
☑ win-2k3-16-3 (Windows Server 2003)

10.20.18.187
Exch2007-Xen-ESXi
W2k12R2s-19-181
win-2k3-16-3
WPY_R210-HA-17-198_ESX51-18-187

Windows proxy address: 10.20.18.117
Linux proxy address:
Proxy subnet mask: 255.255.248.0
Proxy gateway: 10.20.16.1
Proxy VM Data store: Storage (2)
Proxy VM Network: VM Network 2

Click the **ENROLL** button, then **OKAY**.



Enrolling following PNs from ESX Host:
W2k12R2s-19-181, Exch2007-Xen-ESXi

Enrolling W2k12R2s-19-181
Enrolling Exch2007-Xen-ESXi
Success: Completed enrollment of nodes

The PNs that you selected appear in the Protected Nodes list; however, they are `unverified` as evidenced by the status in the **PROTECTED NODES** page > **Protection Disabled** column.

i. From the ESXi/ESX host, power on the PN proxies.

j. Activate (aka *verify*) the PNs so that onQ can protect them.

Go to **PROTECTION CONFIG** tab, select the PN, then click the **MODIFY** button.

Specify values for the node parameters, then **SAVE**. The act of saving a PN's configuration instructs onQ to activate that PN's configuration. If the PN is a Linux PN, onQ cannot enroll these XFS mount points automatically, so you must do so now. See Linux Filesystem Format Requirements.

The onQ Portal groups the PNs by ESXi server. If you do not want these PNs in such a group, clear the default **Group Name** field to remove the PNs from this group and place them in the shared pool.

1.

2. Copy and modify `/boot/grub/menu.lst`:

```
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title Red Hat Enterprise Linux (2.6.32-279.el6.x86_64)
    root (hd0,0)
    kernel /vmlinuz-2.6.32-279.el6.x86_64 ro 
root=/dev/mapper/VolGroup-lv_root rd_NO_LUKS 
LANG=en_US.UTF-8 rd_NO_MD rd_LVM_LV=VolGroup/lv_swap 
SYSFONT=latarcyrheb-sun16 crashkernel=auto 
rd_LVM_LV=VolGroup/lv_root  KEYBOARDTYPE=pc KEYTABLE=us 
rd_NO_DM rhgb quiet
    initrd /initramfs-2.6.32-279.el6.x86_64.img
```

Note: If you want a custom boot menu, create a `/boot/grub/grub.conf.xvf5` file. If `.xvf1` thru `.xvf4` exist, delete them because those files have a higher priority than `.xvf5`.

3. Wait for the RN to build, then perform a self-test.

Troubleshooting RN Build or Self-test Problems

Mistakes with the grub boot menu enforcement can prevent the RN from booting. The following list represents the most common errors.

- Kernel parameters are not on one single line. Some file editors wrap long parameters.
- You have a typo in `grub.con` or `grub.conf.xvf5` file name.
- You have a typo in the kernel file name or the initramfs file name, or these files don't exist.
- There is a mismatch, on the boot menu, between the kernel versions and the initramfs version. If the kernel's version does not match the contents of initramfs, the RN won't boot.The system could have more than one kernel installed:

  7.0:

  `vmlinuz-3.10.0-123.13.2.el7.x86_64`

  should match

  `initramfs-3.10.0-123.13.2.el7xen.x86_64.img`

  6.x:

  `vmlinuz-2.6.32-279.el6.x86_64`

  should match

  `initramfs-2.6.32-279.el6.x86_64.img`

  5.x:

  `vmlinuz-2.6.18-371.el5xen`

  should match

  `initrd-2.6.18-371.el5xen.img.5`

  To find the driver versions packed inside the init ram file system (`initramfs`) of the boot menu: Locate the initramfs and kernel name from the boot menu prepared for the RN (you'll find it under `/boot)`, then use the following command to peek the contents of initramfs. For example:

RHEL 6.x or 7.0:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-3.10.0-123.el7.x86_64  ro
root=UUID=9002ec24-fb30-4d16-8a78-b352a807e82b
plymouth.enable=0 console=hvc0 loglvl=all
cgroup_disable=memory sync_console
console_to_ring earlyprintk=xen nomodeset net.if-
names=0 biosdevname=0 LANG=en_US.UTF-8
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initramfs-3.10.0-123.el7xen.x86_64.img
# lsinitrd /boot/initramsfs-3.10.0-
123.el7xen.x86_64.img|grep modules
rw-r--r--   1 root     root         1446 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep
-rw-r--r--   1 root     root         2450 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.dep.bin
-rw-r--r--   1 root     root           52 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.devname
-rw-r--r--   1 root     root       82512 Jun 30
2014 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.order
-rw-r--r--   1 root     root          165 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.softdep
-rw-r--r--   1 root     root        28132 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols
-rw-r--r--   1 root     root        34833 Jan 14
07:06 usr/lib/modules/3.10.0-123.el7.x86_64/mod-
ules.symbols.bin
```

RHEL 5.x:

```
# grep kernel /boot/grub/grub.conf.xvf5
kernel /vmlinuz-2.6.18-371.el5xen ro
root=/dev/xvda1 rd_NO_LUKS rd_NO_MD rhgb crashker-
nel=auto rd_NO_LVM
# grep initrd /boot/grub/grub.conf.xvf5
initrd /initrd-2.6.18-371.el5xen.img.5
# zcat /tmp/initrd-2.6.18-371.el5xen.img.5|cpio
-t|grep -E “xen|ext”
16524 blocks
lib/ext3.ko
lib/xennet.ko
lib/xenblk.ko
```

4. **Log on to the PN and open the** following ports on the firewall in order for onQ to communicate with the PN.
   - UDP port `5990`
   - TCP ports `5000` and `5990`

1.

   iptables:

   a. Verify that udp 5990 and tcp 5000 and 5990 ports are open and above the `REJECT` line:

```
# iptables -L –n | grep -E "5900|5000"
ACCEPT   udp -- 0.0.0.0/0       0.0.0.0/0
udp dpt:5990
ACCEPT   tcp -- 0.0.0.0/0       0.0.0.0/0
state NEW tcp dpt:5000
ACCEPT   tcp -- 0.0.0.0/0       0.0.0.0/0
state NEW tcp dpt:5990
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with
icmp-host-prohibited
```

   b. If these ports are not open, open them.

Find the input chain name, which is reported in the line that appears after `INPUT`:

```
# iptables -L -line numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 RH-Firewall-1-INPUT all -- anywhere anywhere
...
10 REJECT all -- anywhere anywhere reject-with
icmp-host-prohibited
```

Using the line number of the `REJECT` line and the chain name (line `10` and line `1`, respectively, in the step above), insert the onQ ports:

```
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5990 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5000 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -p udp --
dport 5990 -j ACCEPT
```

c. Save and restart iptables.

Afterward, verify that the ports are open and above the `REJECT` line as outlined earlier.

```
# service iptables save
Saving firewall rules to /etc/sysconfig/iptables:
[ OK ]
# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules:
ip_conntrack_netbios_n [ OK ]
```

2. (Oracle database) Install `RMAN` scripts.

If the PN has an Oracle database, install the `RMAN` scripts so that onQ can execute a hot backup of your database as outlined in Back up and restore Oracle 11g database on Linux.

1.

(RHEL 5.x/vCenter) To enroll an agent-less Linux PN:

Use this procedure to enroll an agent-less Linux PN running RHEL 5.x and that's being managed by vCenter.

1. **Install the PN proxies**:
   - **a.** Enable `ssh` on each ESXi/ESX server in the vMotion cluster.
   - **b.** Reserve 1 to 3 unique static IP addresses for each PN proxy type (Linux and Windows). The more proxies you configure, the more concurrent backups onQ can perform.
   - **c.** Log on to the HA's onQ Portal.
   - **d.** Click the **PROTECTION CONFIG** tab > double-plus button (**++**).

     The **Add Protected Nodes via Host** dialog appears.
   - **e.** In the **Server Type** field, select the **vCenter** radio button.
   - **f.** Provide the vCenter credentials for any user with root privileges and either the hostname or the IP address for vCenter, then **GET LIST**. The **Add Protected Nodes via vCenter** dialog appears.

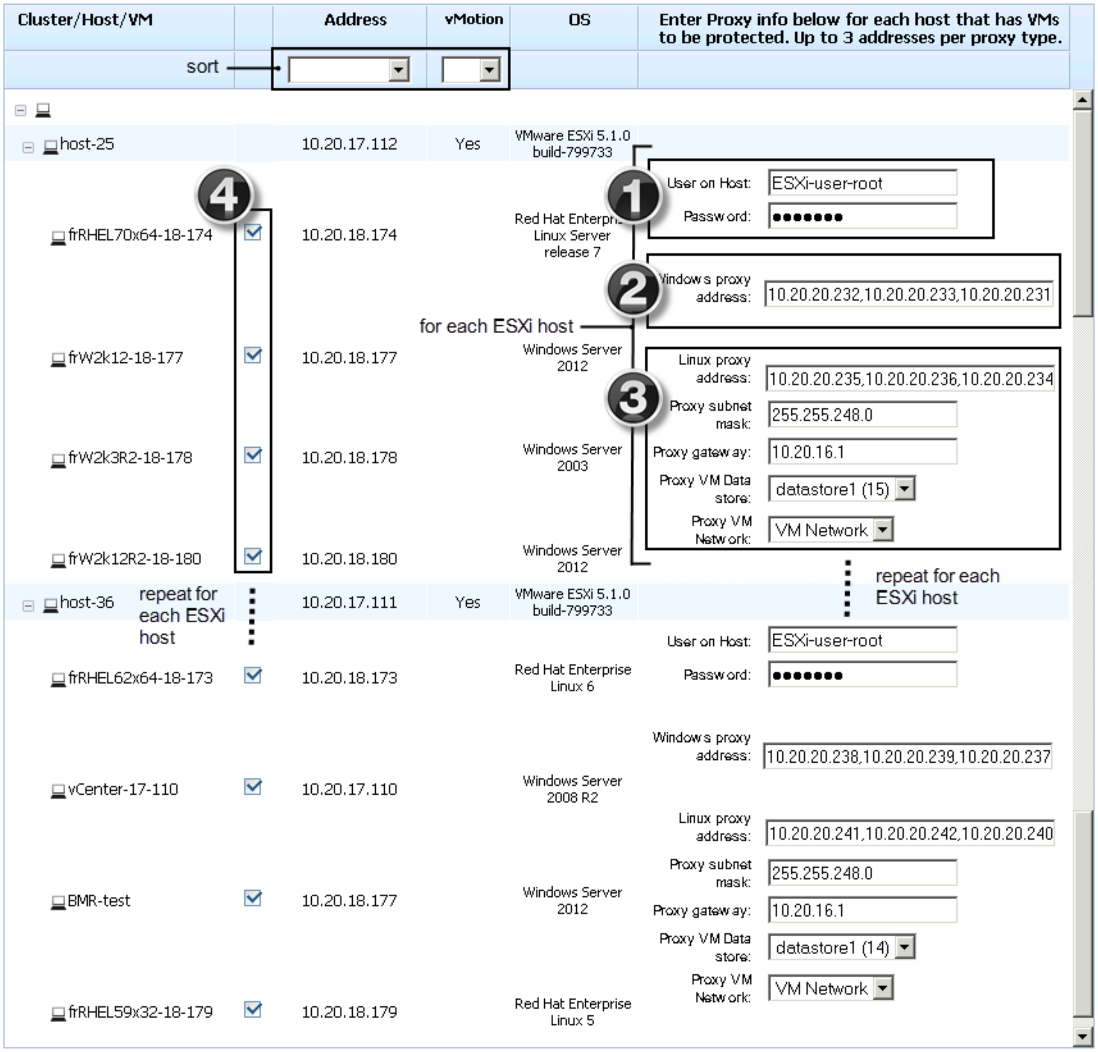
     The onQ Portal queries the virtual machines managed by vCenter, then displays the inventory.
   - **g.** Provide ESXi host credentials for any user with root privileges, specify proxy information for each proxy type, and select the check boxes for the PNs that you want to enroll.

     If an expected virtual machine does not appear in the list, it's likely that the virtual machine does not have VMware Tools installed.

     Provide the network properties for each proxy. Use the unique IP address(es) that you reserved above. If more than one IP per proxy type, provide a comma-separated list.
     - **Windows proxy address**. The static IP address that you reserved for the Windows PN proxy.
     - **Linux proxy address**. The static IP address that you reserved for the Linux PN proxy.

- **Proxy subnet mask**. The PN proxy's subnet mask.
- **Proxy gateway**. The PN proxy's gateway.
- **Proxy VM Data store**. The directory in which the vm's files are stored.
- **Proxy VM Network**. Your network configuration can include a vCenter-level Distributed Virtual Switches (DVS) or an ESXi host-level virtual switch. When you enroll an ESXi host, all available networks that are visible to that host are listed and available for selection.

In the following example, all PNs on all ESXi hosts in the vMotion cluster are being enrolled and using the maximum number of proxies allowed for each proxy type:



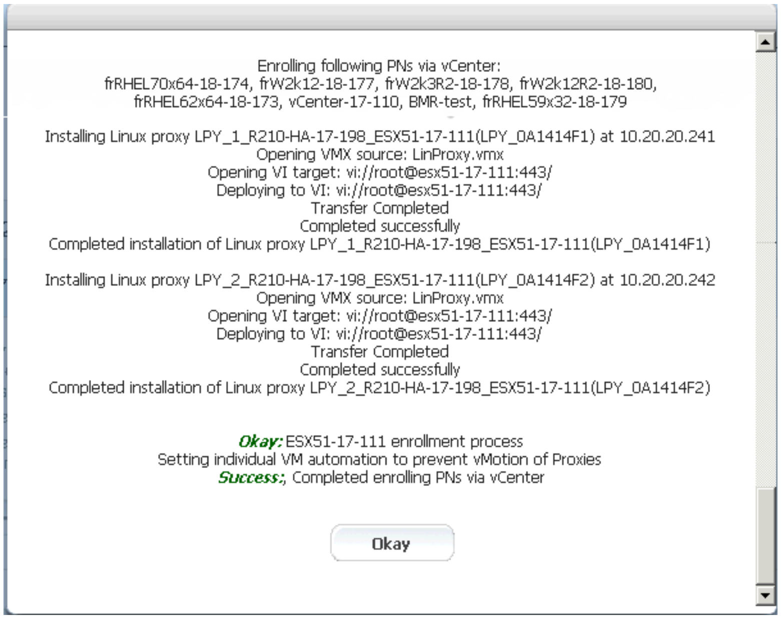
Cluster/Host/VM		Address	vMotion	OS
host-25		10.20.17.112	Yes	VMware ESXi 5.1.0 build-799733
frRHEL70x64-18-174	☑	10.20.18.174		Red Hat Enterpr... Linux Server release 7
frW2k12-18-177	☑	10.20.18.177		Windows Server 2012
frW2k3R2-18-178	☑	10.20.18.178		Windows Server 2003
frW2k12R2-18-180	☑	10.20.18.180		Windows Server 2012
host-36		10.20.17.111	Yes	VMware ESXi 5.1.0 build-799733
frRHEL62x64-18-173	☑	10.20.18.173		Red Hat Enterprise Linux 6
vCenter-17-110	☑	10.20.17.110		Windows Server 2008 R2
BMR-test	☑	10.20.18.177		Windows Server 2012
frRHEL59x32-18-179	☑	10.20.18.179		Red Hat Enterprise Linux 5

Enter Proxy info below for each host that has VMs to be protected. Up to 3 addresses per proxy type.

host-25:
User on Host: ESXi-user-root
Password: •••••••
Windows proxy address: 10.20.20.232,10.20.20.233,10.20.20.231
Linux proxy address: 10.20.20.235,10.20.20.236,10.20.20.234
Proxy subnet mask: 255.255.248.0
Proxy gateway: 10.20.16.1
Proxy VM Data store: datastore1 (15)
Proxy VM Network: VM Network

host-36:
User on Host: ESXi-user-root
Password: •••••••
Windows proxy address: 10.20.20.238,10.20.20.239,10.20.20.237
Linux proxy address: 10.20.20.241,10.20.20.242,10.20.20.240
Proxy subnet mask: 255.255.248.0
Proxy gateway: 10.20.16.1
Proxy VM Data store: datastore1 (14)
Proxy VM Network: VM Network

Click the **ENROLL** button, then **OKAY**.



```
Enrolling following PNs via vCenter:
frRHEL70x64-18-174, frW2k12-18-177, frW2k3R2-18-178, frW2k12R2-18-180,
frRHEL62x64-18-173, vCenter-17-110, BMR-test, frRHEL59x32-18-179

Installing Linux proxy LPY_1_R210-HA-17-198_ESX51-17-111(LPY_0A1414F1) at 10.20.20.241
Opening VMX source: LinProxy.vmx
Opening VI target: vi://root@esx51-17-111:443/
Deploying to VI: vi://root@esx51-17-111:443/
Transfer Completed
Completed successfully
Completed installation of Linux proxy LPY_1_R210-HA-17-198_ESX51-17-111(LPY_0A1414F1)

Installing Linux proxy LPY_2_R210-HA-17-198_ESX51-17-111(LPY_0A1414F2) at 10.20.20.242
Opening VMX source: LinProxy.vmx
Opening VI target: vi://root@esx51-17-111:443/
Deploying to VI: vi://root@esx51-17-111:443/
Transfer Completed
Completed successfully
Completed installation of Linux proxy LPY_2_R210-HA-17-198_ESX51-17-111(LPY_0A1414F2)

Okay: ESX51-17-111 enrollment process
Setting individual VM automation to prevent vMotion of Proxies
Success:; Completed enrolling PNs via vCenter
```

The PNs that you selected appear in the Protected Nodes list; however, they are `unverified` as evidenced by the status in the **PROTECTED NODES** page > **Protection Disabled** column.

h. From the ESXi/ESX host, power on the PN proxies.

i. Activate (aka *verify*) the PNs so that onQ can protect them.

Go to **PROTECTION CONFIG** tab, select the PN, then click the **MODIFY** button.

Specify values for the node parameters, then **SAVE**. The act of saving a PN’s configuration instructs onQ to activate that PN’s configuration. If the PN is a Linux PN, onQ cannot enroll these XFS mount points automatically, so you must do so now. See Linux Filesystem Format Requirements.

The onQ Portal groups the PNs by ESXi server. If you do not want these PNs in such a group, clear the default **Group Name** field to remove the PNs from this group and place them in the shared pool.

1.

2. Copy and modify `/boot/grub/menu.lst`:

```
default=0
timeout=5
hiddenmenu
title Red Hat Enterprise Linux Server by Quorum onQ (2.6.18-
371.el5xen)
root (hd0,0)
kernel /vmlinuz-2.6.18-371.el5xen ro root=/dev/xvda1
rd_NO_LUKS rd_NO_MD rhgb crashkernel=auto rd_NO_LVM
initrd /initrd-2.6.18-371.el5xen.img.5
```

3. **Log on to the PN and open the** following ports on the firewall in order for onQ to communicate with the PN.
   - UDP port `5990`
   - TCP ports `5000` and `5990`

1.

iptables:

a. Verify that udp 5990 and tcp 5000 and 5990 ports are open and above the `REJECT` line:

```
# iptables -L -n | grep -E "5900|5000"
ACCEPT   udp -- 0.0.0.0/0        0.0.0.0/0
udp dpt:5990
ACCEPT   tcp -- 0.0.0.0/0        0.0.0.0/0
state NEW tcp dpt:5000
ACCEPT   tcp -- 0.0.0.0/0        0.0.0.0/0
state NEW tcp dpt:5990
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with
icmp-host-prohibited
```

b. If these ports are not open, open them.

Find the input chain name, which is reported in the line that appears after `INPUT`:

```
# iptables -L -line numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 RH-Firewall-1-INPUT all -- anywhere anywhere
...
10 REJECT all -- anywhere anywhere reject-with
icmp-host-prohibited
```

Using the line number of the `REJECT` line and the chain name (line `10` and line `1`, respectively, in the step above), insert the onQ ports:

```
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5990 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5000 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -p udp --
dport 5990 -j ACCEPT
```

c. Save and restart iptables.

Afterward, verify that the ports are open and above the `REJECT` line as outlined earlier.

```
# service iptables save
Saving firewall rules to /etc/sysconfig/iptables:
[ OK ]
# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules:
ip_conntrack_netbios_n [ OK ]
```

2. (Oracle database) Install `RMAN` scripts.

If the PN has an Oracle database, install the `RMAN` scripts so that onQ can execute a hot backup of your database as outlined in Back up and restore Oracle 11g database on Linux.

1.

(RHEL 5.x/ESXi) To enroll an agent-less Linux PN:

Use this procedure to enroll an agent-less Linux PN running RHEL 5.x and that's being hosted by an ESXi server.

1. **Install the PN proxies**:

   a. Enable `ssh` on the ESXi/ESX server.

   b. Reserve 1 to 3 unique static IP addresses for each PN proxy type (Linux and Windows). The more proxies you configure, the more concurrent backups onQ can perform.

   c. Log on to the HA's onQ Portal.

   d. Click the **PROTECTION CONFIG** tab > double-plus button (**++**).

   The **Add Protected Nodes via Host** dialog appears.

   e. In the **Server Type** field, select the **ESX Host** radio button.

   f. In the **User Name** and **Password** fields, provide the ESXi/ESX host credentials for any user with root privileges.

   g. In the Server field, provide either the hostname or the IP address for the ESXi/ESX host, then **GET LIST**.

   The onQ Portal queries the virtual machines hosted by the ESXi/ESX server, then displays the inventory.

   h. In the virtual machine list, select the check boxes (or **ALL** button) for the PNs that you want to enroll.

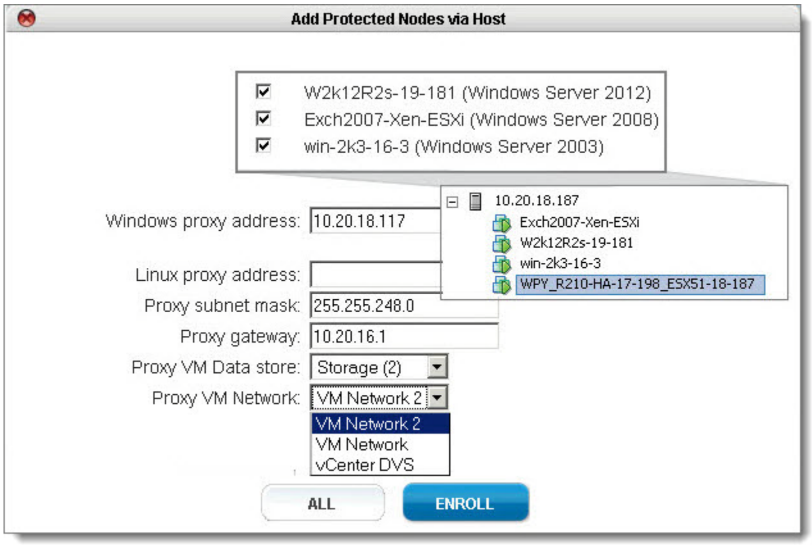
   If an expected virtual machine does not appear in the list, it's likely that the virtual machine does not have VMware Tools installed.

   Provide the network properties for each proxy. Use the unique IP addresses that you reserved above.

   - **Windows proxy address**. The static IP address that you reserved for the Windows PN proxy.
   - **Linux proxy address**. The static IP address that you reserved for the Linux PN proxy.

- **Proxy subnet mask**. The PN proxy’s subnet mask.
- **Proxy gateway**. The PN proxy’s gateway.
- **Proxy VM Data store**. The directory in which the vm’s files are stored.
- **Proxy VM Network**. Your network configuration can include a vCenter-level Distributed Virtual Switches (DVS) or an ESXi host-level virtual switch. When you enroll an ESXi host, all available networks that are visible to that host are listed and available for selection.

In the following example, three Windows PN are being enrolled, so only one static IP address (for the Windows PN proxy `WPY_`<onQhostname>_<ESXhostname>) is needed:



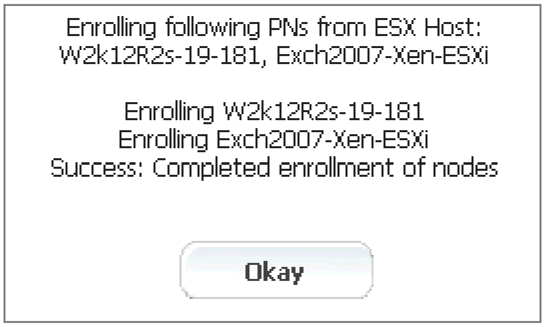
Add Protected Nodes via Host

☑ W2k12R2s-19-181 (Windows Server 2012)
☑ Exch2007-Xen-ESXi (Windows Server 2008)
☑ win-2k3-16-3 (Windows Server 2003)

10.20.18.187
- Exch2007-Xen-ESXi
- W2k12R2s-19-181
- win-2k3-16-3
- WPY_R210-HA-17-198_ESX51-18-187

Windows proxy address: 10.20.18.117
Linux proxy address:
Proxy subnet mask: 255.255.248.0
Proxy gateway: 10.20.16.1
Proxy VM Data store: Storage (2)
Proxy VM Network: VM Network 2

Click the **ENROLL** button, then **OKAY**.



Enrolling following PNs from ESX Host:
W2k12R2s-19-181, Exch2007-Xen-ESXi

Enrolling W2k12R2s-19-181
Enrolling Exch2007-Xen-ESXi
Success: Completed enrollment of nodes

The PNs that you selected appear in the Protected Nodes list; however, they are `unverified` as evidenced by the status in the **PROTECTED NODES** page > **Protection Disabled** column.

i. From the ESXi/ESX host, power on the PN proxies.

j. Activate (aka *verify*) the PNs so that onQ can protect them.

Go to **PROTECTION CONFIG** tab, select the PN, then click the **MODIFY** button.

Specify values for the node parameters, then **SAVE**. The act of saving a PN's configuration instructs onQ to activate that PN's configuration. If the PN is a Linux PN, onQ cannot enroll these XFS mount points automatically, so you must do so now. See Linux Filesystem Format Requirements.

The onQ Portal groups the PNs by ESXi server. If you do not want these PNs in such a group, clear the default **Group Name** field to remove the PNs from this group and place them in the shared pool.

1.

2. Copy and modify `/boot/grub/menu.lst`:

```
default=0
timeout=5
hiddenmenu
title Red Hat Enterprise Linux Server by Quorum onQ (2.6.18-371.el5xen)
root (hd0,0)
kernel /vmlinuz-2.6.18-371.el5xen ro root=/dev/xvda1 rd_NO_LUKS rd_NO_MD rhgb crashkernel=auto rd_NO_LVM
initrd /initrd-2.6.18-371.el5xen.img.5
```

3. **Log on to the PN and open the** following ports on the firewall in order for onQ to communicate with the PN.

- UDP port `5990`
- TCP ports `5000` and `5990`

4.

iptables:

a. Verify that udp 5990 and tcp 5000 and 5990 ports are open and above the `REJECT` line:

```
# iptables -L -n | grep -E "5900|5000"
ACCEPT   udp -- 0.0.0.0/0        0.0.0.0/0
udp dpt:5990
ACCEPT   tcp -- 0.0.0.0/0        0.0.0.0/0
state NEW tcp dpt:5000
ACCEPT   tcp -- 0.0.0.0/0        0.0.0.0/0
state NEW tcp dpt:5990
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with
icmp-host-prohibited
```

b. If these ports are not open, open them.

Find the input chain name, which is reported in the line that appears after `INPUT`:

```
# iptables -L -line numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 RH-Firewall-1-INPUT all -- anywhere anywhere
...
10 REJECT all -- anywhere anywhere reject-with
icmp-host-prohibited
```

Using the line number of the `REJECT` line and the chain name (line `10` and line `1`, respectively, in the step above), insert the onQ ports:

```
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5990 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -m state --
state NEW -p tcp --dport 5000 -j ACCEPT
# iptables -I RH-Firewall-1-INPUT 10 -p udp --
dport 5990 -j ACCEPT
```

c. Save and restart iptables.

Afterward, verify that the ports are open and above the `REJECT` line as outlined earlier.

```
# service iptables save
Saving firewall rules to /etc/sysconfig/iptables:
[ OK ]
# service iptables restart
Flushing firewall rules: [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules: [ OK ]
Applying iptables firewall rules: [ OK ]
Loading additional iptables modules:
ip_conntrack_netbios_n [ OK ]
```

5. **(Oracle database) Install `RMAN` scripts**.

   If the PN has an Oracle database, install the `RMAN` scripts so that onQ can execute a hot backup of your database as outlined in Back up and restore Oracle 11g database on Linux.

6.

To re-enroll a proxy PN:

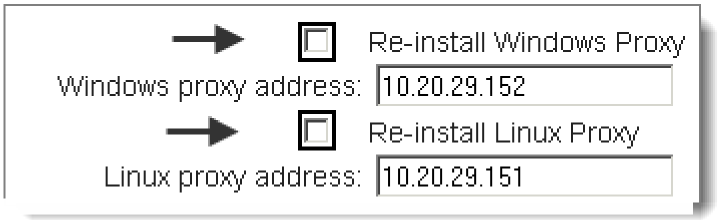
Use this procedure to re-enroll (aka reinstall) the Linux PN proxy or the Windows PN proxy or both. Perform this procedure on each vCenter server or ESX/ESXi host enrolled with the onQ.

1. Log on to the HA’s onQ Portal.
2. Click the **PROTECTION CONFIG** tab.
3. Click the double-plus button (**++**).

   The **Add Protected Nodes via Host** dialog appears.
4. Do one of the following, depending on the enrollment type:
   - In the **Server Type** field, select the **ESX Host** radio button.
   - In the **Server Type** field, select the **vCenter** radio button.
5. Provide the vCenter/ESXi root userid and password and either vCenter/ESXi host name or IP address, then **GET LIST**.

- (vCenter enrollment) The **Add Protected Nodes via vCenter** dialog appears.
- (ESXi Host enrollment) The **Add Protected Nodes via vCenter** dialog appears. The PN check boxes for enrolled PNs are greyed out.

6. In the **Proxy VM Network** field, reattach the virtual network adapter.
7. Select **Re-install Windows proxy** or **Re-install Linux proxy**, depending on the operating system of the proxy you're trying to reinstall, then **ENROLL**.



□ Re-install Windows Proxy

Windows proxy address: 10.20.29.152

□ Re-install Linux Proxy

Linux proxy address: 10.20.29.151

8. Observe the messages that appear in the pop-up window to verify that the proxy reinstalled successfully.

Related Topics

(Agent-less PNs) Connection and Backup Problems

5.5 (Agent-based PNs) Add protected nodes manually

When you enroll a protected node, onQ automatically (1) installs the onQ Service and (2) adds the PN to the onQ Portal's list of protected nodes thereby registering the PN with the onQ Manager.

However, there are reasons why you might want to *manually* add a protected node to the list:

- You attempted to enroll the protected node, but the installer refused to add the node because there is not enough disk space. Remember, onQ needs disk space for both the protected node's virtual machine (vdisk) and the protected node's data, which is stored in the repository. The amount needed is 1.5 x the used disk space on the protected node. If you are certain that the data will not grow, you can add the node manually.

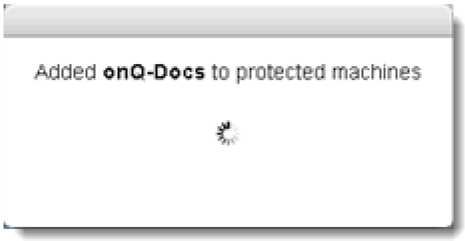
- You want a protected node to appear in the onQ Portal's list of protected nodes but don't want to enroll the node yet.
- You previously enrolled this PN, but deleted it from the onQ Appliance's configuration.

To add a protected node to the list:

1. Log on to the HA's onQ Portal.
2. Stop protection.

   You can only add to the list of protected nodes when **Protection** is **OFF**.
3. Click the **PROTECTION CONFIG** tab.
4. Click the plus button (**+**).
5. From the **Add a Protected Node** dialog, type the PN's host name, and specify values for the node parameters, then **SAVE**.

   If onQ successfully added the Protected Node, a confirmation message appears:

   Added **onQ-Docs** to protected machines
6. From the **PROTECTION CONFIG** tab, confirm that the newly added protected node appears in the list.
7. If you'd eventually like to protect this node, you must stop protection, then enroll the protected node.
8. Start protection.

6

Enrollment in Windows Cluster Services Environment

6.1 Windows Cluster Services Overview

onQ supports the ability to run RNs in a Windows Cluster Services environment. How you enroll and start PNs/RNs is different than in a non-cluster environment. For additional information on cluster support, go to “Windows Cluster Services Support” in onQ Release Notes.

When Exchange or SQL is installed in a cluster environment, it receives its own identity. This identity is not the identity of either of the nodes. This identity is called the Clustered Server (virtual server), and it has its own IP address. This IP address is shared between the nodes. The active node "owns" this virtual IP address until that node fails. The passive node receives heartbeat packets from the active server as long as the active server is up and running.

When the active server goes down/offline, the passive server becomes the active server and the virtual IP address transfers to the new active node. onQ continues to back up the node because it does not see the actual node go offline. In order to support this functionality, the installation of the onQ Service is different than in a non-cluster environment.

Related Topics

Windows Cluster Services Support
Windows Cluster Services Limitations
(Step 1) Prepare the cluster nodes
(Step 2) Install onQ Service on cluster
(Step 3) Configure cluster for the onQ Service
(Step 4) Configure the onQ Appliance for cluster environment
(Step 5) Enroll the cluster on the onQ Appliance
Work with RNs in cluster environment

6.2 (Step 1) Prepare the cluster nodes

To install the cluster modules (*Windows 2012 & 2012R2*):

If your PNs (aka cluster nodes) are running Win2k12 or Win2k12R2, you must perform the following procedure on those PNs prior to protecting the onQ. If you don’t, the corresponding RNs will not work.

1. Open a power shell and choose to **Run as Administrator**.
2. Add the required modules.

   Both the Failover Cluster Automation Server module and the Failover Cluster Command Interface module must be installed on each PN (cluster node).

a. Determine which modules are currently installed:

```
> PS C:\Users\administrator> Get-WindowsFeature RSAT-Cluster*
Display Name                                    Name            Install State
------------                                    ----            -------------

[X] Failover Clustering Tools                   RSAT-Clustering
Installed

    [X] Failover Cluster Management Tools       RSAT-Clustering-Mgmt
    Installed

    [X] Failover Cluster Module for Windows... RSAT-Clustering-Powe...
    Installed

    [X] Failover Cluster Automation Server      RSAT-Clustering-Auto...
    Installed

    [ ] Failover Cluster Command Interface      RSAT-Clustering-CmdI...
    Available
```

b. Add the **Failover Cluster Automation Server** module:

```
> Install-WindowsFeature -Name RSAT-Clustering-
AutomationServer
```

c. Add the **Failover Cluster Command Interface** module:

```
> Install-WindowsFeature -Name RSAT-Clustering-
CmdInterface
```

3. Import the modules that you just added:

```
> import-module failoverclusters
```

4. Verify that the required modules are installed:

```
> Get-WindowsFeature RSAT-Cluster*
Display Name                                        Name              Install State
------------                                        ----              -------------

[X] Failover Clustering Tools                       RSAT-Clustering
Installed

    [X] Failover Cluster Management Tools               RSAT-Clustering-Mgmt
    Installed

    [X] Failover Cluster Module for Windows... RSAT-Clustering-Powe...
    Installed

    [X] Failover Cluster Automation Server              RSAT-Clustering-Auto...
    Installed

    [X] Failover Cluster Command Interface              RSAT-Clustering-CmdI...
    Installed
```

Next Step: Go to (Step 2) Install onQ Service on cluster.

To install the iSCSI initiator (*Windows 2003*)

Microsoft iSCSI initiator must be installed on the PN, if not installed already. Installation is required on Windows 2003. The iSCSI initiator is preinstalled on the following Windows versions:

- Windows 2012
- Windows 2008 R2
- Windows 2008

Once installed on the protected node, the initiator will become available in the Recovery Node and will be used for configuration of Virtual SAN connectivity when Recovery Node is started in either Test Mode or in Production Mode.

Go to http://www.quorum.net/file_share/Initiator.zip. The `Initiator.zip` file contains following versions of initiators. Install the appropriate version on the cluster node.

- `Initiator-2.08-build<version>-x64fre.exe`
- `Initiator-2.08-build<version>-x86fre.exe`

Next Step: Go to (Step 2) Install onQ Service on cluster.

6.3 (Step 2) Install onQ Service on cluster

Use this procedure to download and install the onQ Service installer on the Windows cluster server that you want to protect.

To manually install the onQ Service on a cluster server:

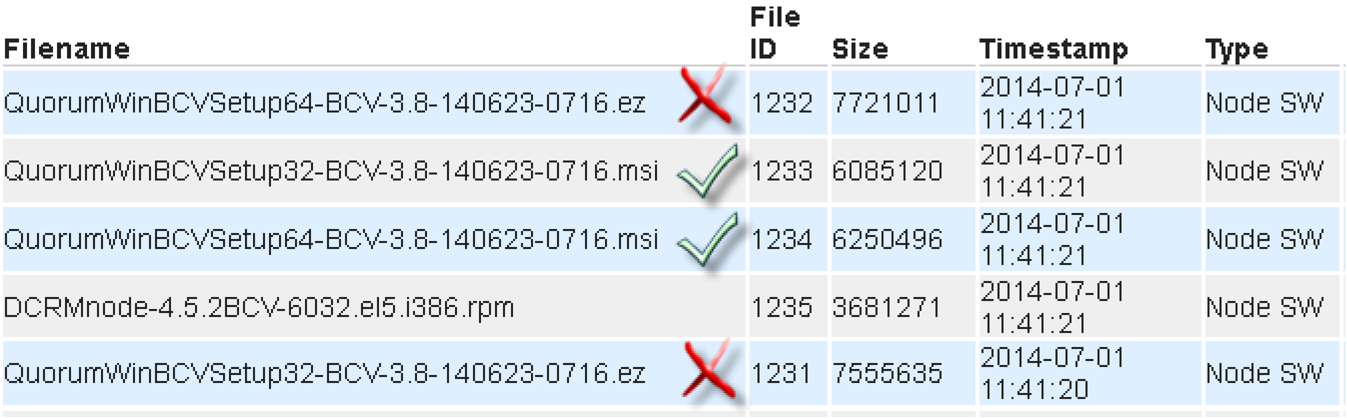
Before You Begin: Go to (Step 1) Prepare the cluster nodes.

In this procedure, you will perform a *manual* install of the onQ Service on the cluster server.

1. RDP to the server that you want to protect, then log on to that server as a user with administrative privileges.
2. From that server, launch a browser (see Browser Support), then log on to the HA's onQ Portal as `varadmin`.
3. Download the onQ Service installer.
   a. In the onQ Portal, go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **DOWNLOADS** page.

Warning: Do not download the `.ez` file, which is only intended for *Protect Me-based* enrollments as outlined in (Agent-based PNs) Restart the onQ Service), not manual installs.

b. Scroll down and select the `QuorumWinBCVSetup<bitVersion>-BCV<build>.msi` file that matches your server’s operating system.



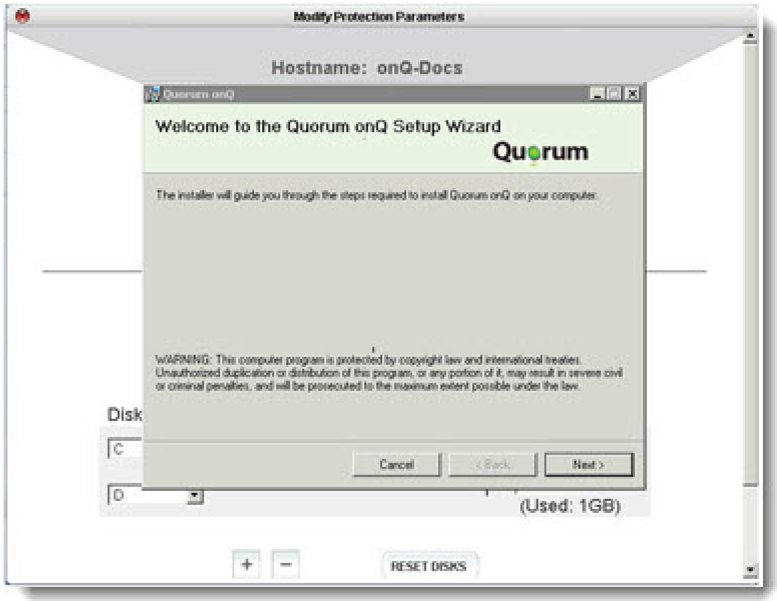
	File			
Filename	ID	Size	Timestamp	Type
QuorumWinBCVSetup64-BCV-3.8-140623-0716.ez ✗	1232	7721011	2014-07-01 11:41:21	Node SW
QuorumWinBCVSetup32-BCV-3.8-140623-0716.msi ✓	1233	6085120	2014-07-01 11:41:21	Node SW
QuorumWinBCVSetup64-BCV-3.8-140623-0716.msi ✓	1234	6250496	2014-07-01 11:41:21	Node SW
DCRMnode-4.5.2BCV-6032.el5.i386.rpm	1235	3681271	2014-07-01 11:41:21	Node SW
QuorumWinBCVSetup32-BCV-3.8-140623-0716.ez ✗	1231	7555635	2014-07-01 11:41:20	Node SW

c. Click the **DOWNLOAD** button, saving the file to your `Downloads` folder. Stop! Do not run this file yet because you might not have the necessary User Account Control levels.

4. Install the onQ Service:

a. Open the `Downloads` folder. On the newly downloaded msi installer, right-click > **Run as Administrator**. If prompted, do not put any restrictions on this account.

b. Follow the on-screen instructions in the **Setup Wizard**.

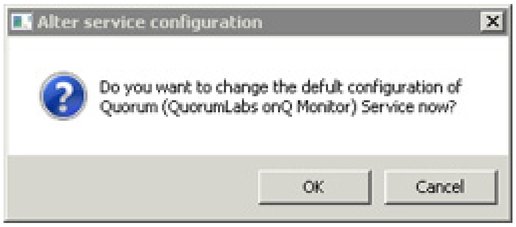


Welcome to the Quorum onQ Setup Wizard

The installer will guide you through the steps required to install Quorum onQ on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

When prompted, choose whether or not you want to configure the service to use a specific account. This account must have adequate privileges to back up all the files that you want to protect.

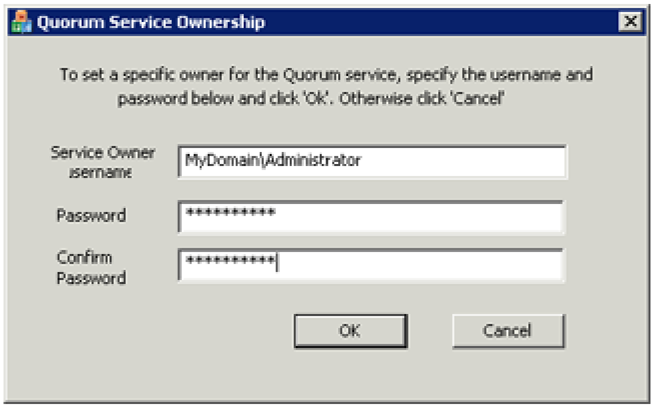


Do you want to change the defult configuration of Quorum (QuorumLabs onQ Monitor) Service now?

In the After service configuration dialog, do one of the following:

- Click **Cancel** to configure the service to use `Local System` as the owner of the onQ Service.
- Click **OK**, then, in the dialog that launches, specify the account and credentials that you want the service to use, then **OK**. For example, you can configure the service to run as `administrator`. If you want the service to run as the *domain*

administrator specify the domain:



Quorum Service Ownership

To set a specific owner for the Quorum service, specify the username and password below and click 'Ok'. Otherwise click 'Cancel'

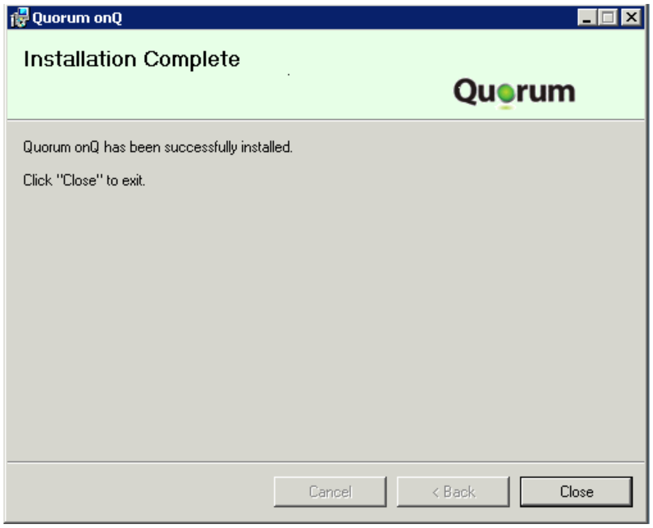
Service Owner username: MyDomain\Administrator

Password: ***********

Confirm Password: ***********

A service running on Windows generally runs as a user account, usually `Local System` by default. However, you can configure the service to run as any user. At the end of the process, onQ Manager presents you with a summary of the PN's proposed configuration.

Congratulations, you’ve installed the onQ Service.



Quorum onQ

Installation Complete

Quorum onQ has been successfully installed.

Click "Close" to exit.

Next Step: Go to (Step 3) Configure cluster for the onQ Service.

6.4 (Step 3) Configure cluster for the onQ Service

Use this procedure to create a resource and resource group for the onQ Service on the Windows cluster server that you want to protect.

To configure the cluster for onQ Service (*Windows 2012*):

Before You Begin: Go to (Step 2) Install onQ Service on cluster.

Add the “Quorum onQ Service” as a Generic Service Resource:

1. On the active cluster node, launch the Failover Cluster Manager from the **Start** menu and connect to the cluster.
2. Under the Cluster name on the left pane, right-click **Roles** and select **Configure Role**.
3. In the resulting High Availability wizard, do the following:
   a. On the **Before You Begin** page (if shown), click **Next**.
   b. On the **Select Role** page, select **Generic Service** and click **Next**.
   c. Select **Quorum onQ Service** and click **Next**.
   d. On the **Client Access Point** page, do the following:
      - In the **Name** field, type `QuorumOnQSvc`, or type a unique name if onQ is protecting more than one cluster setup and if clusters are using the same Domain Controller to prevent any conflicts.
      - In the **Address** field, type a valid available IPv4 address.
   e. On the **Select Storage** page, click **Next**.
   f. On the **Replicate Registry Settings** page, click **Next**.
   g. On the **Confirm** page, click **Next**.
   h. On the **Summary** page, click **Finish**.

Configure the “Quorum onQ Service” resource:

1. On the active node, launch the Failover Cluster Manager from the **Start** menu and connect to the cluster.
2. Click on the **Roles**.

3. Click **QuorumOnQSvc** in the top middle pane.
4. Switch to the **Resources** tab in the middle pane, at the bottom, and right-click **Quorum onQ Service** under **Roles** and select **Properties**.
5. On the **General** tab, do the following:
   a. Clear the entry in the **Startup Parameters** field.
   b. Enter a space.
   c. Click **Apply**.
6. On the **Policies** tab, do the following:
   a. Select the **if resource fails, attempt to restart...** radio button.
   b. In the **Period for restart(mm:ss)** field, type a value of `2:00`.
   c. In the **Maximum restart in the specified period** field, type `10`.
   d. Select all check boxes on the page.
   e. In the **If all the restart attempts fail, begin restarting again after the specified period(hh:mm)** field, type `01:00`.
   f. In the **Pending timeout(mm:ss)** field, type a value of `03:00`.
7. Click **OK** to exit the wizard.

Restart "QuorumOnQSvc" Resource Group:

1. On the active node, launch the Failover Cluster Manager from the **Start** menu and connect to the cluster.
2. Click **Roles**.
3. Right-click **QuorumOnQSvc** in the middle pane and select **Take offline**.
4. Right-click **QuorumOnQSvc** again and select **Bring online**.

Next Step: Go to (Step 4) Configure the onQ Appliance for cluster environment.

To configure the cluster for onQ Service (*Windows 2008 & 2008 R2*):

Before You Begin: Go to (Step 2) Install onQ Service on cluster.

Add "Quorum onQ Service" as a Generic Service Resource:

1. On the active cluster node, launch the Failover Cluster Manager from the **Start** menu and connect to the cluster.

2. Right-click **Services and Applications** and select **Configure a Service or Application**.
3. In the resulting High Availability wizard, do the following:
   a. On the **Before You Begin** page (if shown), click **Next**.
   b. On the **Select Service or Application** page, select **Generic Service** and click **Next**.
   c. Select **Quorum onQ Service** and click **Next**.
   d. On the **Client Access Point** page, do the following:
      - In the **Name** field, type `QuorumOnQSvc`, or type a unique name if onQ is protecting more than one cluster setup and if clusters are using the same Domain Controller to prevent any conflicts.
      - In the **Address** field, type a valid available IPv4 address.

   e. On the **Select Storage** page, click **Next**.
   f. On the **Replicate Registry Settings** page, click **Next**.
   g. On the **Confirm** page, click **Next**.
   h. On the **Summary** page, click **Finish**.

Configure QuorumOnQSvc Resource group:

1. On the active node, launch the Failover Cluster Manager from **Start** menu and connect to the cluster.
2. Click the **+** to expand **Services and Applications**.
3. Right-click **QuorumOnQSvc** and click **Properties**.
4. On **General** tab, check **Auto Start** (If available).
5. On **Failover** tab, do the following:
   a. In the **Maximum failure in the specified period** field, type a value of `10`.
   b. In the **Period** field, type a value of `1`.
6. Click **OK**.

Configure “Quorum onQ Service” resource:

1. On the active node, launch the Failover Cluster Manager from **Start** menu and connect to the cluster.

2. Click the **+** to expand **Services and Applications**.
3. Click **QuorumOnQSvc**.
4. On the **Summary of QuorumOnQSvc** page (in the middle pane), right-click **Quorum onQ Service**, and click **Properties**.
5. On the **General** tab, do the following:
   a. Clear the entry in the **Startup Parameters** field. If needed enter a couple of spaces.
   b. In the **Please confirm action** window, click **Yes**.
   c. In the **Information** dialog, click **OK**.
   d. Click **Apply**.
6. On the **Policies** tab, do the following:
   a. Select the **if resource fails, attempt to restart...** radio button.
   b. In the **Period for restart(mm:ss)** field, type a value of `2:00`.
   c. In the **Maximum restart in the specified period** field, type `10`.
   d. Select all check boxes on the page.
   e. In the **If all the restart attempts fail, begin restarting again after the specified period(hh:mm)** field, type `01:00`.
   f. In the **Pending timeout(mm:ss)** field, type a value of `03:00`.
7. Click **OK** to exit the wizard.

Restart QuorumOnQSvc Resource group:

1. On the active node, launch the Failover Cluster Manager from the **Start** menu and connect to the cluster.
2. Click the **+** to expand **Services and Applications**.
3. Right-click **QuorumOnQSvc** and select **Take this service or application offline**.
4. Confirm the action.
5. Right-click **QuorumOnQSvc** and select **Bring this service or application online**.

Next Step: Go to (Step 4) Configure the onQ Appliance for cluster environment.

To configure the cluster for onQ Service (*Windows 2003*):

Before You Begin: Go to (Step 2) Install onQ Service on cluster.

Add QuorumOnQSvc group:

1. On the active node, launch Cluster Administration from **Start** menu and connect to the cluster.
2. Click the **+** to expand **Group**.
3. Right-click **Group** and select New and then Group.
4. In the **New Group** window, do the following:
   a. Type `QuorumOnQSvc`, or type a unique name if onQ is protecting more than one cluster setup and if clusters are using the same Domain Controller to prevent any conflicts.
   b. Enter a description, if desired.
   c. Click **Next**.
5. In the **Preferred Owners** window, do the following:
   a. Select from the **Available Nodes** list and move them to the **Preferred Owners** list, if required. Set the order of preference, if preferred owners are set.
   b. In the **Period** field, type a value of `1`.
6. Click **OK** on the group creation confirmation.

Add “Quorum OnQ Service” as a Generic Service Resource:

1. On the active node, launch Cluster Administration from **Start** menu and connect to the cluster.
2. Right-click **Resources** from under the cluster, select **New**, and then select **Resource**.
3. In the resulting New Resource wizard, do the following:
   a. In the **Name** field, type `Quorum onQ Service`.
   b. In the **Description** field, type the desired description.
   c. In the **Quorum onQ Service** drop-down menu, select **Generic Service**.
   d. In the **Group** drop-down menu, select the **QuorumOnQSvc**.

   e. Select the **ON** check box for **Run this resource in a separate resource monitor**.
   f. Click **Next**.
4. In the **Possible Owners** window, select desired owners from **Possible Owners** list and click **Next**.
5. In the **Dependencies** window, click **Next**.
6. On the **Generic Service Parameters** page, do the following:
   a. In the **Service Name** field, type `Quorum`.
   b. Leave the **Start Parameters** field empty.
7. In the **Registry Replication** window, click **Finish**.

Configure "Quorum onQ Service" resource:

1. On the active node, launch Cluster Administration from **Start** menu and connect to the cluster.
2. Click the **+** to expand the cluster.
3. Right-click **QuorumOnQSvc** and select **Properties**.
4. On the **QuorumOnQSvc Properties** page, do the following in the **Failover** tab:
   a. In the **Threshold** field, type a value of `10`.
   b. In the **Period** field, type a value of `1`.
   c. Click **OK**.
5. Click **QuorumOnQSvc** on the left pane and select the **Quorum onQ Service** on the right pane.
6. On the **Advanced** tab, do the following:
   a. Select the **Restart** radio button.
   b. Select the **Affect the group** check box.
   c. In the **Threshold** field, type a value of `10`.
   d. In the **Period** field, type a value of `7200`.
   e. In the **Pending timeout** field, type a value `180`.
   f. Click **OK**.

Restart QuorumOnQSvc Resource group:

1. On the active node, launch Cluster Administration from **Start** menu and connect to the cluster.
2. Right-click **QuorumOnQSvc**, and select **Take offline**.
3. Right-click **QuorumOnQSvc**, and select **Bring online**.

Next Step: Go to (Step 4) Configure the onQ Appliance for cluster environment.

6.5 (Step 4) Configure the onQ Appliance for cluster environment

Before You Begin: Go to (Step 3) Configure cluster for the onQ Service.

Use this procedure to configure an onQ Appliance for a cluster environment by installing the SAN template on which onQ depends for running recovery nodes. Use this procedure only if your onQ Appliance was configured with a version prior to onQ v3.8 as onQ 3.8 or later shipments include the SAN template by default. The SAN template is not part of the onQ software itself.

To configure the onQ Appliance for cluster environment:

1. Stop protection.
2. Upgrade to the latest onQ version. Go to Update Appliance software.
3. Log on to the hypervisor using Putty or Terminal.
4. Download the SAN template and store it locally on the hypervisor (preferably under `/var/run/sr-mount/xxxxxxxxx-xxxx-xxxx-xxxx` folder).
5. In the console command prompt, do the following:
   a. Extract the SAN template to its original size. When extracted the template should end with `.xva` extension.

```
# gunzip SAN-TEMP.cluster.xva.gz
```

   b. Run the following command, then record the uuid for the item with name-label set to `VHD_SR`:

```
# xe sr-list
```

c. Using the uuid that you just identified, run the following command:

The import can take a long time. Nonetheless, the command returns immediately, and so you can monitor the import using XenServer’s log screen; also, when the import disappears from the **ps -ef** command output, the import completed.

```
# xe vm-import filename=SAN-TEMP.cluster.xva sr-
uuid=<UUID>
```

To import a template and create the VHD on the hypervisor can take 10-15 minutes.

Next Step: Go to (Step 5) Enroll the cluster on the onQ Appliance.

6.6 (Step 5) Enroll the cluster on the onQ Appliance

Use this procedure to enroll the cluster on the onQ Appliance.

Before You Begin: Go to (Step 4) Configure the onQ Appliance for cluster environment.

To enroll the cluster on onQ:

1. Do the following:

   a. Stop protection.

   b. Go to the **Protection Config** tab.

   c. Click **+** to enroll the cluster.

   d. In the **Hostname** field, enter the cluster name.

   If the cluster name is not known, run the following command on the active cluster node:

   ```
   > cluster /PROPERTIES
   ```

   e. Set other parameters as needed.

   f. Configure the cluster node and SAN disks that are associated with the cluster. Verify that the **Disk Letter** and corresponding **Size** for each disk is appropriate.

   g. Click **SAVE**.

2. Click on the **Modify** button, then in the protection list, add all volumes and applications that the cluster requires.

   If you are enrolling the PN for the first time using the **Protect Me** button on the onQ Portal, then all volumes (local and iSCSI) on the PN are auto discovered.

3. Click on the **Advanced** button, then in the window, set the radio button for **Enable Cluster Support** to `Yes` to display additional fields for the configuration.

4. From the expanded display for cluster configuration, do the following:

   a. Select the volumes pertaining to cluster services and also any application or other services desired from the list for 'Cluster Volumes'.

   b. In the **Virtual SAN IP Address** field, type a valid and unique IP address that you want to be used with the virtual SAN. The IP used should be in the same subnet as that of onQ. Also, this IP should not be the same as that of physical SAN currently used with the PN.

   c. Type a gateway address that is associated with the virtual SAN IP address.

   d. Type a subnet mask for the virtual SAN.

5. **SAVE** the protected node configuration.

6. Do the following:

   a. Go to **APPLIANCE CONFIG** tab > **ADVANCED…** button > **HOSTS** tab.

   b. In the **IP Address** field, type the cluster (shared) IP address.

   c. In the **Host(s)/comments** field, type the cluster name.

   d. Click **+** to add the host.

   e. Click APPLY.

Next Step: Test your RNs. Go to Work with RNs in cluster environment.

6.7 Work with RNs in cluster environment

After deploying onQ in your cluster environment, use the following procedures to administer your PNs/RNs.

To back up the PN:

1. Start protection.
2. Trigger (scheduled or manual) backups as needed for the configured node.
3. Allow the backup to complete and the RN to be built.
4. If new volumes were added to protection, reinitialize the RN.

   If the PN was added for the first time, this is not required.

To start the RN in test mode (*Windows 2003)*:

Start the Recovery Node for the Domain Controller first in test mode, if the cluster is configured to work with a domain account.

1. Create and start the RN and iSCSI SAN clones. To do so, select the Recovery Node for the cluster node and start it in Test Mode
2. In the RN console for the cluster node, do the following:
   a. Log on with same administrative account that you used on the PN.

      If necessary, to log on to the virtual SAN use the default password for the `root` user account. If you do not know this password, contact Quorum Support.

   b. From a command prompt on the RN, run the following:

```
> cd /d c:\Program Files\Quorum\usr\ONQSUP
> CLUSSERVICEFQ.BAT
```

3. Start the Microsoft iSCSI initiator.
4. Select the **Targets** tab, then log off from any existing or reconnecting targets.
5. Select **Discovery** tab, then do the following:
   a. In the **Target Portals** section, remove any residual entries.

   b. Select **Discover Portal** > **ADD**, then type the virtual SAN IP that was provided earlier when you configured the PN in the onQ Portal. Leave the default port set to `3260`.

   c. Click **OK**.

6. Select **Targets** tab, then do the following:

   a. Select the default Target name or the appropriate one, if more than one exists, then **Logon** button.

   b. In the Log on to Target pop-up window, select the **Automatically restore this connection** check box, then **OK**.

   c. Select **Persistent Targets** tab, then ensure that the same target that you selected previously on the Targets tab appears in the list.

Note: Click **Finish** to ignore any error while loading a driver for new hardware (IET Controller).

7. Select **OK** on the main window to exit the iSCSI initiator setup.

8. From a command prompt, do the following:

   a. Execute the following commands:

```
> cd C:\Program Files\Quorum\usr\ONQSUP
> FIX_CLUSTER.BAT
```

   b. Ignore errors at the end of the output and ascertain that the cluster service started.

   c. Rejoin the domain, if cluster service fails to start because the RN does not have a domain trust relationship established.

   d. Restart the cluster service.

9. Launch Cluster Administrator interface, then do the following:

   a. If the Open Connection to Cluster dialog doesn’t appear, use the FileOpen Connection dialog.

   b. In the Open Connection to Cluster dialog, choose `Open Connection to Cluster` value in the drop-down menu.

   c. In the **Cluster or server name** field, type a value ‘.’ (dot), then **OK**.

d. Under **Groups**, ensure that **Cluster Group** and any other **Application Cluster** (SQL Cluster for example) are all on-line, indicating that the cluster is in a usable state.

To start the RN in test mode (*Windows 2008*):

Start the Recovery Node for the Domain Controller in test mode, if the cluster is configured to work with a domain account.

1. Create and start the RN and ISCSI SAN clones. To do so, select the Recovery Node for the cluster node, then start it in Test Mode.
2. In the RN console for the cluster node, do the following:
    a. Log on with same administrative account that you use on the PN.

       If necessary, to log on to the virtual SAN use the password `password` for the `root` user account.

    b. From a command prompt on the RN, run the following:

```
> cd /d c:\Program Files\Quorum\usr\ONQSUP
> CLUSSERVICEFQ.BAT
```

3. Start the Microsoft iSCSI initiator.
4. Select the **Targets** tab, then log off from any existing or reconnecting targets.
5. Select **Discovery** tab, then do the following:
    a. In the **Target Portals** section, remove any residual entries.

    b. Select **Discover Portal** > **Add Portal**, then type the virtual SAN IP that was provided earlier when you configured the PN in the portal. Leave the default port set to `3260`.

    c. Click **OK**.
6. Select **Targets** tab, then do the following:
    a. Select the default Target name or the appropriate one, if more than one exists, then click on the **Logon** button.

    b. In the Log on to Target pop-up window, select the **Automatically restore this connection** check box, then **OK**.
7. Select **Volumes and Devices** tab to list the volumes that reflect the cluster disks. If none appear, choose **Autoconfigure** to force the iSCSI properties to display all cluster volumes configured, then **OK**.

8. From a command prompt, do the following:

   a. Execute the following commands:

   ```
   > cd C:\Program Files\Quorum\usr\ONQSUP
   > FIX_CLUSTER.BAT
   ```

   b. Verify that all disks are marked as `Reserved` using the `diskpart` command. If all volumes expected are not listed and/or are not marked as `Reserved` after few minutes from RN starting, reboot the RN.

9. Rejoin the domain. If the cluster service fails to start because RN does not have a domain trust relationship established, then restart the cluster service.

10. Launch the Failover Cluster Manager interface to perform additional administration, if necessary: **Start** > **Administrative Tools** > **Failover Cluster Manager**.
    - When the interface comes up, the left hand pane lists the clusters available along with the Services and applications, Nodes, Storage, and Networks associated with them.
    - Select the items under **Services and applications**, to list the status of the cluster (server name, disk drives and other resources) as it relates to the specific application. The **Status** of all of these items listed display `on-line` to indicate that the cluster is in a usable state.

To start the RN in test mode (*Windows 2008R2, 2012 & 2012R2*):

Start the Recovery Node for the Domain Controller in test mode, if the cluster is configured to work with a domain account.

1. Create and start the RN and ISCSI SAN clones. To do so, select the Recovery Node for the cluster node, then start it in Test Mode.

2. In the RN console for the cluster node, do the following:

   a. Log on with the administrative account (local or domain if configured for domain) for the PN.

      If necessary, to log on to the virtual SAN, use the password `password` for the `root` user account.

b. From a command prompt on the RN, run the following:

```
> cd /d c:\Program Files\Quorum\usr\ONQSUP
> CLUSSERVICEFQ.BAT
```

3. Start the Microsoft iSCSI initiator.

4. Select the **Targets** tab, then disconnect from any existing targets.

5. Select **Discovery** tab, then do the following:

a. Remove any residual entries under **Target Portals** and **iSNS servers** sections.

b. Select **Discover Portal**. Type the virtual SAN IP that you used to configure the PN in the onQ Portal. Leave the default port set to `3260`. Click **OK**.

6. Select **Targets** tab, then do the following:

a. Select the Target name from under **Discovered Targets**. If the **Status** for the same is `Inactive`, then click on the **Connect** button, bringing the **Status** to `Connected`.

b. If the Target name doesn't display, type the target IP (same as the virtual SAN IP in the **Discovery** tab), then **Quick Connect** to connect to the virtual SAN, bringing the **Status** to `Connected`.

7. Select **Volumes and Devices** tab to list the volumes that reflect the cluster disks. If none appear, choose **Auto Configure** to force the iSCSI properties to display all cluster volumes configured, then **OK**.

8. From a command prompt, do the following:

a. Execute the following commands:

```
> cd C:\Program Files\Quorum\usr\ONQSUP
> FIX_CLUSTER.BAT
```

b. Verify that all disks are marked as `Reserved` using the `diskpart` command. It might take a long time for the volumes to reflect `Reserved` or to appear in the list from `list vol` command. If still not correctly listed after 30 minutes, reboot the RN.

9. If the cluster service fails to start (for example, you cannot see the cluster in the Failover Cluster Manager) or there are issues seeing the domain controller, rejoin the domain.

10. Launch the Failover Cluster Manager interface to perform additional administration, if necessary: **Start** > **Administrative Tools** > **Failover Cluster Manager**.
    - When the interface comes up, the left hand pane lists the clusters available along with Services and applications, Nodes, Storage, and Networks associated with them.
    - Select the items under **Services and applications**, to list the status of the cluster (server name, disk drives and other resources) as it relates to the specific application. The **Status** of all of these items listed display `on-line` to indicate that the cluster is in a usable state.

To start the RN in production mode:

1. Before your start the RN, do the following:
    a. Ensure that physical iSCSI target SAN is turned off and/or the drives configured to work with cluster node are not accessible.

    This is a precautionary step. The Recovery Node registry is updated with the information provided in the onQ Portal for the virtual SAN.

    b. Ensure that all failover nodes in the cluster are turned off.

    The RN you choose must have the latest backup in order for the data to be correct. Only one RN at a time can run in the cluster. When the RN is running in the production cluster, failover is not available.
2. Start the Recovery Node in production mode. Go to “Start recovery nodes on HA” on page 342 or “Start recovery nodes on DR Appliance or DR Mirror” on page 349.
3. Perform the procedure for your respective platform. The remaining steps are identical to those for test mode.
    - “To start the RN in test mode (Windows 2003):” on page 204
    - “To start the RN in test mode (Windows 2008):” on page 206
    - “To start the RN in test mode (Windows 2008R2, 2012 & 2012R2):” on page 207

7
Updates

7.1 (Start Here) Upgrade Support and Requirements

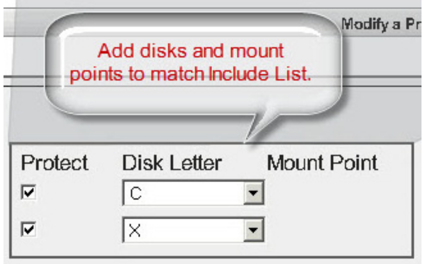
Upgrading *directly* to version 3.9 is supported for onQ Appliances and protected nodes running any previous release. If you want to migrate to an onQ Flex configuration, simply install your new onQ Flex license—after you upgrade to 3.9 (see "Install onQ Appliance license" in onQ Administrator's Guide).

Frequently Asked Questions:

Question	Answer
When should I expect to see the **Install Updates** button?	Upgrade packages are deployed through onQ Central. onQ Appliances and onQ Archive Vaults auto-download the necessary packages when the daily cron job runs. This job runs between 10pm and 2am each day. This deployment occurs for all onQ Appliances and onQ Archive Vaults for which onQ Central is set, by Quorum Support, to allow download of the latest software packages. If you received an upgrade announcement from Quorum Support, but do not see the **Install Updates** button in the onQ Portal and want to upgrade immediately, contact Quorum Support.
Do I need to upgrade my Appliances in any particular order?	**No (Single-tenant).** However, be sure to upgrade both HAs, DR Appliances, and onQ Archive Vaults synchronously. **Yes (Multi-tenant)**. Upgrade them one tenant at a time and sequentially. Due to the changes in the underlying platform, this approach is required to prevent onQs from becoming non-bootable.

Question	Answer
Do I need to initiate a reboot of onQ or appliance?	**No (On-Premise)**. onQ upgrade process *automatically* reboots onQ twice, followed by one onQ Appliance reboot thereby applying an important vulnerability (VENOM) patch for Xen Server. **Yes (DRaaS)**. Reboot your HA Appliance after Quorum Support upgrades and reboots your cloud AV/DR. Quorum Support notifies you when the reboot is needed. Quorum Support adheres to the following reboot order: AV > DR > and HA.
Do I need to stop protection to apply Appliance updates?	**No**. If protection is on, onQ quiesces the system, stops protection, applies the new software, then restarts protection.
What if I experience a problem during the upgrade?	Browse the troubleshooting tips in “Upgrade Problems” in onQ Administrator’s Guide. If you still have an issue, contact Quorum Support.

Before you upgrade:

Behavior/Change	What should I do?
In a File Backup Only configuration, onQ does not back up files and folders that do not have the corresponding disks and mount points defined and protected.	Add the disks and mount points to reflect the files and folders in your Include List. For more information, go to “Edit backup include list” in onQ Administrator’s Guide.  Modify a Pr Add disks and mount points to match Include List. Protect Disk Letter Mount Point ☑ C ☑ X
As outlined in Agent-less PN Enrollment Limitations, onQ is not able to enroll XFS mount points automatically for agent-less Linux PN.	For all previously enrolled Linux PNs with XFS mount points, add the XFS mount points manually: in the Modify a Protected Node dialog, click the plus (+) button to add a mount point.

After you upgrade:

Behavior/Change	What should I do?
onQ Portal provides UI enhancements.	Refresh your browser using CTRL-F5. If you don’t, portal changes will not be activated and some user actions will not work.

Behavior/Change	What should I do?
onQ Flex configurations, both new and existing, provides RN type to augment the Build type. onQ Portal sets RN type as follows: Auto RN Creation=Yes > R2R Auto RN Creation=No > OD	Nothing. Automatic. For more information, go to "(onQ Flex) Modify RN type and/or RN build policy" in onQ Administrator's Guide.
(Agent-less PNs only) There are two related changes that require your attention: Due to a change in how onQ interacts with an ESXi host, the upgrade process needs to purge any Quorum history associated with the PNs; afterward, onQ needs to perform a full backup of those PNs. Also, onQ needs to add a Quorum "history" volume (`QuorumDisk.vmdk`) to the RNs in order to optimize the resources it spends on performing backups.	Prior to restarting onQ protection, re-install all existing proxies to activate these changes. Afterward, re-initialize each agent-less RN to enable onQ to add the Quorum volume. `QuorumDisk.vmdk` is added as a protected volume; therefore, onQ can no longer protect up to 15 volumes: onQ now supports up to 14 volumes for agent-less RNs. If you have an RN that is configured with 15 volumes, unprotect one of those volumes, then re-intialize the RN.

Next Step: Now that you've read this topic, you're ready to upgrade. Go to Update Appliance software.

Related Topics

Update Appliance software

Upgrade Problems

7.2 Update Appliance software

Quorum regularly releases new versions of onQ Appliance software, including service packs and, from time to time, hot fixes.

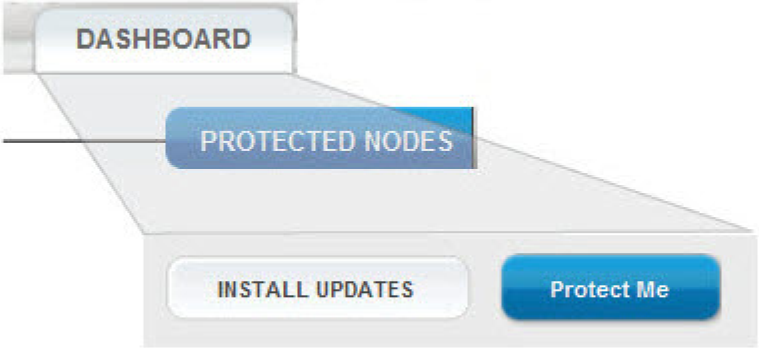
To *automatically* apply an update:

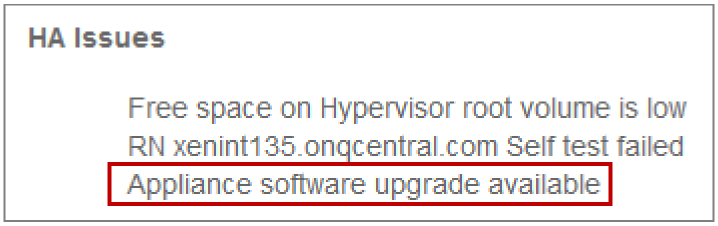
Before you begin: learn about any changes you should know about or pre-upgrade and post-upgrade requirements (for example, system reboots). Go to "(Start Here) Upgrade Support and Requirements" in onQ Administrator's Guide.

1. Log on to the onQ Portal. You must log on as `varadmin` user.
2. 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 software downloads from onQ Central. The **onQ STATUS** page > **Issues** pane also displays an `Appliance software upgrade available` message.





HA Issues

Free space on Hypervisor root volume is low
RN xenint135.onqcentral.com Self test failed
Appliance software upgrade available

3. Apply the new software:
   a. Go to the **DASHBOARD** tab.
   b. Scroll down and click the **INSTALL UPDATES** button.
   c. From the Install Updates dialog, click the **UPGRADE** button when prompted to initiate the upgrade.

4. From the **DASHBOARD**, mouse-over the Updates icon ⟳ to display the status of the upgrade, or open the Event log to observe the PN or proxy upgrade.

   Immediately after this onQ Appliance upgrade, onQ automatically initiates a PN software (agent-based) and PN proxy software (agent-less) upgrade as outlined in the following topics:
   - (Agent-based Windows PNs) Update node software
   - (Agent-based Linux PNs) Update node software
   - (Agent-less Windows/Linux PNs) Update PN Proxy software

5. Verify that all onQ Appliances are running the same software version. Go to Verify onQ software compatibility.

Next step: learn about any actions you take to complete the upgrade. Go to “(Start Here) Upgrade Support and Requirements” in onQ Administrator’s Guide.

7.3 (Agent-based Windows PNs) Update node software

If you're experiencing PN upgrade problems, go to Upgrade Problems.

You do not need to initiate an upgrade of the onQ Service on your agent-based PNs because onQ does this for you automatically and immediately after you initiate an onQ Appliance upgrade and from that point forward if the:

- PN is available.
- onQ is not backing up the PN or processing a recent snapshot from the PN. Otherwise, onQ performs the upgrade after the PN is no longer busy with these tasks.

If you hover-over the **DASHBOARD** tab > **PROTECTED NODES** page > **RN Status** icon, you'll see messages for the upgrade in progress.

Lastly, onQ sends alerts about the upgrade. If you aren't a recipient of such alerts, you can generate the Event Log for a given PN; this log shows the coordination that transpired between onQ and the PNs.

There is no way to disable automatic upgrades of the onQ Service. However, you can use the alternative method outlined in (Alternative) To manually install or reinstall agent-based Windows PN software: if your PNs are in a state that requires a manual upgrade.

If, at any time, you want to verify version compatibility, go to (Agent-based PNs) Verify PN software compatibility.

Related Topics

(Start Here) Upgrade Support and Requirements
Upgrade Problems
(Agent-based Linux PNs) Update node software
Get software packages

7.4 (Agent-based Linux PNs) Update node software

If you're experiencing PN upgrade problems, go to Upgrade Problems.

You do not need to initiate an upgrade of the onQ Service on your agent-based PNs because onQ does this for you automatically and immediately after you initiate an onQ Appliance upgrade and from that point forward if the:

- PN is available.
- onQ is not backing up the PN or processing a recent snapshot from the PN. Otherwise, onQ performs the upgrade after the PN is no longer busy with these tasks.

If you hover-over the **DASHBOARD** tab > **PROTECTED NODES** page > **RN Status** icon, you'll see messages for the upgrade in progress.

Lastly, onQ sends alerts about the upgrade. If you aren't a recipient of such alerts, you can generate the Event Log for a given PN; this log shows the coordination that transpired between onQ and the PNs.

There is no way to disable automatic upgrades of the onQ Service. However, you can use the alternative method outlined in (Alternative) To manually install or reinstall agent-based Windows PN software: if your PNs are in a state that requires a manual upgrade.

If, at any time, you want to verify version compatibility, go to (Agent-based PNs) Verify PN software compatibility.

To manually update an agent-based Linux PN:

1. Stop protection.

Log on to the Linux PN as `root` or `administrator`.

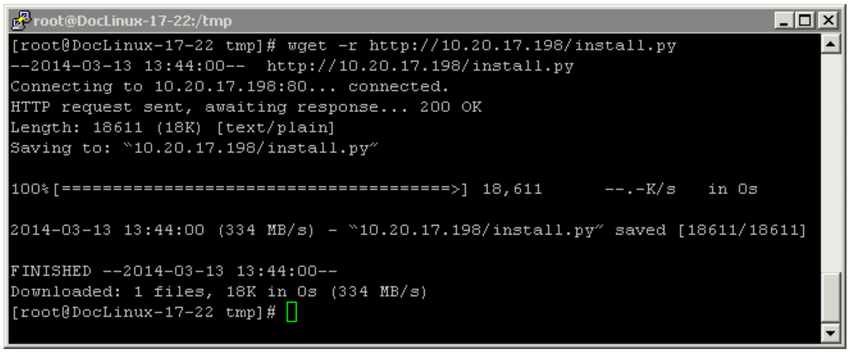
2. Install the agent software:

a. Launch the installer:

> **Note:** By default, wget preserves the original files. Newly retrieved install.py is saved with extensions `.1`, `.2`, etc. Use the `-r` option (see wget man page) to overwrite the existing file.

b. From within a folder (`/tmp`) where you want to save the install script, run the following command:

```
# wget -r http://<onQ-IP-address>/install.py
```

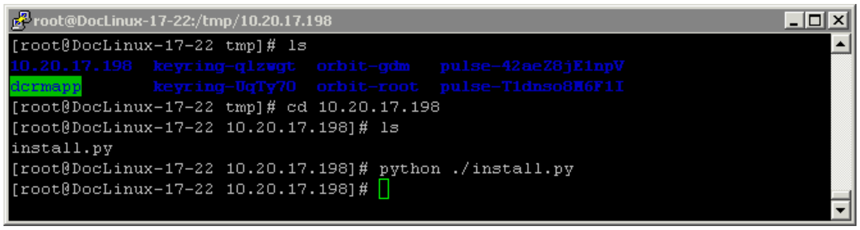


root@DocLinux-17-22:/tmp

```
[root@DocLinux-17-22 tmp]# wget -r http://10.20.17.198/install.py
--2014-03-13 13:44:00--  http://10.20.17.198/install.py
Connecting to 10.20.17.198:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18611 (18K) [text/plain]
Saving to: `10.20.17.198/install.py'

100%[=====================================>] 18,611      --.-K/s   in 0s

2014-03-13 13:44:00 (334 MB/s) - `10.20.17.198/install.py' saved [18611/18611]

FINISHED --2014-03-13 13:44:00--
Downloaded: 1 files, 18K in 0s (334 MB/s)
[root@DocLinux-17-22 tmp]#
```

c. Start the installer:

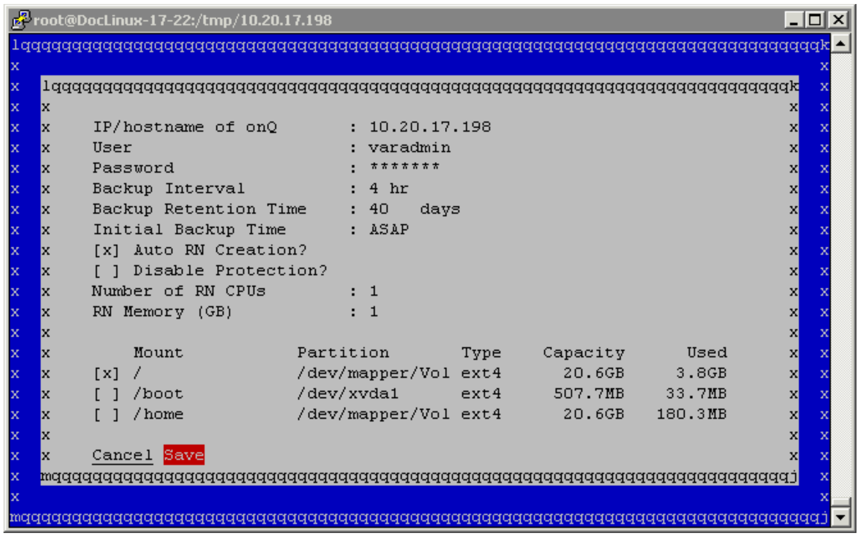
```
# cd <onQ-IP-address>
# python ./install.py
```



root@DocLinux-17-22:/tmp/10.20.17.198

```
[root@DocLinux-17-22 tmp]# ls
10.20.17.198  keyring-qlzwgt  orbit-gdm   pulse-42aeZ8jE1npV
dcrmapp       keyring-UqTy70  orbit-root  pulse-T1dnso8M6F1I
[root@DocLinux-17-22 tmp]# cd 10.20.17.198
[root@DocLinux-17-22 10.20.17.198]# ls
install.py
[root@DocLinux-17-22 10.20.17.198]# python ./install.py
[root@DocLinux-17-22 10.20.17.198]#
```

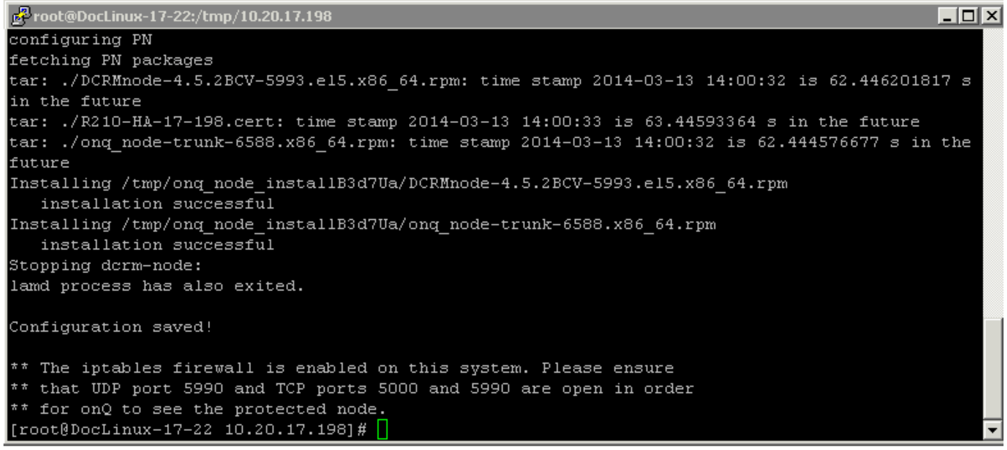
d. Type the credentials for either onQ varadmin or admin user.



```
IP/hostname of onQ       : 10.20.17.198
User                     : varadmin
Password                 : *******
Backup Interval          : 4 hr
Backup Retention Time    : 40   days
Initial Backup Time      : ASAP
[x] Auto RN Creation?
[ ] Disable Protection?
Number of RN CPUs        : 1
RN Memory (GB)           : 1

    Mount            Partition        Type    Capacity      Used
[x] /                /dev/mapper/Vol  ext4      20.6GB     3.8GB
[ ] /boot            /dev/xvda1       ext4     507.7MB    33.7MB
[ ] /home            /dev/mapper/Vol  ext4      20.6GB   180.3MB

Cancel Save
```

e. (Optional) Specify all valid values, excluding file system type and capacity because these values aren't editable, in the node parameter fields provided and modify defaults as needed. (The install utility lists all available volumes/partitions/mount points and the onQ portal enforces any file system requirements as outlined in Linux Filesystem Format Requirements.) You can make these node changes at any point after enrollment via the **Protection Config** tab in the onQ Portal.

f. Select **Save** to update/install the client node package on the Linux node.



```
configuring PN
fetching PN packages
tar: ./DCRMnode-4.5.2BCV-5993.el5.x86_64.rpm: time stamp 2014-03-13 14:00:32 is 62.446201817 s
in the future
tar: ./R210-HA-17-198.cert: time stamp 2014-03-13 14:00:33 is 63.44593364 s in the future
tar: ./onq_node-trunk-6588.x86_64.rpm: time stamp 2014-03-13 14:00:32 is 62.444576677 s in the
future
Installing /tmp/onq_node_installB3d7Ua/DCRMnode-4.5.2BCV-5993.el5.x86_64.rpm
   installation successful
Installing /tmp/onq_node_installB3d7Ua/onq_node-trunk-6588.x86_64.rpm
   installation successful
Stopping dcrm-node:
lamd process has also exited.

Configuration saved!

** The iptables firewall is enabled on this system. Please ensure
** that UDP port 5990 and TCP ports 5000 and 5990 are open in order
** for onQ to see the protected node.
[root@DocLinux-17-22 10.20.17.198]#
```

g. Wait! Do not press Enter. Was the installation successful? Use the error messages below to evaluate the screen output.

- If yes, exit the script.
- If no, press `Enter` to launch the installer UI again. Correct the problem, then repeat Step e through Step g.

Table 1: (Agent-based Linux PNs) Problems *Before* Enrollment

`Completed Successfully`
`The iptables firewall is enabled on this system....`
	Message appears in the shell, after the GUI curser exits. In addition, you’ll be instructed to open up ports.

`Incorrect/invalid values entered`	Install utility stops if you type incorrect/invalid values. Correct the problem and **Save** again or **Cancel**.
`not authorized`	You either typed the credentials incorrectly or the user account does not have root privileges.

7.5 (Agent-less Windows/Linux PNs) Update PN Proxy software

You do not need to initiate an upgrade of the PN proxies on your vCenter/ESXi server(s) because onQ does this for you automatically if the vCenter/ESXi server(s) are available. onQ regularly checks—prior to each backup—the proxy version and, if needed, will update the proxy to latest. If vCenter/ESXi server(s) aren’t available, onQ is persistent and continues to retry the upgrade process.

There is no way to disable automatic upgrades of the PN proxies. However, you can use the alternative method outlined in To re-enroll a proxy PN: if your PN proxies are in a state that requires a manual upgrade as onQ may not be able to back up your PNs otherwise.

During an upgrade, vCenter indicates that the PN’s proxy, Linux PN proxy (`LPY`_<onQhostname>_<ESXhostname>) and Windows PN proxy (`WPY`_<onQhostname>_<ESXhostname>), are shutting down and the replacement PN proxies are being deployed.

After an onQ software upgrade and a protection restart, onQ automatically upgrades all proxies, both Windows and Linux, on the ESXi hosts, if needed. Also, all proxies deployed from a specific onQ across vMotion-clustered ESXi hosts are upgraded, if needed, when the onQ software is upgraded.

The **DASHBOARD** tab > **PROTECTED NODES** page > **Connection Status** icon, indicates the upgrade in progress:

1. Before upgrade ● : solid green carat; white arrow points upward.
2. During upgrade ● : solid green carat; yellow dash.
3. After upgrade ● : solid green carat; white arrow points upward.

You know that the proxy upgraded successfully by browsing the onQ Event log in real-time: the log shows the change in proxy versions before and after the proxy upgrade.

```
12:14:52: Agentless Proxy LPY_0A141506 Service
version is 3.9-9612-6070

12:14:35: Agentless Proxy LPY_0A141506 online

12:14:29: Update of RN completed

12:13:41: Agentless Proxy LPY_0A141506 restarted

12:13:31: Stopping RN update process

12:13:31: Updating backup RN

12:13:31: Export done

12:12:51: Agentless Proxy LPY_0A141506 upgrade
complete

12:11:46: Exporting delta source image from
repository

12:11:24: Auto-upgrade of Agentless Proxy
LPY_0A141506 requested trunk-9550-6069 to 3.9-
9612-6070

12:11:18: Agentless Proxy LPY_0A141506 Service
version is trunk-9550-6069
```

Also, onQ sends alerts about the upgrade. If you aren’t a recipient of such alerts, you can generate the Event Log for a given PN; this log shows the coordination that transpired between the onQ and PN proxies on the ESXi/ESX server.

All PNs on a given ESXi server and having the same operating system (Linux or Windows) will share a common PN proxy. Therefore, when a PN proxy that is common to all PNs is being upgraded, the onQ Event log indicates that all the PNs are being upgraded. Also, the **Connection Status** icon provides the same aforementioned status for all the PNs.

7.6 Get software packages

Before you can install onQ Appliance or PN software updates, you might need to do one of the following to get the updates, though it’s very unlikely:

- Automatically download packages via onQ Central. Keep in mind that a nightly cron job automatically downloads packages as they are available; however, in the event that a package becomes available before the job is scheduled to run, you’ll need to initiate the download to get the latest package.
- Manually upload packages to the onQ Appliance because Quorum Support provides you custom packages to correct an upgrade problem.

After you upload the new software, consider deleting the old version.

To automatically download packages from onQ Central:

Before you can download Appliance software updates, you must enroll with onQ Central, a package distribution system, by installing an Appliance license as outlined in Install onQ Appliance license. onQ queries `https://updates.onqcentral.com`; therefore, ensure that your firewall is configured to allow traffic on outbound port `443`.

After onQ downloads the Appliance software updates, you can manually install them as outlined in Update Appliance software or, in the case of PNs, wait for onQ to install them automatically.

1. Log on to the onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **SOFTWARE UPGRADES** page > **Check for Updates** button.

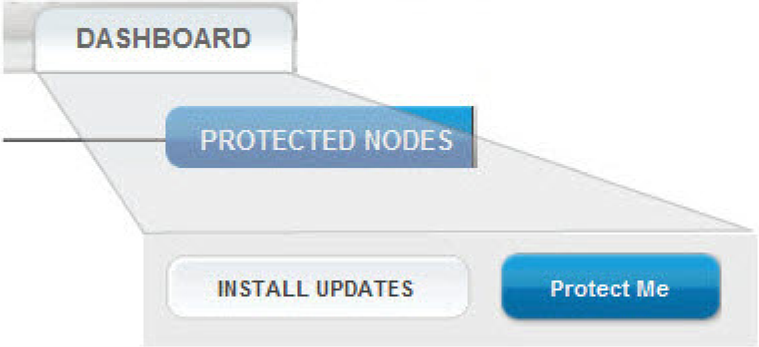
   onQ contacts onQ Central and downloads the latest updates. If a direct upgrade path is not supported for your version, onQ automatically downloads all the prerequisite updates so as to migrate your Appliance and protected nodes to the latest version.
3. Mouse-over the **Check for Updates** button to monitor the status of the download. If there are no new updates, the status indicates `No new updates are available at this time`.

   After onQ downloads the updates, they appear in the list.

Type - indicates `Auto Install` when you download the updates using the method outlined in this procedure.

Installed - indicates when the update was installed on the Appliance. This field is blank until you initiate an install of the update.

Note: The Dashboard displays an **INSTALL UPDATES** button when a package has been downloaded and is available to install. This button remains until you install all available packages:



To manually upload a package to the onQ Appliance:

Although rare, Quorum Support might ask you to upload a special package so as to fix an upgrade problem.

1. From a local computer, download the package from the onQ Download Center.
2. Log on to the onQ Portal.
3. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **Software Upgrades** page > **UPLOAD** button. The Upload SW dialog appears.

   You see a list of a variety of potential software upgrades that have been either delivered with the onQ Appliance or have been transferred to the Appliance or PN subsequent to installation.
4. **Browse** to and select the file that you saved to your local computer.
5. Specify the file type.
   - If the file has a `.qpkg` file format, it's Appliance software. Choose **Appliance SW**.
   - If the file has an `.ez` or `.msi` file format, it's PN software. Choose **Node SW**.
6. Click **Upload**.

Related Topics

Update Appliance software

7.7 Delete software packages

Upgrade packages are deployed through onQ Central. onQ Appliances and onQ Archive Vaults auto-download the necessary packages. After you install these packages, the **Type** column indicates that the package was installed via an `Auto Install`. You cannot delete Auto Install packages; however, the next time the onQ Portal downloads newer packages from onQ Central, the onQ Portal automatically cleans up (purges) the list of old Auto Install packages, keeping only the latest.

The following procedure applies if you manually installed packages. As you manually install software updates, your list of downloads grows. To keep things tidy and save on disk space, it's a good idea to delete old updates. There's never a need to revert to an older version of the software; in fact, Quorum discourages this practice.

To delete a node package:

1. Log on to the onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **Downloads** page.
3. Select the file.
4. Click the minus sign (**-**).

To delete an Appliance package:

1. Log on to the onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **Software Upgrades** page.
3. Select the file.
4. Click the minus sign (**-**).

7.8 (Agent-based Linux PNs) Uninstall node software packages

This procedure assumes that you want to uninstall and remove all PN packages.

To uninstall PN packages:

1. Log on to the Linux PN as `root`.
2. From a command line prompt, find and remove the existing node packages.

```
# pkgs=`rpm -qa|grep node`
# echo pkgs=$pkgs
# if [ "$pkgs" != "" ]; then \
rpm -e $pkgs
fi
# pkgs=`rpm -qa|grep node`
# echo pkgs=$pkgs
```

7.9 Install onQ Appliance license

Each onQ Appliance requires a license for each onQ virtual machine (also called, onQ instances) that the onQ Appliance hosts. Licensing is based on the number of onQ instances, enabling support for multi-tenant onQ Appliances, and the number of protected nodes.

Your licenses are managed by and downloaded from onQ Central, a license server and package distribution system. onQ Appliances ship with the perpetual licenses already installed. You'll need to install or reinstall the license on the onQ instance on the onQ Appliance if you want to:

- add a new perpetual license because you've expanded your configuration to include an additional onQ instance on the onQ Appliance.
- enable an onQ instance on the onQ Appliance to manage more protected nodes.
- extend an evaluation license.
- replace an evaluation license with a perpetual license.
- reinstall your perpetual license to fix a license generation problem.

To view the current license:

1. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **LICENSE** page.
2. Observe the following:
   - The serial number appears in the **onQ Instance Serial #** field. You'll need this serial number if you need to request a permanent or replacement license.
   - If you are licensed for an onQ Flex configuration, `onQ Flex` appears in the **Options** field.
   - The number of protected nodes that your license enables you to protect is the **Managed node count**.

To obtain a permanent or replacement license file:

Simply send an e-mail request to license@quorum.net, requesting a replacement license. In that email include the serial number and specify an appropriate return address.

Afterward, Quorum will advise you to do one of the following:

- **Install the license automatically** via onQ Central as outlined in (Recommended) To automatically install a license:.
- **Perform a local installation** as outlined in To manually install a license:. In this case, Quorum will email you the license as an attachment.

(Recommended) To *automatically* install a license:

1. Log on to the onQ Portal as VARadmin.
2. Configure the alerts delivery mechanism. Go to Modify e-mail alert settings.
3. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **LICENSE** page.

4. Click **Install License (QLI)** to check for the latest license on the onQ Central.
5. Wait while the onQ Manager retrieves the latest license from onQ Central, then automatically installs the license on the onQ Appliance.

   When complete, the onQ Manager returns a `License was installed` message. If your onQ Appliance is already running the latest license, the onQ Manager simply reinstalls the same license.

   If you receive either of the following error messages, contact Quorum Support:
   - `Unable to contact QuorumLabs license server...`
   - `Unable to install license...`

To *manually* install a license:

This manual process is not as elegant as allowing the onQ Appliance to do the work for you. Use this manual procedure if onQ Central is not accessible to your onQ Appliance through the internet.

1. Save the license file that Quorum provided in a location that is accessible by your browser.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **LICENSE** page.
3. Click **Install License (Local)** to load and install the license.
4. **Browse...** to the new license file, then **Upload**.

   The new license automatically installs on the onQ Appliance.

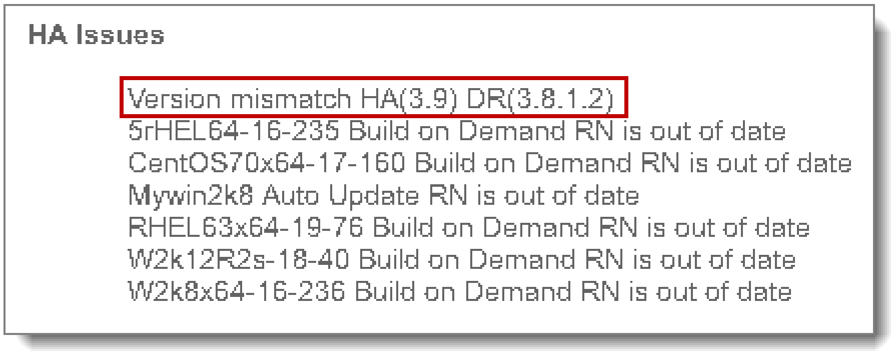
Related Topics

License Expiration and Upgrade Alerts

7.10 Verify onQ software compatibility

After an appliance upgrade, it’s important to view the software status on each onQ Appliance to determine that both Appliances are running the same component versions. If they aren’t in sync, you’ll receive many indicators:

- **DASHBOARD** tab > **onQ STATUS** page > **Issues** pane states `Version mismatch`.



HA Issues

Version mismatch HA(3.9) DR(3.8.1.2)
5rHEL64-16-235 Build on Demand RN is out of date
CentOS70x64-17-160 Build on Demand RN is out of date
Mywin2k8 Auto Update RN is out of date
RHEL63x64-19-76 Build on Demand RN is out of date
W2k12R2s-18-40 Build on Demand RN is out of date
W2k8x64-16-236 Build on Demand RN is out of date

- A0014 or A0015 alerts.
- **DR Transfer** status hover-over help states `Version mismatch`.

In this case, upgrade the outdated onQ Appliance. Quorum does not support onQ Appliances running different software versions.

As outlined in How does onQ work?, onQ is comprised of several components, which are delivered via three distinct packages. onQ Manager is aware of all the versions for each component that a given onQ Appliance is running, but onQ doesn’t disclose, in the onQ STATUS page, the version of the overall installation bundle that the onQ Appliance is running. Only Quorum Support can determine the bundle that the onQ Appliance is running.

To verify onQ Appliance software versions:

1. Log on to the onQ Appliance’s onQ Portal.
2. Go to **DASHBOARD** tab > **onQ STATUS** page.
3. Wait a few seconds while the onQ Manager performs a software inventory.

4. Compare the revisions listed in the **Version**, **Platform Status**, **Software Status** panes against all other onQ Appliances.

Related Topics

(Agent-based PNs) Verify PN software compatibility

7.11 (Agent-based PNs) Verify PN software compatibility

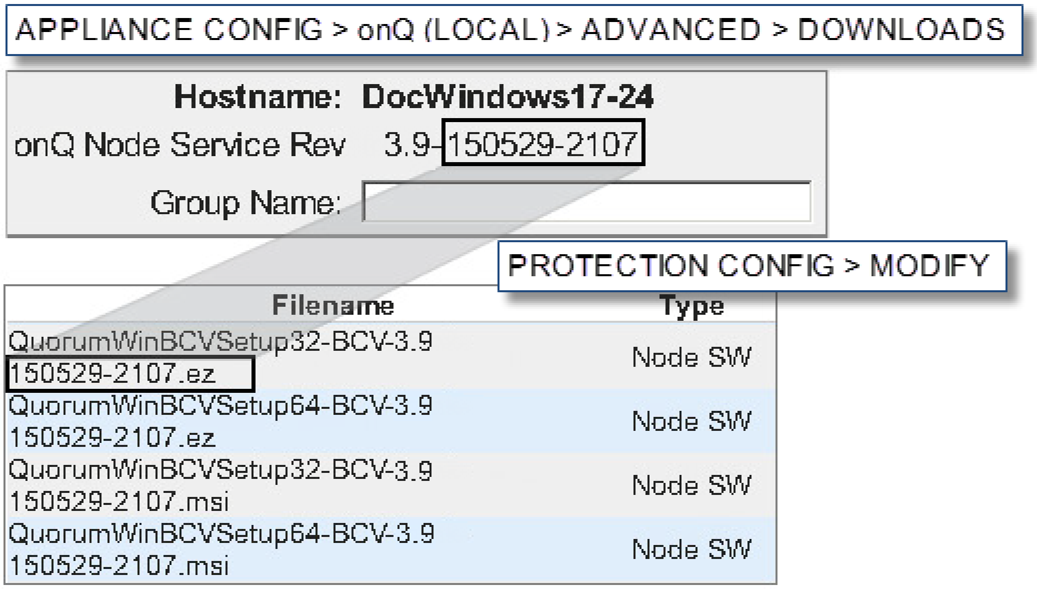
It's important to verify the software version for each PN to determine that all PNs are running an onQ Service software version that matches the onQ Appliance software version. If a given PN is running an outdated version of the onQ Service, an `Auto Update RN is out of date` error message appears in the **DASHBOARD** tab > **onQ STATUS** page > **Issues** pane.

As outlined in (Agent-based Windows PNs) Update node software and (Agent-based Linux PNs) Update node software, onQ automatically updates the PN software (onQ Service) after an onQ Appliance upgrade and, in the event that the PN is unavailable, retries after a protection restart. However, there are times when your PN never becomes available and, therefore, cannot be automatically upgraded or backed up. If a PN is outdated, restart protection to trigger the auto-upgrade process. If that doesn't work, try the troubleshooting tips in Upgrade Problems. You can use the alternative method outlined in (Alternative) To manually install or reinstall agent-based Windows PN software: if your PNs are in a state that requires a manual upgrade.

To verify onQ Service version:

1. Go to **APPLIANCE CONFIG** tab > **onQ (LOCAL)** tab > **ADVANCED** button > **DOWNLOADS** page and observe the build number in the `.ez` file.
2. In the **PROTECTION CONFIG** tab, highlight the PN, then **MODIFY**. Observe the build number in the **onQ Node Service Rev** field.

3. Compare these build numbers. They must match.



APPLIANCE CONFIG > onQ (LOCAL) > ADVANCED > DOWNLOADS

Hostname: DocWindows17-24

onQ Node Service Rev 3.9-150529-2107

Group Name:

PROTECTION CONFIG > MODIFY

Filename	Type
QuorumWinBCVSetup32-BCV-3.9 150529-2107.ez	Node SW
QuorumWinBCVSetup64-BCV-3.9 150529-2107.ez	Node SW
QuorumWinBCVSetup32-BCV-3.9 150529-2107.msi	Node SW
QuorumWinBCVSetup64-BCV-3.9 150529-2107.msi	Node SW

Related Topics

Verify onQ software compatibility

7.12 (Agent-less PNs) Verify Proxy version compatibility

You do not need to know the proxy version that's running on your vCenter/ESXi server(s). onQ is intelligent: If it detects there is a different proxy version on the vCenter/ESXi server(s) than what onQ currently has, onQ upgrades the PN proxy to that version.

As outlined in (Agent-less Windows/Linux PNs) Update PN Proxy software, onQ automatically updates the PN proxies and, in the event that the vCenter/ESXi server(s) is unavailable, continues to retry. However, you can use the alternative method outlined in To re-enroll a proxy PN: if your PN proxies are in a state that require a manual upgrade.

7.13 Specify onQ Central Proxy

If all your internet traffic goes through a firewall/proxy server, onQ Central needs to know in order to send updates to the onQ Appliance(s). This *onQ Central proxy* is not to be confused with onQ Proxy.

To specify the onQ Proxy:

1. Log on to the onQ Appliance’s onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **Software Upgrades** page.
3. Click the **onQ Central Proxy** button.
4. Specify the networking information for the proxy server, including the IP address, port, and credentials, then **SAVE**.

8

Protection

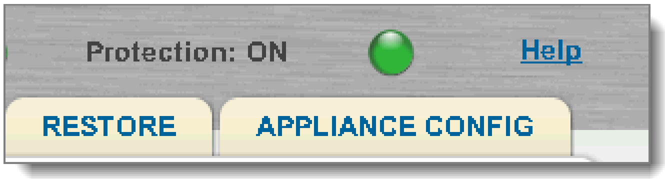
8.1 Start node protection

After you enroll protected nodes, you’re ready to protect them. The initial backup cycle and recovery node construction will take several hours to complete, but incremental snapshots are usually very fast.

To start protection:

1. Log on to either the HA’s onQ Portal or the DR Appliance’s onQ Portal.
2. From the drop-down menu, choose **Start Protection** menu option > **Start** button.

   The **Protection**:**ON** icon turns green:



8.2 Stop node protection

You must explicitly stop the protection process in order to:

- permanently delete protected nodes that no longer want to protect or back up
- add a protected node
- change any PN’s local or remote configuration
- change the hypervisor’s configuration

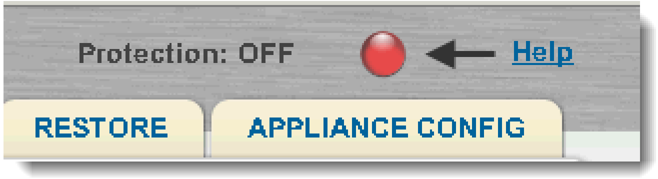
There’s no need to stop protection to stop backups for a specific PN. Instead, simply disable protection for that PN.

You can stop protection at any time, even if onQ is in the process of creating an RN or backing up a PN: onQ pauses those processes and resumes after protection starts; in short, onQ can handle such interruptions.

To stop protection:

1. Log on to either the HA's onQ Portal or the DR Appliance's onQ Portal.
2. From the drop-down menu, choose **Stop Protection** menu option > **Stop** button.

   The **Protection:OFF** icon turns red:



8.3 Restart node protection

From time to time you might need to restart protection to:

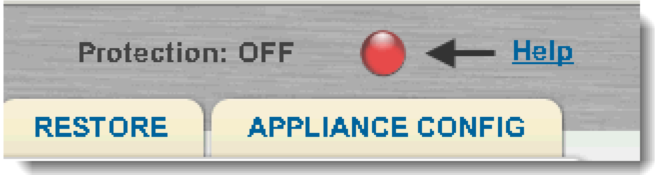
- fix a problem with onQ
- complete a PN update

You can restart protection at any time. If onQ is in the process of creating an RN or backing up a PN, those processes resume.

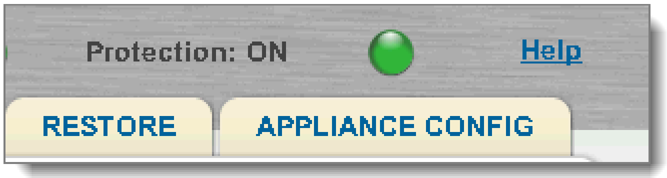
You can stop protection at any time, even if onQ is in the process of creating an RN or backing up a PN: onQ pauses those processes and resumes after protection starts; in short, onQ can handle such interruptions.

1. Log on to either the HA's onQ Portal or the DR Appliance's onQ Portal.
2. From the drop-down menu, choose **Restart Protection** menu option > **Restart** button.

After protection stops, the **Protection:OFF** icon turns red:



After protection starts, the **Protection:ON** icon turns green:



8.4 About RN Build Policies

onQ can create recovery nodes either automatically with each backup cycle or on-demand as needed. When you initially protect a PN, you must instruct onQ to use a build policy (aka build mode) for the RN. You can always change this policy. An RN build policy represents your potential downtime in the event of a disaster (aka RTO). For more information, see the topic relevant to your configuration:

- (On-Site/Prime/Plus) Modify RN build policy - onQ On-Site, onQ Prime, or onQ Plus.
- (onQ Flex) Modify RN type and/or RN build policy - onQ Flex.

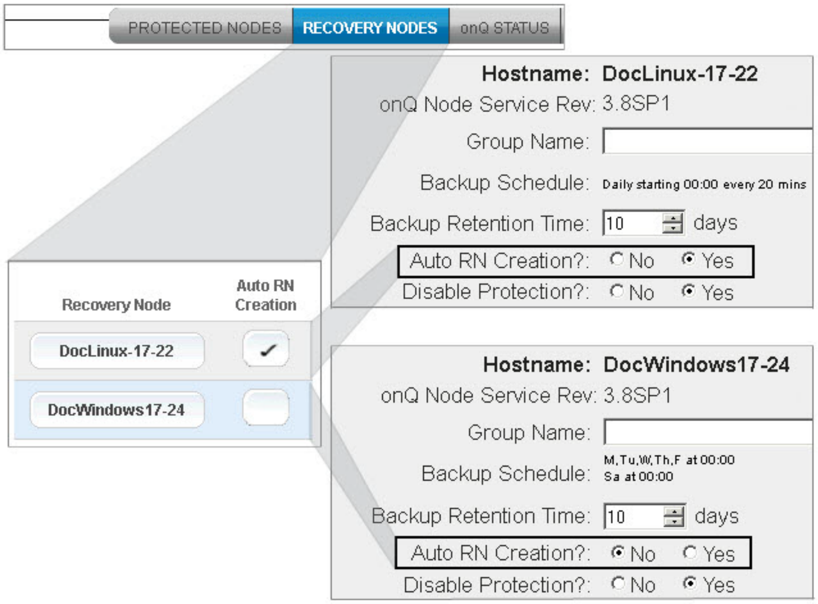
8.5 (On-Site/Prime/Plus) Modify RN build policy

Use this procedure if you have an onQ On-Site, onQ Prime, or onQ Plus configuration. In these configurations you have optimum RTO with no variable RTO costs for RN availability. If you have an onQ Flex configuration, go to (onQ Flex) Modify RN type and/or RN build policy.

onQ can create recovery nodes either automatically with each backup cycle or on-demand as needed. When you initially protect a PN, you must instruct onQ to use a build policy for the RN. You can always change this policy.

An RN can have one of the following build policies. This build policy represents your potential downtime in the event of a disaster (aka RTO).

- **Auto RN Creation=Yes** (aka *Ready-to-Run*) - Used to represent the systems in your business continuity plan that are the least tolerant of downtime. When set to `Auto RN Creation=Yes`, the RN is updated after each backup cycle, and is one-click away from taking the place of the PN. Go to "Start recovery nodes on HA" on page 342 to see how easy it is to bring an RN online.
- **Auto RN Creation=No** (aka *Build-on-Demand*) - Used to represent the systems in your business continuity plan that are the most tolerant of downtime. When set to `Auto RN Creation=No`, you must manually create this RN. This process may take a few hours or more, depending on a few factors. There must be enough disk space on the onQ Appliance to accommodate the RN.



Recovery Node	Auto RN Creation
DocLinux-17-22	✓
DocWindows17-24	

Hostname: DocLinux-17-22
onQ Node Service Rev: 3.8SP1
Group Name:
Backup Schedule: Daily starting 00:00 every 20 mins
Backup Retention Time: 10 days
Auto RN Creation?: ○ No ● Yes
Disable Protection?: ○ No ● Yes

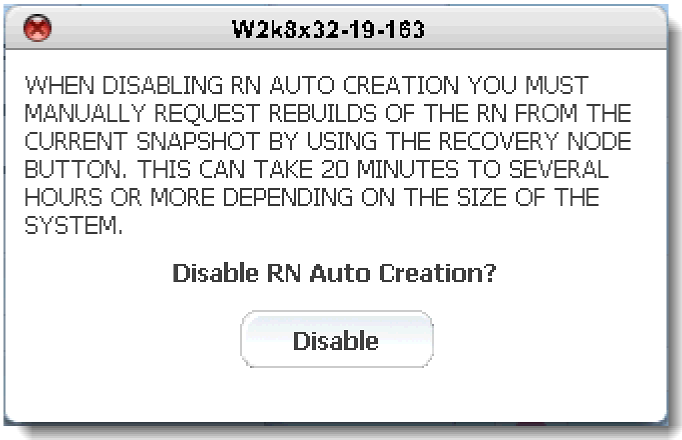
Hostname: DocWindows17-24
onQ Node Service Rev: 3.8SP1
Group Name:
Backup Schedule: M,Tu,W,Th,F at 00:00
Sa at 00:00
Backup Retention Time: 10 days
Auto RN Creation?: ● No ○ Yes
Disable Protection?: ○ No ● Yes

To change the build policy:

1. Log on to the HA's onQ Portal.
2. Go to **DASHBOARD** tab > **RECOVERY NODES** page.
3. Unlock the page.

4. Do one of the following:
   - (All RNs) Click either the **ALL BoD** or **ALL AUTO** button at the bottom of the page. A dialog appears. Click **Disable/Enable** button to switch all RNs to a given policy.
   - (Single RN) Click the **Auto RN Creation** button next to the RN. A dialog appears. Click **Disable/Enable** button to switch to the other policy.

   If you attempt to disable `Auto RN Creation`, the following warning appears:

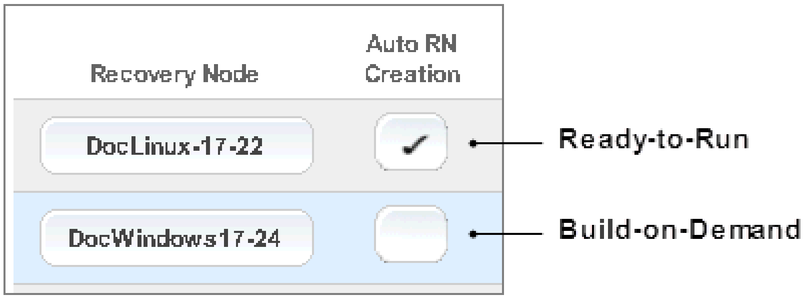


W2k8x32-19-163

WHEN DISABLING RN AUTO CREATION YOU MUST MANUALLY REQUEST REBUILDS OF THE RN FROM THE CURRENT SNAPSHOT BY USING THE RECOVERY NODE BUTTON. THIS CAN TAKE 20 MINUTES TO SEVERAL HOURS OR MORE DEPENDING ON THE SIZE OF THE SYSTEM.

Disable RN Auto Creation?

The acronym `BoD` (Build-on-Demand) appears next to the RN Status icon (HA) or RN Ready Status icon if `Auto RN Creation` is set to disabled.



Recovery Node	Auto RN Creation
DocLinux-17-22	✓
DocWindows17-24	

Related Topics

(onQ Flex) Build recovery nodes

(onQ Flex) Modify RN type and/or RN build policy

8.6 (onQ Flex) Modify RN type and/or RN build policy

Use this procedure if you have an onQ Flex configuration. In this configurations you have a flexible RTO with variable RTO costs for RN availability. If you have an onQ On-Site, onQ Prime, or onQ Plus configuration, go to (On-Site/Prime/Plus) Modify RN build policy.

onQ can create recovery nodes either automatically with each backup cycle or on-demand as needed. An RN in an onQ Flex configuration can have one of the following build policies (aka build modes) and RN types. The build policy represents your RTO (Recovery Time Objective) and the RN type indicates your preferred RTO cost (or plan) for that objective. All newly enrolled PNs default to *Build-on-Demand* (build policy) and *OD* (RN type). You can change the build policy and RN type at any time.

Build policies: ✓

- **Auto RN Creation=Yes** (aka *Ready-to-Run*) - Used to represent the systems in your business continuinty plan that are the least tolerant of downtime. When set to `Auto RN Creation=Yes`, the RN is updated after each backup cycle, and is one-click away from taking the place of the PN. Go to “Start recovery nodes on HA” on page 342 to see how easy it is to bring an RN online.
- **Auto RN Creation=No** (aka *Build-on-Demand*) - Used to represent the systems in your business continuinty plan that are the most tolerant of downtime. When set to `Auto RN Creation=No`, you must manually build this RN. This process may take a few hours or more, depending on a few factors. There must be enough disk space on the onQ Appliance to accommodate the RN.

RN types:

- **R2R** - Reiterates that you prefer a Ready-to-Run objective—the highest level of RN availability—and indicates that you want a monthly service charge for this RN. You must set this RN type independently of the RN’s build policy.
- **OD** - Reiterates that you prefer a Recovery-on-Demand objective to conserve Hybrid Cloud resources and to aim for lower upfront costs by creating RNs less frequently and only as they are needed. Indicates that you want to be charged a flat price per RN build. You must set this RN type independently of the RN’s build policy.

RN type is independent of the build policy so as to account for specific disaster scenarios: under normal circumstances an RN that’s set to `Auto RN Creation=Yes` should use the most recent snapshot; however, if you know that a backup is corrupt, you need your RN to run an older snapshot version—and you don’t want the RN to be overwritten by the most recent snapshot after the next backup. To achieve this goal, whenever you create an RN from an old backup, onQ automatically sets the RN to `Auto RN Creation=No`.

When you make changes to the build policy, onQ does not automatically change the RN type and, therefore, does not change the RTO cost:

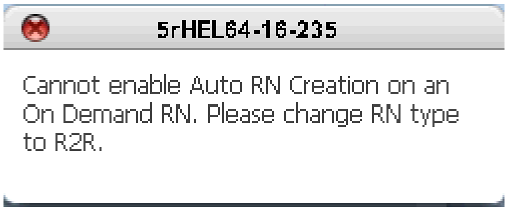
RN Type	If you change build policy to:	RTO Cost
R2R	✓ Auto RN Creation=Yes	Default. No change to RN type. Reoccurring charge per R2R RN.
	Auto RN Creation=No	No change to RN type. Reoccurring charge per R2R RN. If you desire a flat price per build, change RN type to OD.
OD	✓ Auto RN Creation=Yes	Cannot enable Auto RN Creation when RN type is OD. onQ Flex dialog reminds you to manually change RN type to R2R, then enable Auto RN Creation; if you do so, the result is a reoccurring charge per R2R RN.

To change the RN type:

1. Launch the onQ Flex Manager.
2. From the onQ Flex Manager, click **Change RN Type** button > **Convert RN** button.

To change the build policy:

Before You Begin: If the RN type is set to R2R and you want to enable Auto RN Creation, change the RN type to OD, then change the build policy.

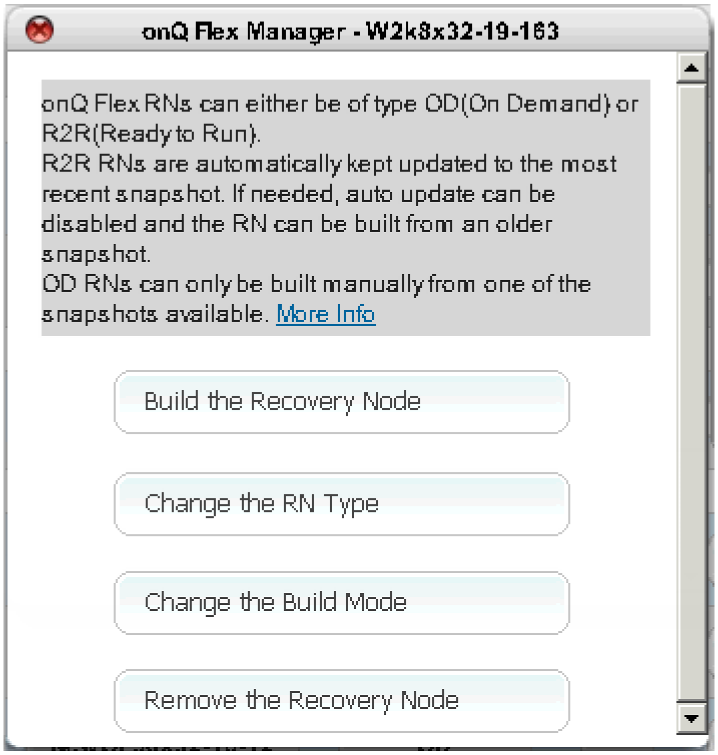


5rHEL64-16-235

Cannot enable Auto RN Creation on an On Demand RN. Please change RN type to R2R.

1. Log on to the HA’s onQ Portal.
2. Go to **DASHBOARD** tab > **RECOVERY NODES** page.
3. Unlock the page.
4. Click the **Auto RN Creation** button next to the RN, or simply launch the onQ Flex Manager using any of the available methods.

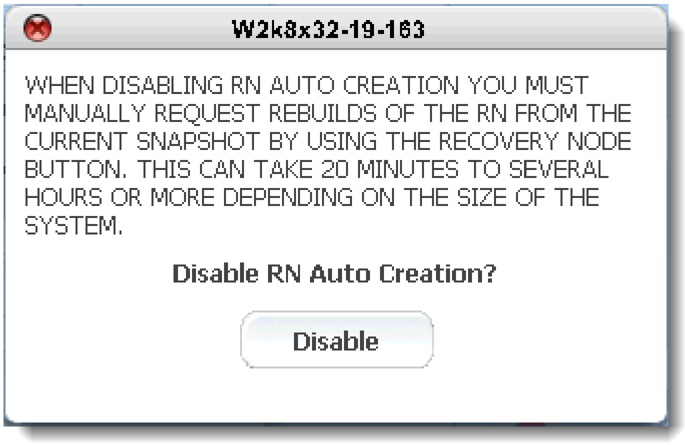
   A dialog appears:



onQ Flex Manager - W2k8x32-19-163

onQ Flex RNs can either be of type OD(On Demand) or R2R(Ready to Run).
R2R RNs are automatically kept updated to the most recent snapshot. If needed, auto update can be disabled and the RN can be built from an older snapshot.
OD RNs can only be built manually from one of the snapshots available. More Info

5. Click on the **Change the Build Mode** button. If you attempt to disable `Auto RN Creation`, the following warning appears:



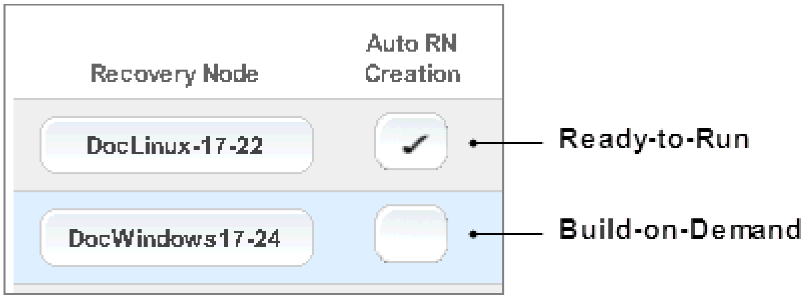
W2k8x32-19-163

WHEN DISABLING RN AUTO CREATION YOU MUST MANUALLY REQUEST REBUILDS OF THE RN FROM THE CURRENT SNAPSHOT BY USING THE RECOVERY NODE BUTTON. THIS CAN TAKE 20 MINUTES TO SEVERAL HOURS OR MORE DEPENDING ON THE SIZE OF THE SYSTEM.

Disable RN Auto Creation?

6. Click **Disable/Enable** button to switch to the other policy.

   The acronym `BoD` (Build-on-Demand) appears next to the RN Status icon (HA) or RN Ready Status icon if `Auto RN Creation` is set to disabled.



Recovery Node	Auto RN Creation
DocLinux-17-22	✓
DocWindows17-24	

Related Topics

(On-Site/Prime/Plus) Modify RN build policy
About onQ Flex
“onQ Flex Limitations” in onQ Release Notes

8.7 Disable protection of nodes

If you disable protection, the most recent re-build of the recovery node is retained but backups are suspended.

If you disable protection while a backup is in progress or an RN is being rebuilt, that process continues to completion but further backups are suspended. You can re-enable protection at any time.

To disable protection of a node when *Protection is On*:

1. Log on to the HA's onQ Portal.
2. Go to **DASHBOARD** tab > **PROTECTED NODES** page.
3. Unlock the page.
4. Do one of the following:
   - (All PNs) Click on the **DISABLE ALL** button at the bottom of the page, then click **DISABLE** to change protection for all PNs.
   - (Group of PNs) For the group, click the **Protection Disabled** (🛡) button.
   - (Single PN) Locate the **Protection Disabled** column**.** When you click a button in this column, protection toggles between enabled and disabled for the indicated node.

   A check mark appears in the field if protection is disabled. Otherwise it is blank.

To disable protection of a node when *Protection is Off*:

1. Log on to the HA's onQ Portal.
2. From the **PROTECTION CONFIG** tab, select the node, then click the **MODIFY** button.
3. Select the **Disable Protection?: Yes** radio button, then **SAVE**.

Related Topics

"Enable protection of nodes" on page 249

8.8 Enable protection of nodes

If you subsequently disabled protection of a PN, you can re-enable at any time. When you re-enable protection, backups resume and subsequent RN rebuilds are based on the retained RN.

To enable protection of a node when *Protection is On*:

1. Log on to the HA’s onQ Portal.
2. Go to **DASHBOARD** tab > **PROTECTED NODES** page.
3. Unlock the page.
4. Do one of the following:
   - (All PNs) Click on the **ENABLE ALL** button at the bottom of the page, then click **ENABLE** to change protection for all PNs.
   - (Single PN) Locate the **Protection Disabled** column**.** When you click a button in this column, protection toggles between enabled and disabled for the indicated node.

   A check mark appears in the field if protection is disabled. Otherwise it is blank.

Related Topics

“Disable protection of nodes” on page 247

8.9 Cancel RN updates

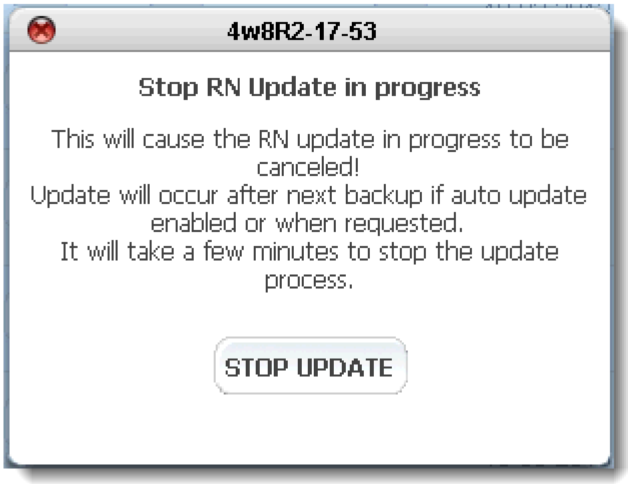
onQ builds Recovery Nodes in the order that they are listed in the onQ Portal. If the first RN in the list has a lot of incremental changes that onQ needs to apply, the other RNs awaiting updates must wait for the first RN update to complete. In this case, you might want to cancel the update for the highest priority RN so as to eliminate the bottleneck.

The RN's next update, which will presumably include even more incremental changes than the update you canceled, will automatically occur as scheduled. If, after the queue clears, you want to immediately apply incremental changes to the RN you can increase its priority by modifying the policy for all but the one RN to BoD as outlined in (On-Site/Prime/Plus) Modify RN build policy, then restart protection; however, this approach might be overkill.

To cancel a RN update that is in progress:

You cannot cancel/stop and RN update if a self-test is running.

1. Log on to the HA's onQ Portal.
2. Go to **DASHBOARD** tab > **PROTECTED NODES** page.
3. Unlock the page.
4. Click on the **RN Status** button next to the recovery node, then click **STOP RN UPDATE** button.



4w8R2-17-53

Stop RN Update in progress

This will cause the RN update in progress to be canceled!
Update will occur after next backup if auto update enabled or when requested.
It will take a few minutes to stop the update process.

8.10 Disable replication *globally*

Use this procedure to disable backup transfers for all PNs. If you want to disable backup transfers for a given PN, simply disable replication for that PN only.

Quorum does not recommend that you disable backup transfers globally, unless your configuration is an HA-only configuration, meaning you don't have a DR Appliance; if you have an HA-only configuration, disabling all snapshot transfers saves space and improves performance on your HA.

However, there are situations in which you might need to *temporarily* disable snapshot transfers globally. Before you do so, you must have enough disk space to accumulate backups.

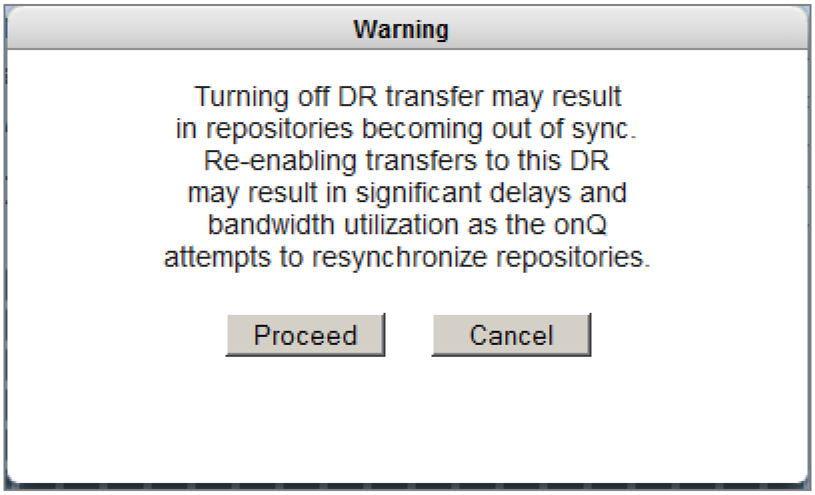
If the HA cannot communicate with the DR Appliance, it will retain the backups in its queue and transfer them when the DR Appliance comes online.

An alternative to disabling all transfers is stopping protection on the HA so as to keep the repositories in sync, but the downside is that the HA will not perform any backups until you turn on protection. This method is not recommended. Besides, when you re-enable transfers, the repositories will resync automatically.

To disable replication *globally*:

1. Log on to the onQ Appliance's onQ Portal.
2. Ensure that your onQ Appliance has enough disk space to accumulate backups. For the related alert, go to Recovery Node and PN Disk Space Alerts.
3. Go to **APPLIANCE CONFIG** tab > **onQ (REMOTE)** page > **MODIFY** button.
4. Do one of the following:
   - (Recommended) Set the bandwidth to zero.
   - Change the DR Appliance's/DR Mirror's IP address to an unused IP address or disconnect the DR Appliance/DR Mirror from the network.
5. Stop protection.

6. In the **Enable DR Transfer?** field, select the **No** radio button, then **Proceed**.



Warning

Turning off DR transfer may result in repositories becoming out of sync. Re-enabling transfers to this DR may result in significant delays and bandwidth utilization as the onQ attempts to resynchronize repositories.

Disable Transfer: ON icon no longer displays at the top of each UI page on the onQ Appliance.

7. Start protection.

Related Topics

Enable replication globally
Disable replication for individual nodes

8.11 Disable replication for *individual* nodes

Use this procedure to disable transfers for a given PN. If you want to disable transfers for all your PNs, disable replication globally.

You might want to disable replication for a specific PN if it is not important for business continuity, but you do want backups and the ability to archive them.

With protection *enabled* and replication *disabled*, the HA Appliance continues to back up the node, but it will *not* be available on the DR Appliance in the event of a disaster. You can re-enable replication at any time.

To disable replication for a single PN:

1. Log on to the HA's onQ Portal.

2. From the **PROTECTION CONFIG** tab, select the node, then click the **MODIFY** button.
3. Verify that **Disable Protection?:Yes**. You need protection on to enable PN backups.
4. Click the **ADVANCED** tab, then select the **Disable DR Replication?:Yes** radio button, then **SAVE**.

Related Topics

Enable replication for individual nodes
Disable replication globally

8.12 Enable replication *globally*

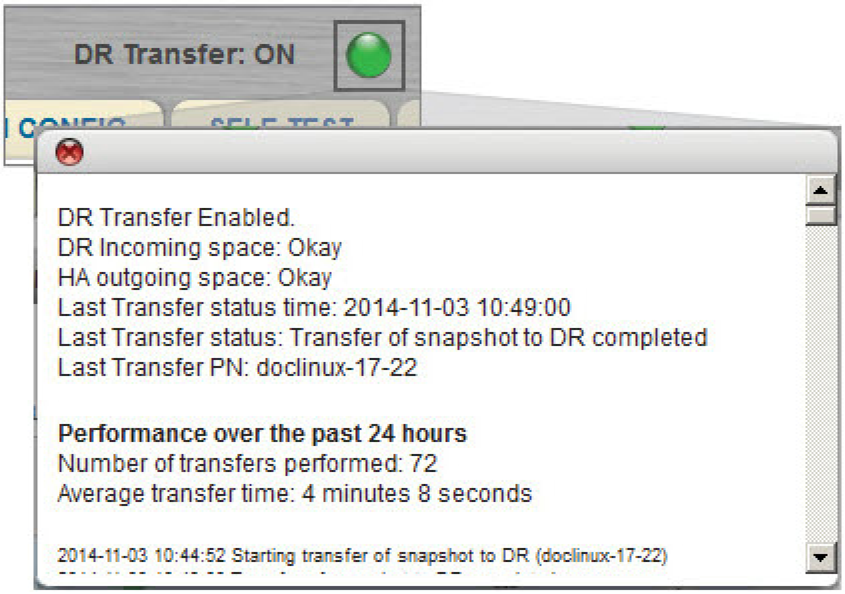
If you subsequently disabled backup transfers globally, you can re-enable at any time. You may experience significant delays and more than usual bandwidth utilization as the onQ resynchronizes the HA Repository and the DR Repository.

To enable replication globally:

1. Log on to the onQ Appliance's onQ Portal.
2. Stop protection.
3. Go to **APPLIANCE CONFIG** tab > **onQ (REMOTE)** page > **MODIFY** button.
4. In the **Enable DR Transfer?** field, select the **Yes** radio button, then **SAVE**.

   Disable Transfer: OFF displays at the top of each UI page on the onQ Appliance.
5. Start protection.

   Disable Transfer: ON displays at the top of each UI page on the onQ Appliance.



DR Transfer Enabled.
DR Incoming space: Okay
HA outgoing space: Okay
Last Transfer status time: 2014-11-03 10:49:00
Last Transfer status: Transfer of snapshot to DR completed
Last Transfer PN: doclinux-17-22

Performance over the past 24 hours
Number of transfers performed: 72
Average transfer time: 4 minutes 8 seconds

```
2014-11-03 10:44:52 Starting transfer of snapshot to DR (doclinux-17-22)
```

Related Topics

Disable replication globally
Disable replication for individual nodes

8.13 Enable replication for *individual* nodes

If you subsequently disabled replication for a specific PN, you can re-enable at any time.

To re-enable replication for a single PN:

1. Log on to the HA’s onQ Portal.
2. From the **PROTECTION CONFIG** tab, select the node, then click the **MODIFY** button > **ADVANCED** button.
3. Select the **Disable DR Replication?: No** radio button, then **SAVE**.
4. Initiate two immediate backups, and wait for two successful backup transfers.

   onQ automatically restores the full snapshot of that PN and transfers that snapshot and the delta snapshot for the next backup to the DR. However, onQ does so based on the PN's preconfigured backup schedule. Quorum recommends that you leapfrog the onQ by executing the backup immediately so as to put the DR into a healthy state as soon as possible.

Related Topics

Disable replication for individual nodes
Enable replication globally

8.14 Manage hosts

An onQ Appliance maintains a table that enables the onQ Appliance to resolve host names to their IP address. Quorum recommends that you include all protected nodes as well as any external nodes. Define these nodes on both the HA Appliance and the DR Appliance. This best practice ensures hostname resolution in the event that your DNS server fails or if you have a site failure.

To add a host:

1. Log on to the Appliance's onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **HOSTS** page.

   You see a list showing IP address and names of hosts that cannot be resolved by DNS.
3. Click the plus button (**+**).
4. Type the IP Address and hostname in the fields provided, then **SAVE** (or **RESET** to discard your changes).

To delete a host:

If you've removed a node from protection because it's no longer in your production environment, you can delete it from the list of hosts, to keep things tidy. However, if you intend to add the node later, there's really no harm in leaving the host in the list.

1. Log on to the Appliance's onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **HOSTS** page.
3. Select the host form the list, then click the minus button (**-**), then **YES** to confirm.

To edit an existing host:

1. Log on to the Appliance's onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **HOSTS** page.
3. Select the host from the list, then **MODIFY**.
4. Change the IP address or hostname in the fields provided, then **SAVE**.

8.15 Resize protected node’s vdisk

As outlined in “(Agent-based PNs) Add protected nodes manually” on page 184, a protected node’s virtual disk (vdisk) requires a specific amount of disk space.

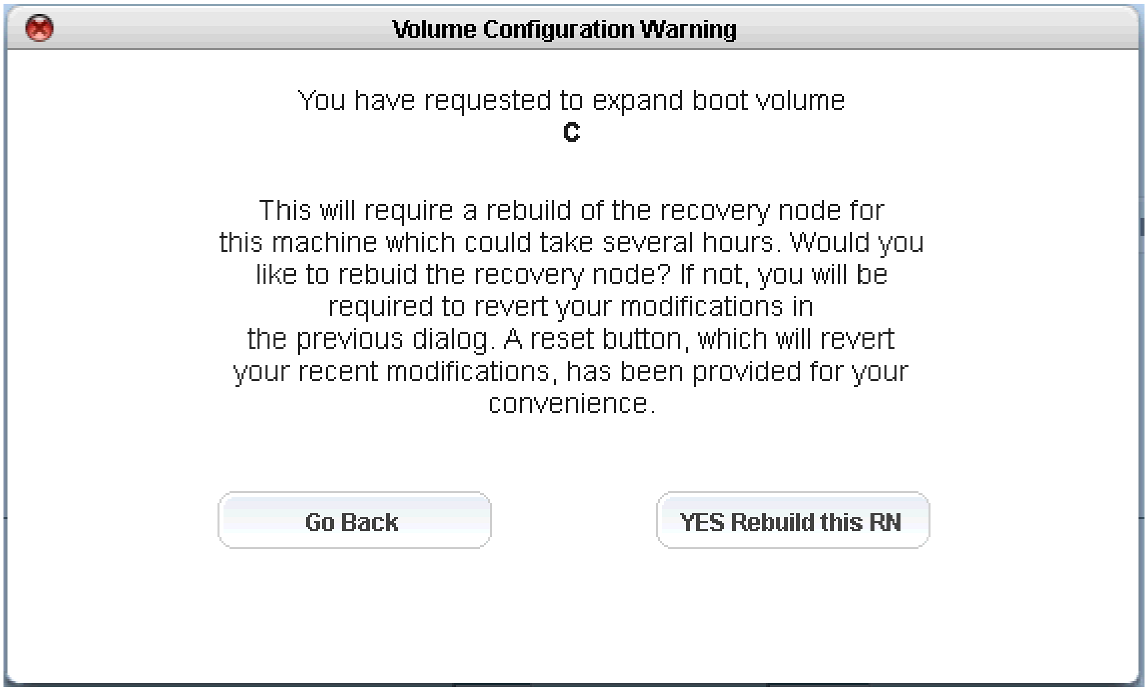
onQ alerts you (see “Recovery Node and PN Disk Space Alerts” on page 508) when your protected node’s vdisk capacity used exceeds 90%. If you wait until a vdisk fills up, onQ cannot protect that protected node.

- If you decrease the size of the vdisk for any volume, you must rebuild the entire RN.
- If you increase or decrease the size of `C:\`, you must rebuild the entire RN.
- If you increase the size of a vdisk for any drive/volume other than `C:\`, you do *not* need to rebuild the RN because onQ simply adds an additional vdisk for the delta. However, there is one exception. An RN is limited to a total of 15 vdisks. If you exceed this limit, the onQ Portal prompts you to rebuild the RN so that onQ can consolidate the vdisks and provide you the vdisk size that you requested.

To resize a vdisk:

1. Log on to the HA’s onQ Portal.
2. Go to **PROTECTION CONFIG** tab, select the protected node, then click **MODIFY**.
3. Specify a new size for the vdisk, then **SAVE**.

If prompted, click **YES Rebuild this RN**.



Volume Configuration Warning

You have requested to expand boot volume
C

This will require a rebuild of the recovery node for this machine which could take several hours. Would you like to rebuid the recovery node? If not, you will be required to revert your modifications in the previous dialog. A reset button, which will revert your recent modifications, has been provided for your convenience.

Related Topics

Recovery Node and PN Disk Space Alerts
Monitor disk space and memory usage

8.16 Enable and disable DR Mirroring

A typical onQ configuration consists of an HA and a DR Appliance, providing high availability. However, if you prefer additional protection in the event that your HA and your DR Appliance are unavailable, you can expand your existing configuration to include a DR Mirror.

DR mirroring enables you to replicate the data in the DR repository to another onQ Appliance, a *DR Mirror*. A DR Mirror is identical to the DR Appliance. The data moves from the HA to the DR Appliance, as usual. The only difference is that, with DR mirroring, the DR Appliance transfers/replicates the data on to the DR Mirror.

In a typical DR mirroring configuration, there are 3 different appliances: HA, DR Appliance, *and* DR Mirror. However, you can “daisy-chain” as many DR Mirrors as you would like; in this case, the DR Appliance is chained to the first DR Mirror, and the first DR Mirror is chained to the second DR Mirror (and so on) by way of trust relationships.

After an initial configuration, do not disable DR mirroring as outlined below.

To enable DR mirroring:

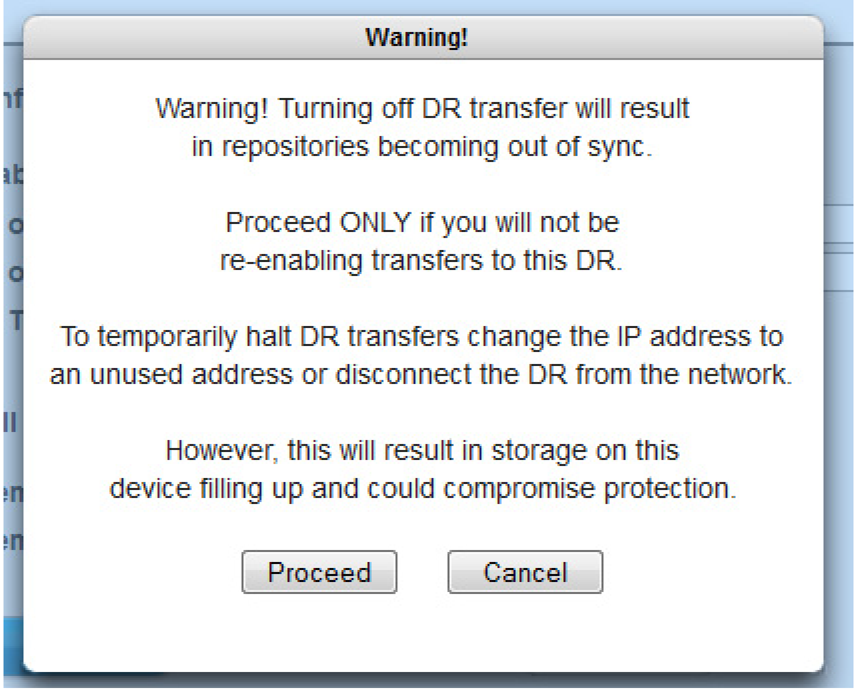
1. Log on to the DR Appliance or DR Mirror’s onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **onQ (REMOTE)** page.
3. Click **Modify**. The **Modfiy Remote onQ Setup** page appears.
4. Select the **Enable DR Mirroring?: Yes** radio button.
5. In the drop-down text boxes provided, specify the networking parameters for the DR Mirror.

   Mirror onQ is the DR Mirror that you want to mirror. A DR Mirror can mirror a DR Appliance or, in the case of multiple DR Mirrors, the next DR Mirror in the chain.
6. Click **SAVE**.

To disable DR mirroring:

Before you disable DR mirroring, ensure that your onQ Appliance has enough disk space to accumulate backups.

If you need to temporarily stop transfers, change the DR Mirror’s IP address to an unused address or disconnect the DR Mirror from the network, as the warning below advises:.



Warning!

Warning! Turning off DR transfer will result in repositories becoming out of sync.

Proceed ONLY if you will not be re-enabling transfers to this DR.

To temporarily halt DR transfers change the IP address to an unused address or disconnect the DR from the network.

However, this will result in storage on this device filling up and could compromise protection.

If the DR Appliance cannot communicate with the DR Mirror, it will retain the backups in its queue and transfer them when the DR Mirror comes online.

Stopping protection on the HA will also keep the repositories in sync, but the downside is that the HA will not perform any backups until you turn on protection. This method is not recommended.

Related Topics

Step 2: Configure the onQ Appliances
Set up trust relationships

8.17 Enroll and Disenroll onQ Archive Vault

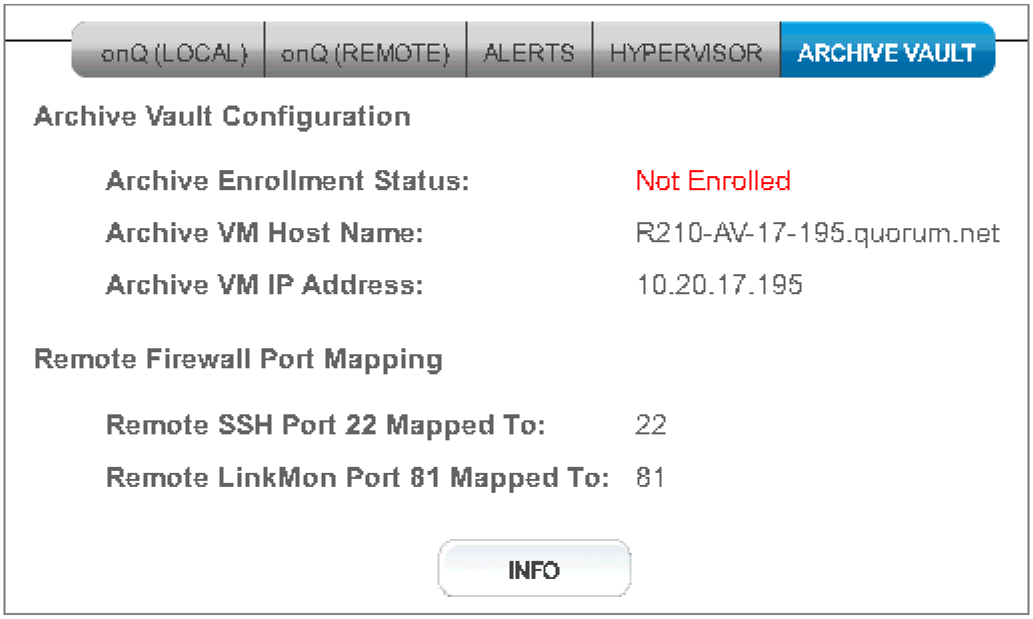
When you disenroll an onQ Archive Vault on the onQ Appliance, the AV disables all the jobs that correspond to that onQ Appliance.

To learn about enrollment, go to Monitor onQ Archive Vault enrollment or refer to the AV online help.

To disenroll onQ Archive Vault:

1. Log on to the onQ Appliance's onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ARCHIVE VAULT** page.
3. Click on the **Disenroll** button.

   The **Disenroll** button now reads **Info**, and the **Archive Enrollment Status** is `Not Enrolled`:



Archive Vault Configuration

Archive Enrollment Status: Not Enrolled

Archive VM Host Name: R210-AV-17-195.quorum.net

Archive VM IP Address: 10.20.17.195

Remote Firewall Port Mapping

Remote SSH Port 22 Mapped To: 22

Remote LinkMon Port 81 Mapped To: 81

Related Topics

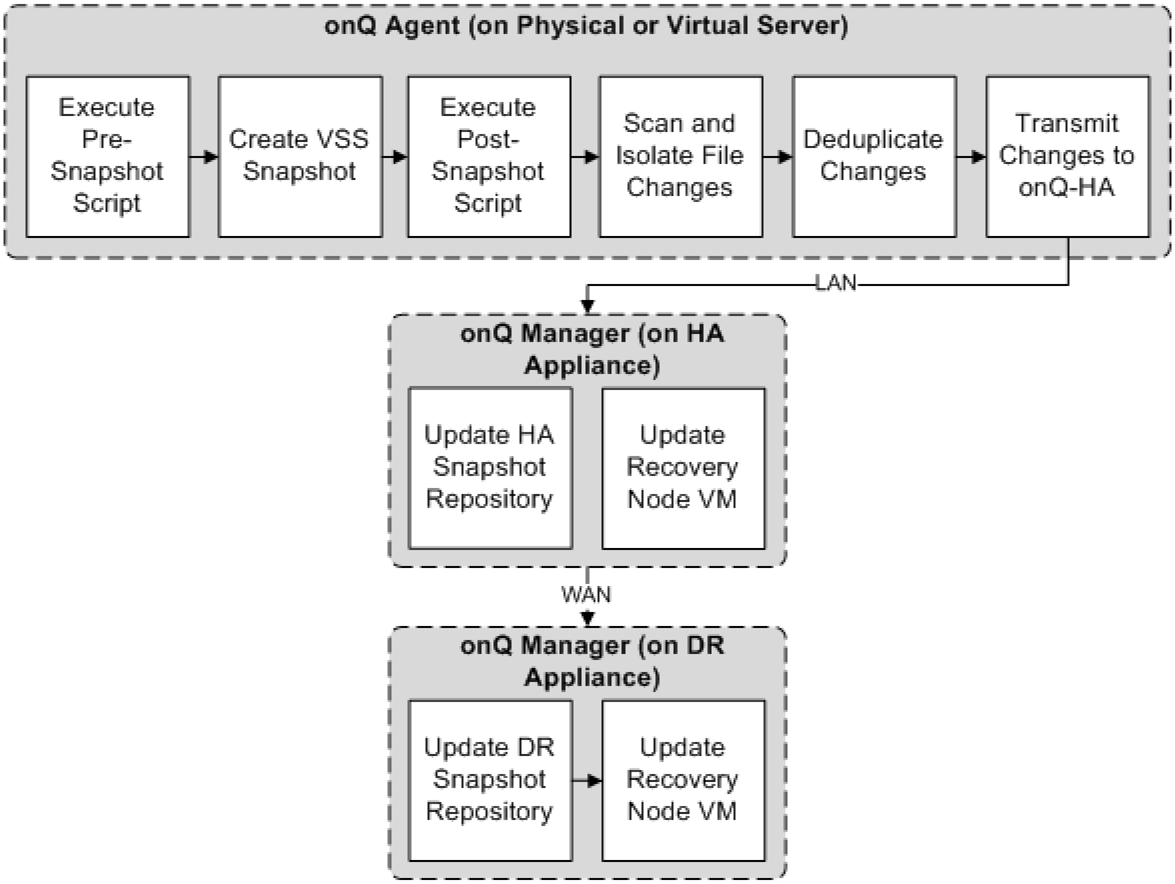
Monitor onQ Archive Vault enrollment

9

Backup and Restore

9.1 Backup and Recovery Workflow

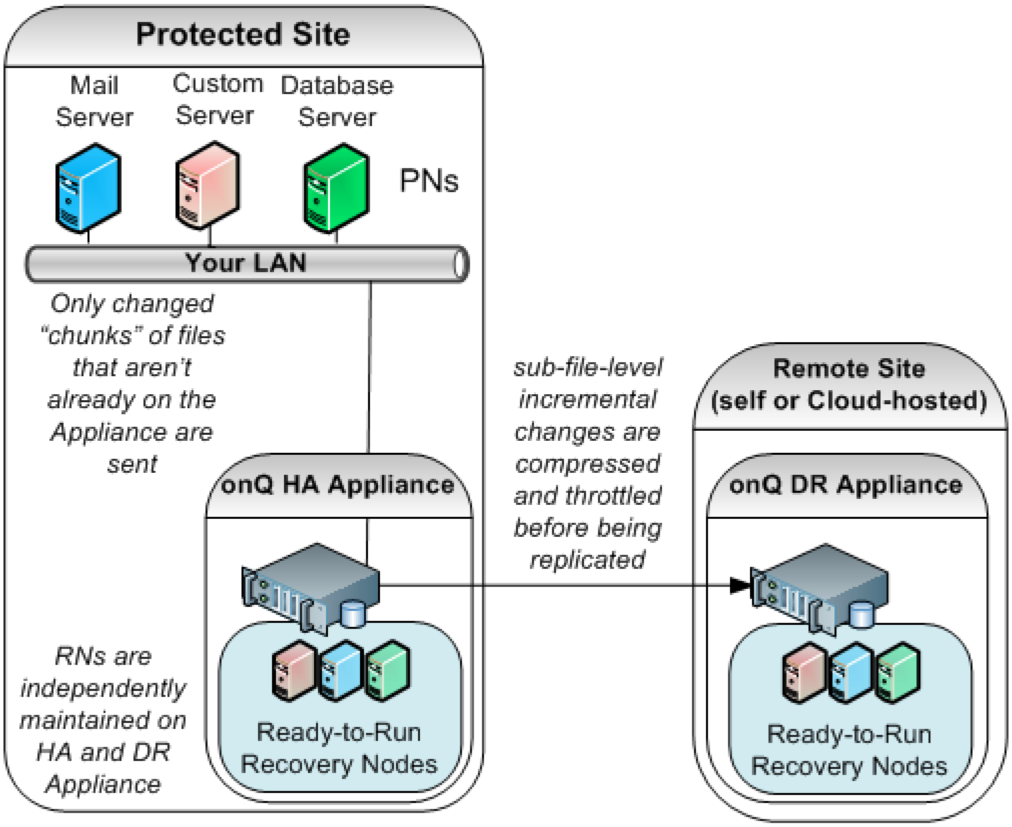
The repository is the deduplicated archive of all snapshots of all of your Protected Nodes. From the repository, onQ can reproduce a complete system image from any snapshot.


onQ Agent (on Physical or Virtual Server)
Execute Pre-Snapshot Script
Create VSS Snapshot
Execute Post-Snapshot Script
Scan and Isolate File Changes
Deduplicate Changes
Transmit Changes to onQ-HA
LAN
onQ Manager (on HA Appliance)
Update HA Snapshot Repository
Update Recovery Node VM
WAN
onQ Manager (on DR Appliance)
Update DR Snapshot Repository
Update Recovery Node VM

onQ provides HA and DR protection in the following way:

- At scheduled intervals, the onQ Manager takes crash-consistent, open-file incremental snapshots of your Protected Nodes.
- The snapshot is deduplicated, so only the changed files (or changed parts of large files) are sent to the HA.
- The HA adds the changes to the repository and then compresses and sends the changes to the DR site.
- Ready-to-run recovery nodes are created on the HA.

- Ready-to-run recovery nodes are created on the DR Appliance.
- The onQ Manager monitors the health of your PNs. If the onQ Manager detects a PN or backup failure, the onQ Manager issues an email alert. You can then determine if the condition of the PN requires that you start the HA or DR recovery nodes using the onQ Portal.


Protected Site
Mail Server
Custom Server
Database Server
PNs
Your LAN
Only changed "chunks" of files that aren't already on the Appliance are sent
onQ HA Appliance
Ready-to-Run Recovery Nodes
RNs are independently maintained on HA and DR Appliance
sub-file-level incremental changes are compressed and throttled before being replicated
Remote Site (self or Cloud-hosted)
onQ DR Appliance
Ready-to-Run Recovery Nodes

Related Topics

Seed the DR Repository
Initiate immediate backups
Resize protected node's vdisk

9.2 Edit RN services list

A Recovery Node (RN) services list is a list of services that can run on a given PN. Some services installed on a PN will cause problems if they attempt to run on the RN. In this case, you can configure the startup settings for these services.

The onQ Portal provides a default RN services list that includes all known services that are problematic. For this reason, the start option is set to `Disabled`. Alternatively, the onQ Portal enables you to retrieve a comprehensive list of services from which you can build your own custom list.

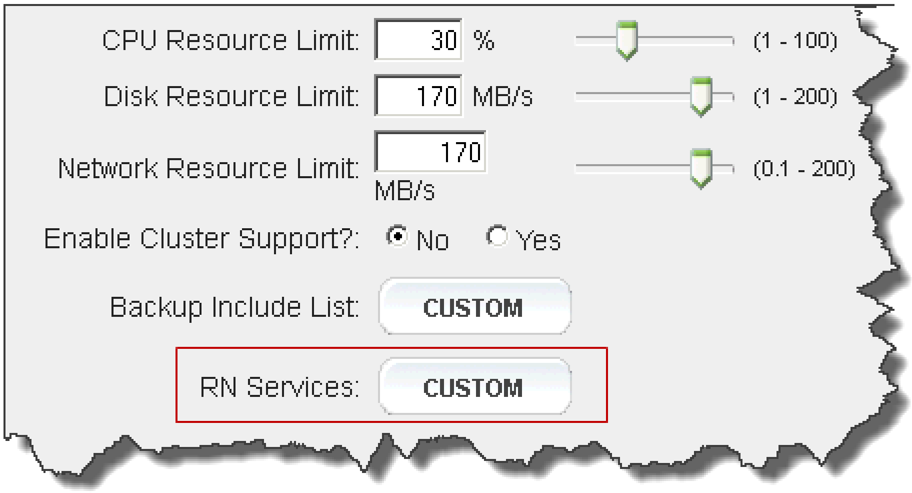
- If a custom list exists for an RN, the onQ Portal uses that list instead of the defaults list.
- If you later delete the PN, the onQ Portal deletes the custom list for that PN.

To specify the start option for a service:

This procedure assumes that you’re modifying the RN services list for an existing protected node. However, you can perform this procedure from either the **Add Protected Node** page or the **Modify Protected Node** page.

1. Log on to the HA’s onQ Portal.
2. Click the **PROTECTION CONFIG** tab.
3. Select the node, then **MODIFY** button > **ADVANCED** button.
4. In the **RN Services** field, click **Custom** or **Default**.

When you click **Custom**, the onQ Portal overwrites the values from the custom list with the values from the default list so that the known services that are problematic always default to `Disabled`.



CPU Resource Limit: 30 % (1 - 100)

Disk Resource Limit: 170 MB/s (1 - 200)

Network Resource Limit: 170 MB/s (0.1 - 200)

Enable Cluster Support?: ● No ○ Yes

5. Do any of the following to create or modify a custom list:

> **Note:** If you delete all entries in the custom list, the onQ Portal assumes you no longer want a custom list and applies the default list.

- Select an existing service from the table and **Modify** its start option.
- Click **Extract** to retrieve a list of services and settings that recently appeared in your PN's registry. Prune and or selectively modify this list to meet your needs. This option prevents you from unintentionally misspelling a service name. If no snapshot exists for the PN, which only occurs if you added a PN and the backup is in progress, then the onQ Portal displays an error.
- In the text box, type the name of the service and specify its start option, then click the plus (**+**) button.

6. Do one of the following:

> **Note:** The onQ Portal validates the service to the extent that it checks for duplicates and blank entries.

- Click **Save** - onQ Portal saves your exclude list as shown in the list, then returns you to the previous page. The **Backup Exclude List:** button is labeled **Custom**.

- Click **Default** - onQ Portal deletes the custom list and replaces the custom list with the default list (also known as *factory default*), then returns you to the previous page. The **Backup Exclude List:** button is labeled **Default.**
- Click **Revert** - onQ Portal discards your changes, then returns you to the previous page. The **Backup Exclude List:** button does not change.

9.3 Edit backup exclude list

A backup exclude list is a list of folders and files that need not be backed up. The purpose of the list is to improve the efficiency of the backup process by minimizing the quantity of data to be processed. For each protected node there is a backup exclude list.

By default, the onQ Appliance excludes temporary files. You must take great care in selecting files and folders to exclude from backup. Excluding some key files might prevent your recovery nodes from working properly.

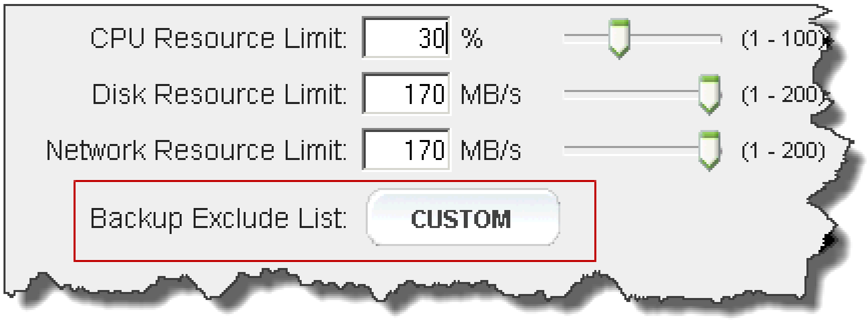
For an exclude list, onQ Portal recognizes file and folder names expressed as IEEE POSIX Basic Regular Expressions (BRE).

To add a file or folder to the exclude list:

This procedure assumes that you're modifying the exclude list for an existing protected node. However, you can perform this procedure from either the **Add Protected Node** page or the **Modify Protected Node** page. Exclude lists are specific to the protected node's operating system.

1. Log on to the HA's onQ Portal.
2. Click the **PROTECTION CONFIG** tab.
3. Select the node, then **MODIFY** > **ADVANCED**.

4. In the **Backup Exclude List** field, click **Custom** or **Default.**



CPU Resource Limit: 30 % (1 - 100)

Disk Resource Limit: 170 MB/s (1 - 200)

Network Resource Limit: 170 MB/s (1 - 200)

Backup Exclude List: CUSTOM

Note: On a DR Appliance, the Backup Exclude List is a read-only field.

5. Specify a new exclusion.
   a. In the text box, type the path to the file or folder. Your path cannot contain any of the following characters:

      < (less than)

      > (greater than)

      : (colon)

      " (double quote)

      / (forward slash)

      \ (backslash)

      | (vertical bar or pipe)

      ? (question mark)

      * (asterisk)

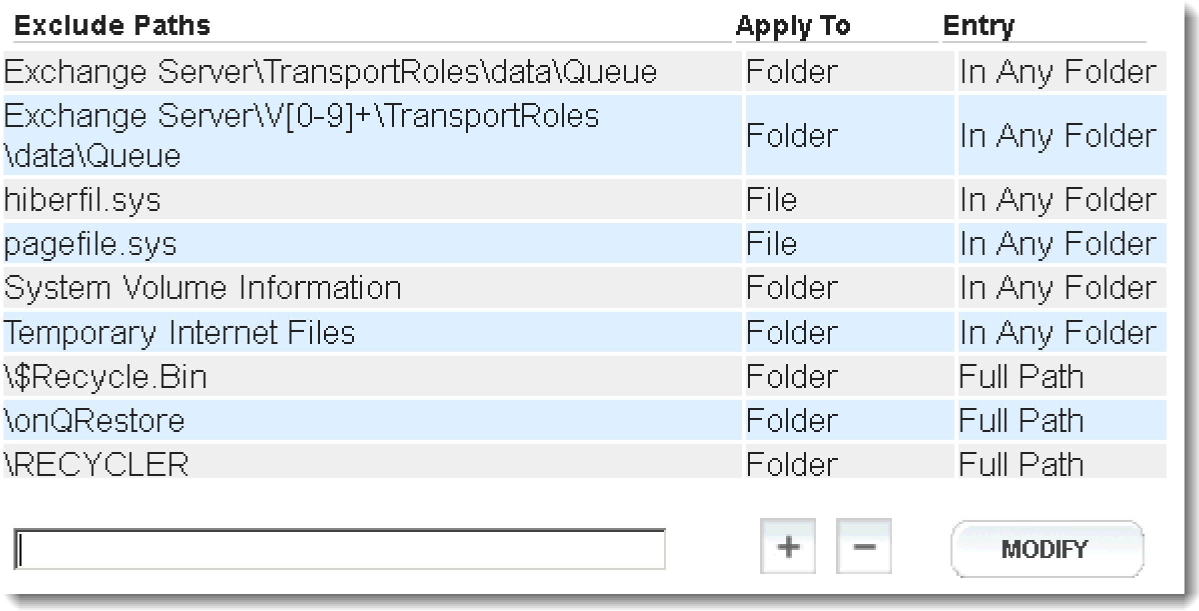
      & (ampersand)

   b. Select an **Apply To:** radio button that represents the path type. The path can be the folder or file or both.

Note: For a CIFS mount, you do not need to specify the full path of the mounted share volume. Simply type the drive letter and folder name: `P:\applications` where `applications` is the folder that you want to exclude.

c. Select an **Entry:** radio button to indicate that you'd like to exclude the file or folder wherever it is found or if you want to exclude only that specific full path.

In the following example, the contents listed will not be backed up. These exclude paths represent some of the paths that are listed in the *default* Backup Exclude List defined by Quorum.



Exclude Paths	Apply To	Entry
Exchange Server\TransportRoles\data\Queue	Folder	In Any Folder
Exchange Server\V[0-9]+\TransportRoles \data\Queue	Folder	In Any Folder
hiberfil.sys	File	In Any Folder
pagefile.sys	File	In Any Folder
System Volume Information	Folder	In Any Folder
Temporary Internet Files	Folder	In Any Folder
\$Recycle.Bin	Folder	Full Path
\onQRestore	Folder	Full Path
\RECYCLER	Folder	Full Path

6. Click the plus (**+**) button.

7. Do one of the following:
   - Click **Save** - onQ Portal saves your exclude list as shown in the list, then returns you to the previous page. The **Backup Exclude List:** button is labeled **Custom**. You cannot save the list if the total length of all paths exceeds 2,000 characters. Also, each line cannot exceed 512 characters.
   - Click **Default** - onQ Portal replaces the entire list with the default list (also known as *factory default*), then returns you to the previous page. The **Backup Exclude List:** button is labeled **Default.**
   - Click **Revert** - onQ Portal discards your changes, then returns you to the previous page. The **Backup Exclude List:** button does not change.

9.4 Edit backup include list

A backup include list (via the **File Backup Only** parameter) feature can only be enabled by Quorum Support and is typically used only for file servers.

A backup include list is a user-defined set of folders/files that need to be backed up. The purpose of the list is to improve the efficiency of the backup process by being able to specify only the necessary files without having to create a large exclude list. For each protected node one can define a list of files or folders.

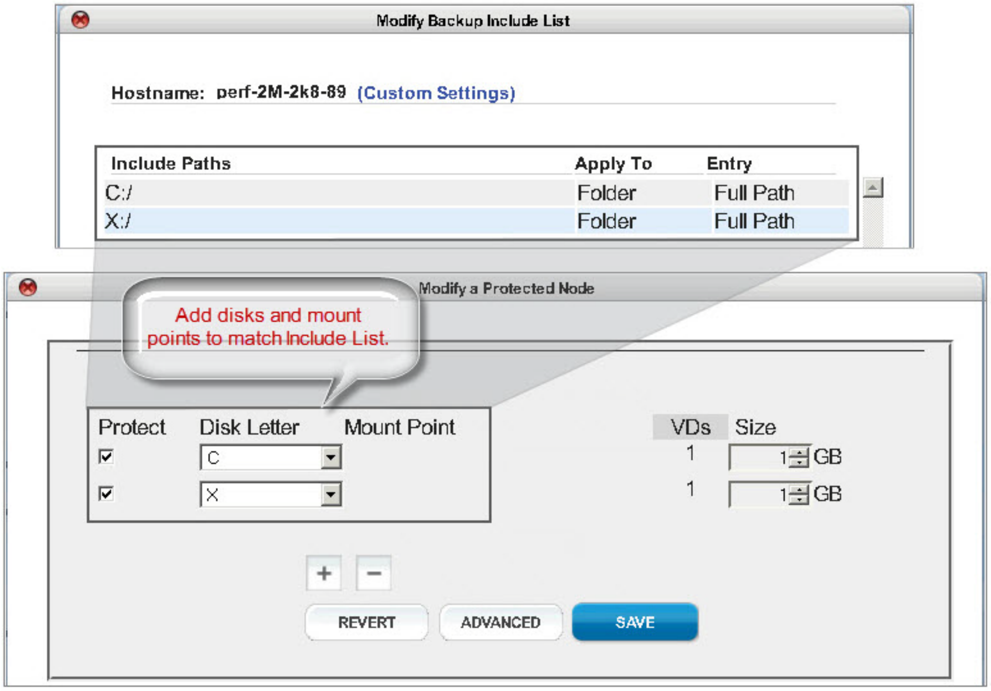
For an include list, onQ Portal recognizes file and folder names expressed as IEEE POSIX Basic Regular Expressions (BRE).

To add a file or folder to the include list:

This procedure assumes that you're modifying the include list for an existing protected node. However, you can perform this procedure from either the **Add Protected Node** page or the **Modify Protected Node** page. Include lists are specific to the protected node's operating system.

1. Log on to the HA's onQ Portal.
2. Click the **PROTECTION CONFIG** tab.
3. Select the node, then **Modify**.
4. Select **File Only Backup** > **Yes** radio button > **ADVANCED** button. If you do not see this parameter, contact Quorum Support.
5. Specify the disk drives and mount points for the files and folders that you want to specify in the include list.

6. Specify and protect the files and folder for inclusion:



Modify Backup Include List

Hostname: perf-2M-2k8-89 (Custom Settings)

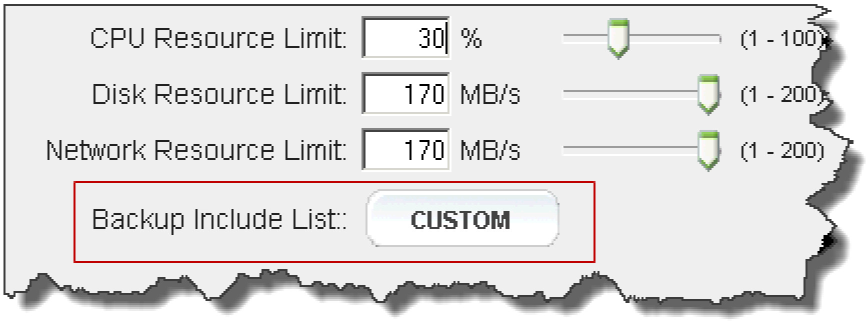
Include Paths	Apply To	Entry
C:/	Folder	Full Path
X:/	Folder	Full Path

Modify a Protected Node

Add disks and mount points to match Include List.

Protect	Disk Letter	Mount Point	VDs	Size
☑	C		1	1 GB
☑	X		1	1 GB

a. In the **Backup List** field, click **Custom.**



CPU Resource Limit: 30 % (1 - 100)

Disk Resource Limit: 170 MB/s (1 - 200)

Network Resource Limit: 170 MB/s (1 - 200)

Backup Include List:: CUSTOM

b. Enter a path/folder/file and click plus (+) to add the entry to the include list.

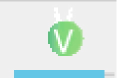
c. Do one of the following:
   - Click **Save** - onQ Portal saves your exclude list as shown in the list, then returns you to the previous page. The **Backup Include List:** button is labeled **Custom**.
   - Click **Revert** - onQ Portal discards your changes, then returns you to the previous page. The **Backup Include List:** button does not change.

9.5 Initiate immediate backups

You can trigger an immediate backup of protected node, regardless of when the next backup is scheduled. You can restore from a backup at any time.

To initiate a backup:

1. Log on to the HA’s onQ Portal.
2. Go to **DASHBOARD** tab > **PROTECTED NODES** page.
3. Unlock the page.
4. In the **Backup Status** column, click the carat icon for the protected node that you want to back up.
5. When prompted, click **Start**.
   - The carat changes to green and moves left to right until the backup completes.

   - After completion, the carat moves to its upright position and the new backup timestamp posts. In addition, the snapshot is saved to the repository, and you can retrieve it at any time.

Related Topics

Initial Backup
Schedule backups
Seed the DR Repository
Resize protected node’s vdisk

9.6 Schedule backups

onQ performs an initial backup of your PN when you first start protection on your nodes. For all subsequent backups, you can instruct onQ when and how often to perform those backups. Each protected node has its own backup schedule with backups to occur at varying times, days of the week, and frequencies. Such granular scheduling is essential for those networks with low bandwidth.

onQ has two built-in policies that affect backups:

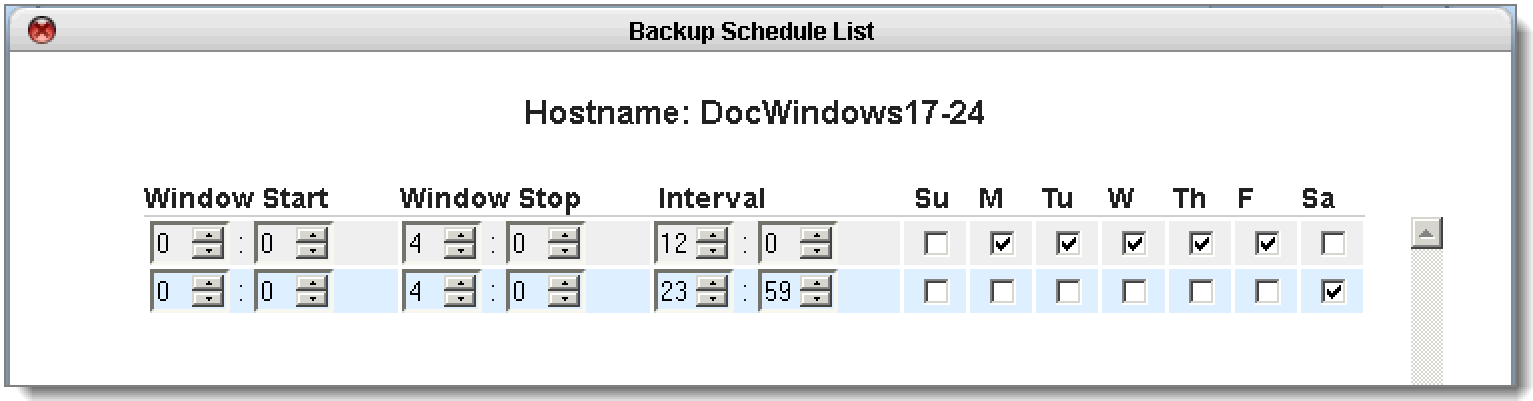
- if an HA’s repository disk space utilization exceeds 85%, onQ deletes old backups. See A0103 for more information.
- if an HA’s repository disk space utilization exceeds 85%, onQ disables schedule backups globally, logging a `Scheduled backup request skipped while backups suspended` error message and resumes scheduled backups when disk space utilization improves (less than 85%); however, during this time, you can perform immediate backups. This suspension policy attempts to prevent your HA from using 100% of its repository’s disk space. onQ does not suspend in-progress backups.

To create or change the backup schedule:

This schedule is automatically transferred to the DR Appliance. In the event of a disaster and if the DR Appliance takes on the HA role, the same backup schedule continues.

1. Log on to the HA’s onQ Portal.
2. Go to **PROTECTION CONFIG** tab, select the PN, then click the **MODIFY** button.
3. In the **Backup Schedule** field, click the **SCHEDULE** button.
4. Configure your schedule. You can create as many schedules as you want. The scheduler prevents you from creating schedule overlaps. If you want to return the default schedule, click **CLEAR**.

   For example, let’s assume you have very little network bandwidth and peak hours of operation are M-F 5am to 11pm and business activity is light on Saturdays with minimal changes and no activity on Sundays. Simply set the schedule as follows:



Backup Schedule List

Hostname: DocWindows17-24

Window Start	Window Stop	Interval	Su	M	Tu	W	Th	F	Sa
0 : 0	4 : 0	12 : 0	☐	☑	☑	☑	☑	☑	☐
0 : 0	4 : 0	23 : 59	☐	☐	☐	☐	☐	☐	☑

Window Start: Based on a 24-hr clock, select the time of day to start the backup. Choose a time when the network is the least busy. The initial backup can take a considerable amount of time. Subsequent backups record only changes that have occurred since the preceding backup and so will be relatively brief.

Window Stop: Based on a 24-hr clock, select the time of day to stop the initiation of new backups. Any backups currently running at the time of the stop period will be allowed to complete. As outlined in Stop in-progress backups, you can stop these backups.

Interval. The interval (in minutes/hours) between the start of the data backup and the next data backup. Basically, the interval represents the frequency of backups. Valid values: hour, `0-23`; minute, `0-59`. As with any backup solution, this interval represents your potential data loss in the event of a failure (aka RPO).The shortest interval is 15 minutes, which is impractical for an onQ that's protecting a large number of PNs, possibly resulting in queued backups as outlined in "Stop in-progress backups" on page 279. If you are not sure what interval to specify, a 4-hr interval is common in enterprises with high network bandwidth and 24-hr interval in low network bandwidth.

Days: Select the check box for the day(s) of the week for which you'd like this policy to apply. If you don't have business activity (for example, Sunday) on a given day, clear that check box.

That's it!

5. (Optional) Monitor these backups. Go to "Monitor protected nodes" on page 440 and "Monitor backups" on page 452. If you receive any email alerts, follow the instructions in Backup Alerts.

9.7 Change Backup Retention Policy

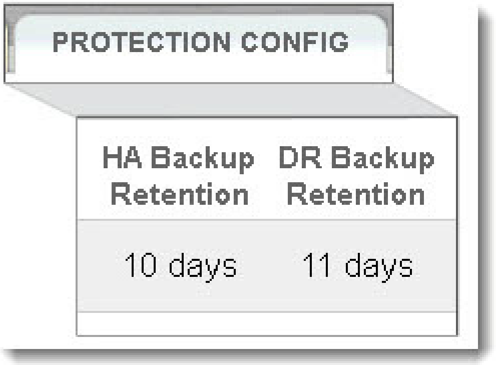
You must tell onQ how long to retain backups for a given PN. Each PN has a unique backup retention period for both the HA and the DR Appliance.

In the event that onQ needs to free up disk space, it will expire backups that agree with your retention policy. In the event that onQ is low on disk space, you will receive one or more alerts outlined in onQ Disk Space Alerts. If onQ is unable to expire backups because doing so conflicts with your retention policy, you might need to reduce the number of days that you specified in the node's retention policy.

To change the backup retention period:

1. Log on to the onQ Appliance's onQ Portal.
2. Click the **PROTECTION CONFIG** tab.

   The PROTECTION CONFIG tab on a DR Appliance is slightly different from its HA counterpart. The DR's tab shows the HA's backup retention time as well as its own backup retention time:



HA Backup Retention	DR Backup Retention
10 days	11 days

3. Select the node that you want to modify, then click **MODIFY**.

   The Modify a Protected Node page appears.
4. In the **Backup Retention Time** field, specify (in *days)* how long you want onQ to retain backups, then **SAVE**.

Related Topics

Delete snapshots
Schedule backups

9.8 Delete snapshots

You cannot delete snapshots for an existing PN. However, if you deleted a PN, because you either removed the PN from production or you moved the PN to another HA, you might want to delete all the orphan data associated with that PN. Such orphan data includes:

- PN snapshots
- RN
- RN snapshots
- Self test schedules

However, in the latter case, don't delete the orphan data without first confirming that backups for the PN are working on the new HA. Moreover, to keep the onQ Appliances in sync, Quorum recommends that you perform this procedure on the HA's DR Appliances and DR Mirrors.

If you remove orphan data for a PN from the HA—but not from the DR, then later re-enroll that same PN on the same HA, the DR fails to add the future snapshots for this PN thereby compromising disaster recovery.

To delete orphan data:

1. Log on to the HA's onQ Portal.
2. Go to **PROTECTION CONFIG** tab > **FIND ORPHANS** button.

   The onQ Portal searches the Repository for orphan data. If onQ Portal doesn't find any orphan data, the onQ Portal returns a `No data found that does not belong to a configured PN` message. Otherwise, the onQ Portal prompts you to purge the orphan data that the onQ Portal did find.

3. Select the check box for the PN whose orphan snapshots you want to delete, then click **YES**.

Warning: You cannot abort a purge after it begins.

A progress dialog appears, highlighting the number of files waiting to be deleted. This process can take several minutes per snapshot.

4. After the purge completes, repeat Step 2 to verify that the onQ Portal removed all orphan snapshots.

Warning: If you delete orphan data for a given PN, Quorum recommends that you do so for both the HA and the DR. If you remove orphan data for a given PN from the HA—but not from the DR, then later re-enroll that same PN on the same HA, the DR fails to add the future snapshots for this PN thereby compromising disaster recovery.

5. (Recommended) Repeat this process on each DR Appliance and DR Mirror so that all onQ Appliances are in sync.

9.9 Stop in-progress backups

Whether you use agent-less or agent-based enrollment, onQ can perform three concurrent PN backups; with agent-less enrollment, these concurrent backups can be running on different ESX/ESXi hosts.

Even when you schedule backups during non-working hours, backups can occur during unscheduled times (working hours) due to queued snapshots. Queued snapshots can occur if onQ is overly busy backing up other PNs or if the PNs have short backup intervals.

If an unwanted backup is in progress during unscheduled times, you might want to stop that backup from continuing if it is affecting performance.

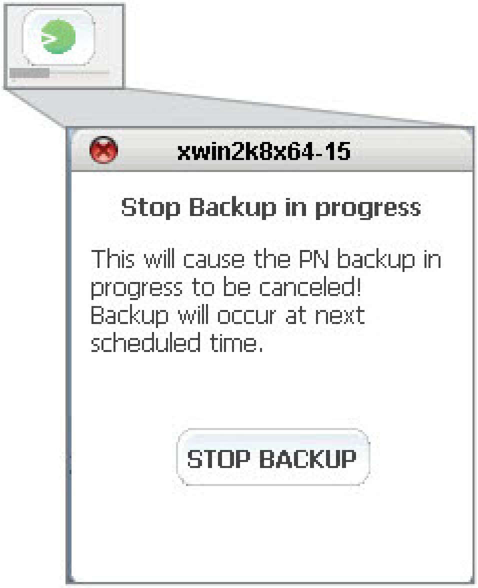
onQ has two built-in policies that affect backups:

- if an HA's repository disk space utilization exceeds 85%, onQ deletes old backups. See A0103 for more information.
- if an HA's repository disk space utilization exceeds 85%, onQ disables schedule backups globally, logging a `Scheduled backup request skipped while backups suspended` error message and resumes scheduled backups when disk space utilization improves (less than 85%); however, during this time, you can perform immediate backups. This suspension policy attempts to prevent your HA from using 100% of its repository's disk space. onQ does not suspend in-progress backups.

To stop a backup:

1. Log on to the HA's onQ Portal.
2. Go to **DASHBOARD** tab > **PROTECTED NODES** page.
3. Unlock the page.
4. Locate the PN with a backup in progress as indicated by the **Backup Status** column (see Monitor backups).
5. Click on the Backup Status button. The **Backup Status in progress** dialog appears.

6. Click **STOP BACKUP**.



xwin2k8x64-15

Stop Backup in progress

This will cause the PN backup in progress to be canceled! Backup will occur at next scheduled time.

The backup will automatically run at the next scheduled interval as displayed in the **Next Scheduled Backup** column.

7. (Optional) Consider increasing your backup interval to prevent queuing of backups.

9.10 Restore files and folders

To retrieve (or browse) files/folders from the Repository, you have two choices:

- Indirectly, using FLR. Copy the files to another Windows server, then browse.
- Directly, using WSR. Simply browse *any object* in the Repository directly or map to a shared location on a Windows server or client.

> **Note:** With WSR, you can use a 3rd party exchange recovery tool and open the exchange database directly from the Repository. In doing so you can retrieve any object, even a single email message within couple minutes and from any prior snapshot.

Restore PNs Using QUARK

9.10.1 Perform WSR Restore

A Windows Share Restore (WSR) restore involves mapping from a drive on a Windows server/client to a shared location generated by the onQ. This shared location will contain all the snapshots for a given PN.

For security purposes, you can only mount the share from one location; besides, one share is recommended because browsing the repository can be resource intensive.

After you create the share, you can browse any of the snapshots (backups) listed for viewing, reading, and copying any folders/files as needed. However, a few things to note:

- You cannot modify or delete folders/files within a snapshot.
- You cannot delete folders/files from the repository.
- You cannot copy new folders/files into the repository.

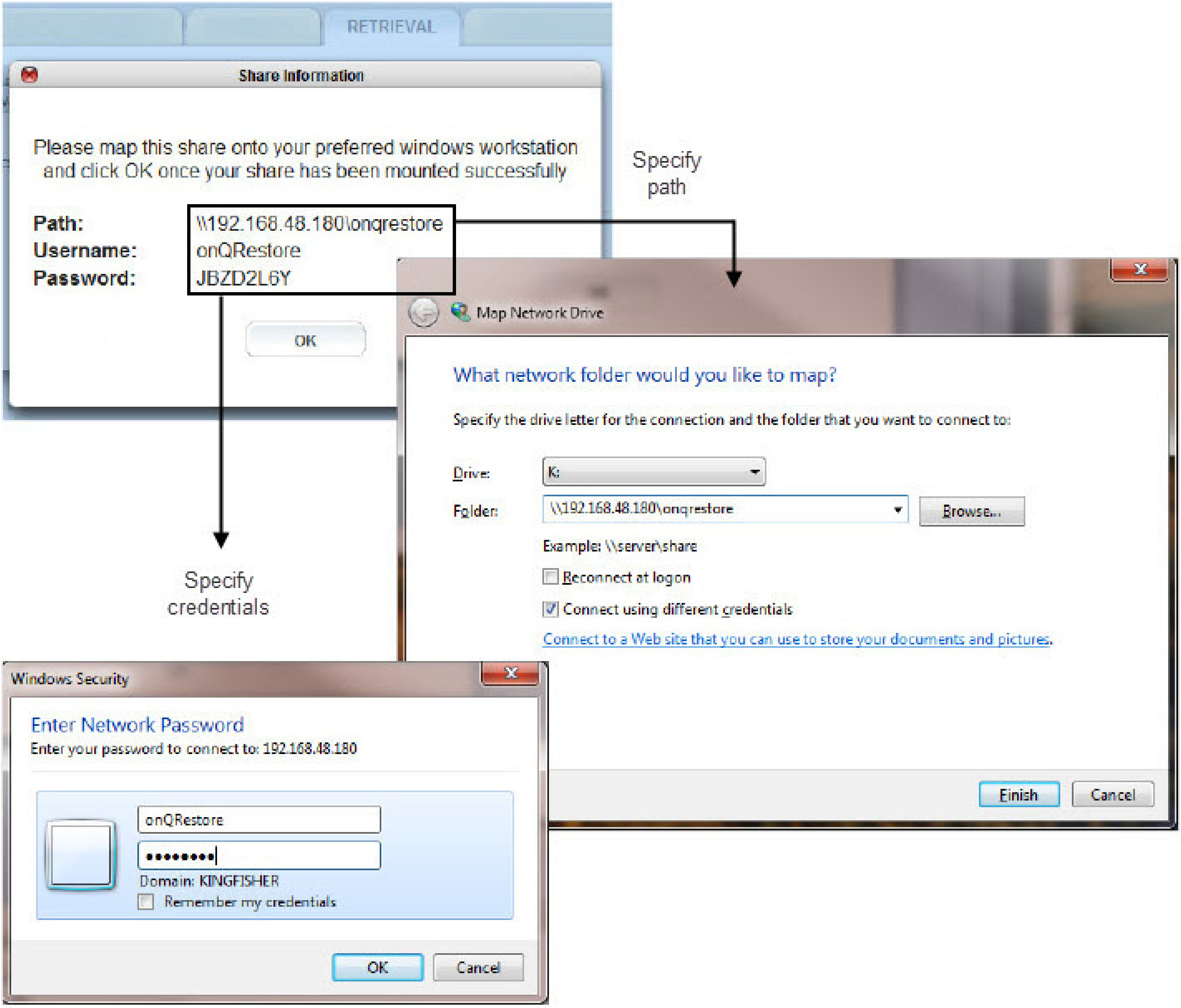
To restore Exchange Server data and mailboxes, consider using Kroll's Ontrack PowerControls.

To retrieve a snapshot, using WSR:

1. Log on to the Appliance's onQ Portal.
2. Click on the **RESTORE** tab > **WINDOWS SHARE** page. onQ displays an empty page if no share was activated.
3. Create a share, then map to this share:
   a. Click on the **ACTIVATE SHARE** button.
   b. From the Active Windows Share Session popup and in the drop-down box, select the desired protected node from which you want to restore, then **START**.

      When a protected node appears in the list, that PN has data in the Repository, including any unprotected nodes that were previously protected.
   c. Using the share path, username, and password that appears in the Share Information popup, map your Windows server/client to this share, then **OK**.

The share expires after 30 minutes of no activity. Also, if the share is not mapped on to a Windows server/client before you exit the popup, both `Client` and `Connection Start Time` values are blank.



Share Information

Please map this share onto your preferred windows workstation and click OK once your share has been mounted successfully

Path: \\192.168.48.180\onqrestore
Username: onQRestore
Password: JBZD2L6Y

Specify path

Specify credentials

Map Network Drive

What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: K:
Folder: \\192.168.48.180\onqrestore

Example: \\server\share

□ Reconnect at logon

☑ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.

Windows Security

Enter Network Password

Enter your password to connect to: 192.168.48.180

onQRestore
••••••••

Domain: KINGFISHER

□ Remember my credentials

4. Launch Windows Explorer to display the snapshots available for the PN.

5. From here, copy the data to any restore location.

To delete a share:

You might want to delete share if you:

- You completed your restore or no longer need to retrieve objects from a snapshot.
- You forget to record the credentials for the share location. For security purposes, you cannot retrieve this information, and so you must delete and recreate the share.

1. Log on to the Appliance's onQ Portal.
2. Click on the **RESTORE** tab > **WINDOWS SHARE** page.
3. Select the share from the list, then **STOP SHARE**.
4. In the Stop Windows Share Session popup, click **YES**.

9.10.2 Perform File-level Restore

onQ provides a way for you to retrieve any combination of files and folders or entire drives from existing snapshots of any protected node. This process is known as a file-level restore (FLR).

If, however, your protected node's server failed, you need to perform a bare metal restore (BMR) as outlined in "Restore PNs Using QUARK" on page 398.

You can choose to *replace* the current file, folder, or drive, or to *store* it on any protected node or standalone server so long as it is reachable from your network.

> **Note:** FLR is supported for both Windows and Linux-based protected nodes, though the example below demonstrates a recovery using a Windows-based protected node.

To retrieve a snapshot, using FLR:

Before you begin:

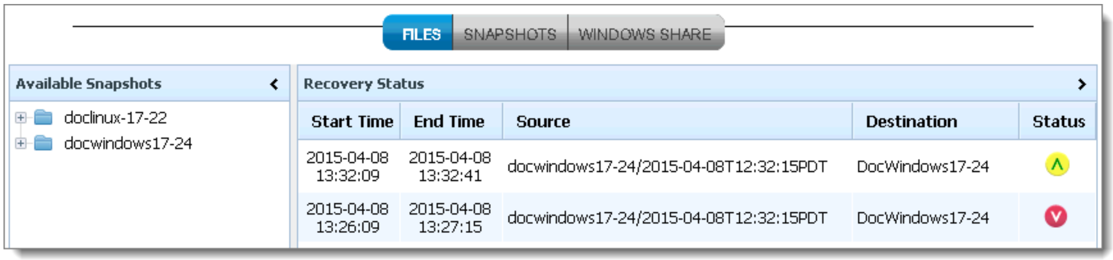
Review the limitations outlined in "File-level Restore Limitations" in onQ

Release Notes.

Ensure that you have the `nc` utility installed as outlined in (Agent-based Linux PNs) Enroll protected nodes.

1. Log on to the Appliance’s onQ Portal.
2. Click on the **RESTORE** tab > **FILES** page.

   A page similar to the following appears:



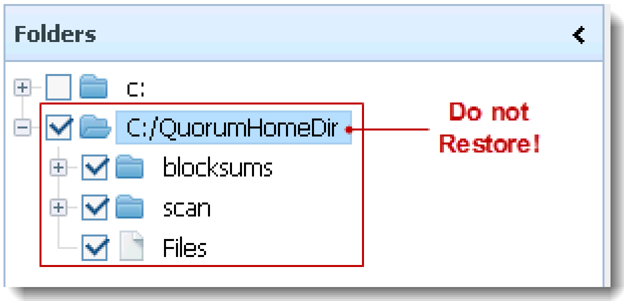
Available Snapshots

- doclinux-17-22
- docwindows17-24

Recovery Status

Start Time	End Time	Source	Destination	Status
2015-04-08 13:32:09	2015-04-08 13:32:41	docwindows17-24/2015-04-08T12:32:15PDT	DocWindows17-24	^
2015-04-08 13:26:09	2015-04-08 13:27:15	docwindows17-24/2015-04-08T12:32:15PDT	DocWindows17-24	V

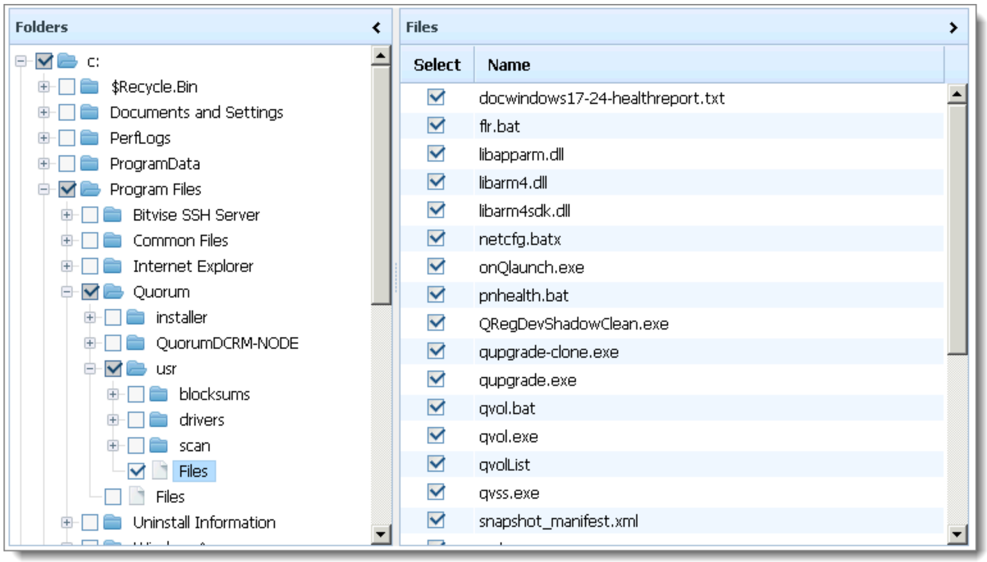
In the case of Agent-less PNs, do not restore `C:\QuorumHomeDir\` or `/data/QuorumHomeDir` as these volumes are for implementation purposes only and do not reside on the PN itself:



Do not Restore!

3. In the **Available Snapshots** pane, expand the folder for the protected node.
4. Double-click on the snapshot that contains the data you want to restore.

A page, labeled **Step 1**, appears:



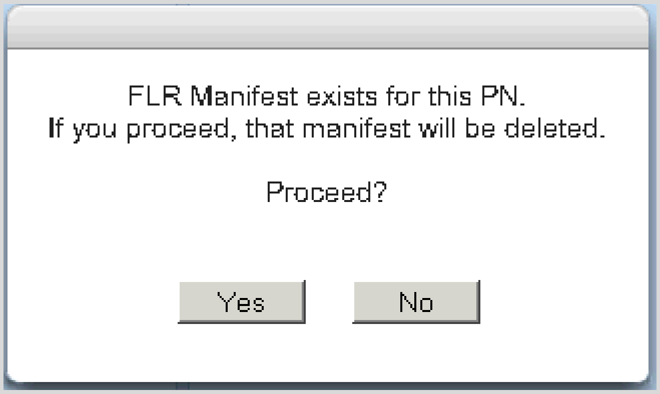
- ☑ c:
  - □ $Recycle.Bin
  - □ Documents and Settings
  - □ PerfLogs
  - □ ProgramData
  - ☑ Program Files
    - □ Bitvise SSH Server
    - □ Common Files
    - □ Internet Explorer
    - ☑ Quorum
      - □ installer
      - □ QuorumDCRM-NODE
      - ☑ usr
        - □ blocksums
        - □ drivers
        - □ scan
        - ☑ Files
      - □ Files
    - □ Uninstall Information

Select	Name
☑	docwindows17-24-healthreport.txt
☑	flr.bat
☑	libapparm.dll
☑	libarm4.dll
☑	libarm4sdk.dll
☑	netcfg.batx
☑	onQlaunch.exe
☑	pnhealth.bat
☑	QRegDevShadowClean.exe
☑	qupgrade-clone.exe
☑	qupgrade.exe
☑	qvol.bat
☑	qvol.exe
☑	qvolList
☑	qvss.exe
☑	snapshot_manifest.xml

5. Specify the files you want to retrieve. Expand the hierarchy on the left, select the desired folder or files, then click **NEXT**:
   - For each folder, select the check box to select all of its contents.
   - Click ***Files*** to display the individual files in the content pane to the right. Then, in the content pane, you can select the individual files that you want.

onQ begins to build the manifest file. If this process completes within minutes, proceed to Step 7.

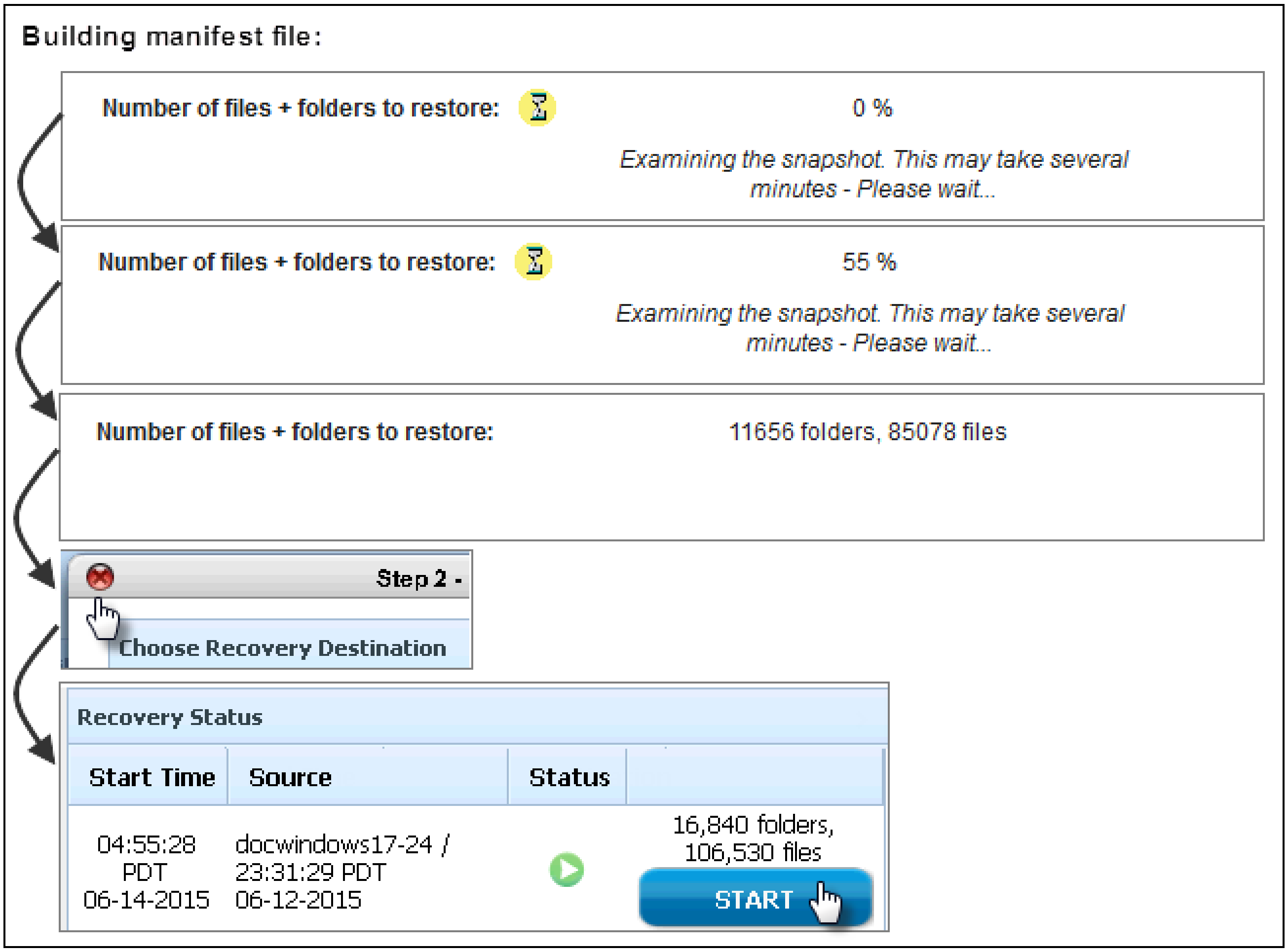
Note: Depending on the number of files, onQ may require a few hours to build the manifest file; in this case, allow onQ to build the manifest file. Return to the onQ Portal at a later time to initiate the restore from the prebuilt manifest: **RESTORE** tab > **Recovery Status** pane > **START** button. If, after the manifest builds, you attempt to perform the restore again by selecting the files again, onQ Portal prompts you to choose the existing manifest (**No**) or to build a new one (**Yes**).



FLR Manifest exists for this PN.
If you proceed, that manifest will be deleted.

Proceed?

6. Initiate the restore: **RESTORE** tab > **Recovery Status** pane > **START** button.



Building manifest file:

Number of files + folders to restore: 0 %

Examining the snapshot. This may take several minutes - Please wait...

Number of files + folders to restore: 55 %

Examining the snapshot. This may take several minutes - Please wait...

Number of files + folders to restore: 11656 folders, 85078 files

Recovery Status

Start Time	Source	Status	
04:55:28 PDT 06-14-2015	docwindows17-24 / 23:31:29 PDT 06-12-2015	▶	16,840 folders, 106,530 files START

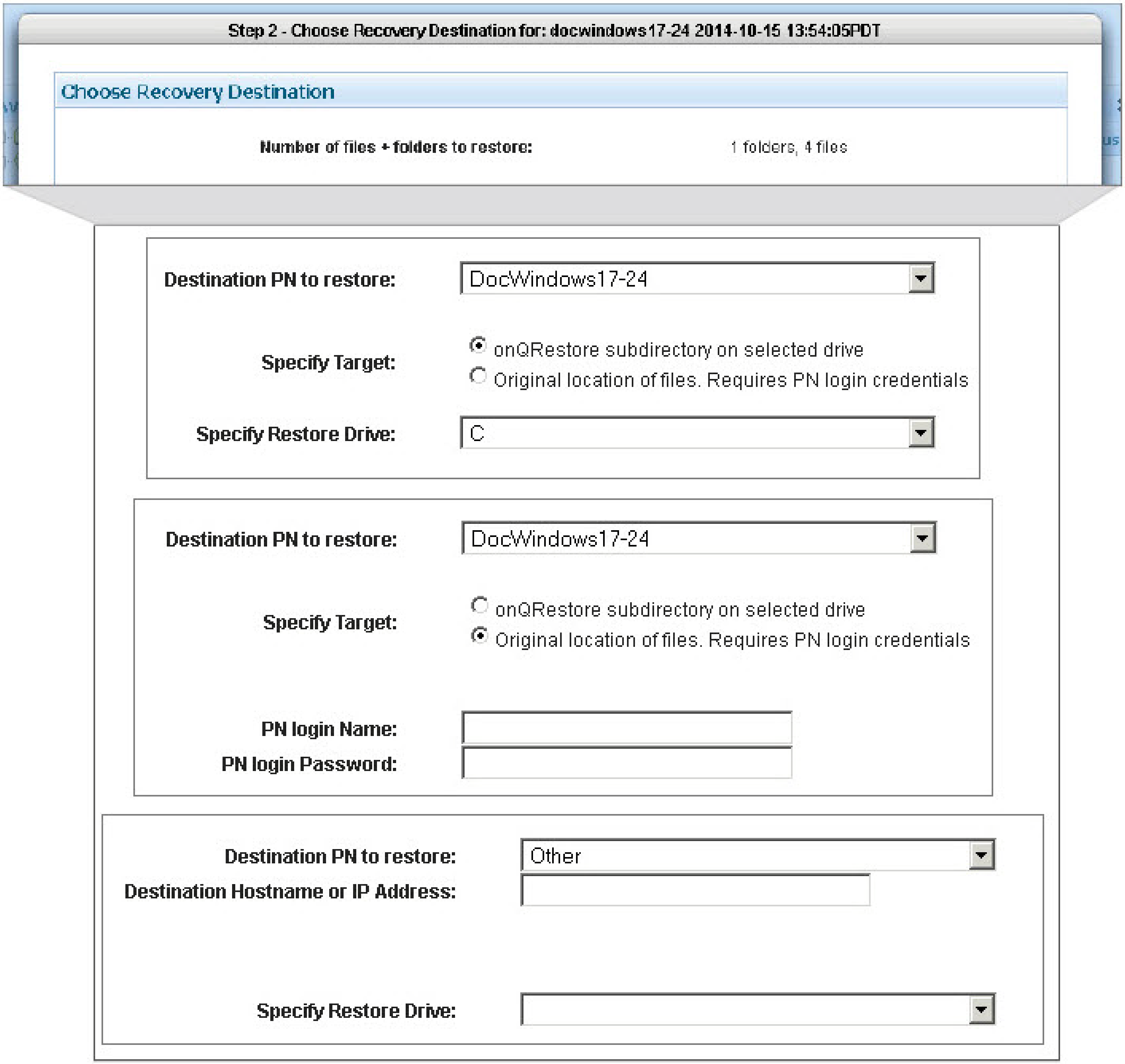
7. Before you proceed with the restore, decide on the host to which you want to restore the files.
   - **Do you want to restore to a *Protected Node***? You can restore to the same or different Protected Node.
   - **Do you want to restore to a *Standalone Server***? Do so if you'd like to inspect the files before you restore a Protected Node with them.

8. Do the following:

   a. In the **Destination PN to restore** drop-down, specify the recovery destinations host where you want to store the retrieved files. The destination can be one of the following:

<***Host***>. This destination is a PN, either the same PN or a different PN. Choose this option if you chose “Protected Node” in Step 7. To ensure that you restore your files correctly, only Pens that share the same operating system as the host that owns the snapshot that you want to restore appear in the list. If applicable, in the **Specify Restore Drive** drop-down, choose a drive to which you want to save the files

Other. This destination is a host that is not a PN. Choose this option if you chose “Standalone Server” in Step 7. If you have an agent-less PN, this is the only supported option for FLR. When you select **Other**, a text box appears labeled **Destination hostname or IP address**. Type the address of your desired destination server. In the **Specify Restore Drive** drop-down, choose a drive to which you want to save the files. Skip to Step c.



Step 2 - Choose Recovery Destination for: docwindows17-24 2014-10-15 13:54:05PDT

Choose Recovery Destination

Number of files + folders to restore: 1 folders, 4 files

Destination PN to restore: DocWindows17-24

Specify Target:
● onQRestore subdirectory on selected drive
○ Original location of files. Requires PN login credentials

Specify Restore Drive: C

Destination PN to restore: DocWindows17-24

Specify Target:
○ onQRestore subdirectory on selected drive
● Original location of files. Requires PN login credentials

PN login Name:

PN login Password:

Destination PN to restore: Other

Destination Hostname or IP Address:

Specify Restore Drive:

b. If applicable, in the **Specify Target** field, choose a target. A target can be one of the following: (1)

- **onQ Restore subdirectory on selected drive**. The files will automatically be saved to a default restore location on the drive that you select and that distinguishes the FLR from multiple different snapshots and maintains the relation of the files to a given snapshot:

(Windows) – *driveLetter*:\onQRestore\pnName AND snapShot timeStamp.

(Linux) – *mountPoint*/onQRestore/*pnName/snapShot timeStamp*. /onQRestore... if you chose /or /boot/onQRestore... if you chose /boot.

- **Original location of files**. Choose this option if you want to overwrite the existing files. There are limitations to this option (see "File-level Restore Limitations" in onQ Release Notes). Skip to Step 9.

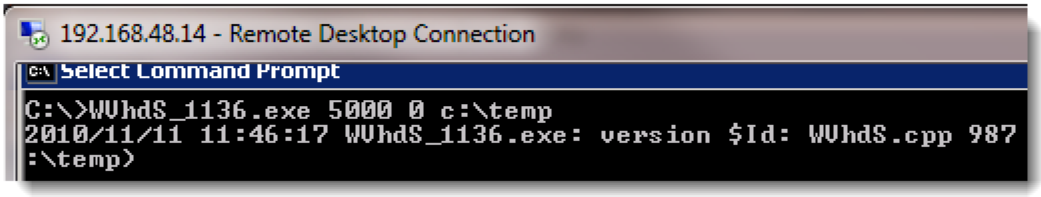
c. If you want to restore to a Standalone Server, which, unlike a restore to a PN, does not already have the onQ Service installed, do one of the following to open up a communication "channel" between the onQ Appliance and the Standalone Server:

- **(Windows/Automatic Process)** Type the PN's credentials, then wait for WVhds_*<build>*.exe to automatically validate those credentials. These credentials are not stored on the onQ in any database or log file.
- **(Windows/Manual Process)** Download and execute WVhdS_*<build>*.exe on the remote host as the example below shows. Retrieve this file from **APPLIANCE CONFIG** tab > **ADVANCED** button > **DOWNLOADS** subtab. From a DOS prompt, run the following command:

```
# wvhdS_version.exe 5000 0 restore-location
```

For example:

(where c:\temp in the following example is the restore location)



```
C:\>WVhdS_1136.exe 5000 0 c:\temp
2010/11/11 11:46:17 WVhdS_1136.exe: version $Id: WVhdS.cpp 987
:\temp>
```

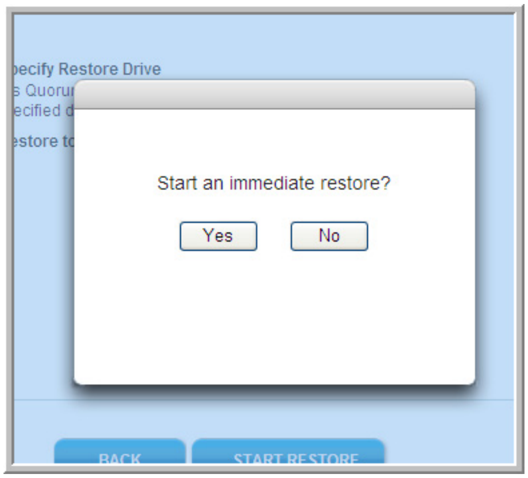
- **(Linux/Manual Process)** Download and execute onQFLRSelf.sh, which automatically untars a file to the recipient that you define, on the remote host. Retrieve this file from

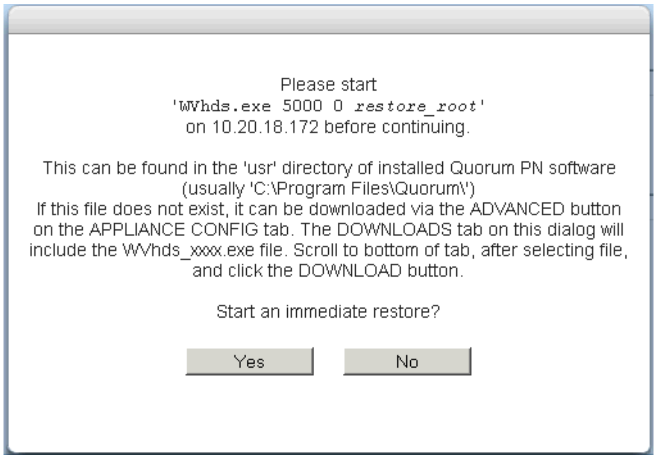
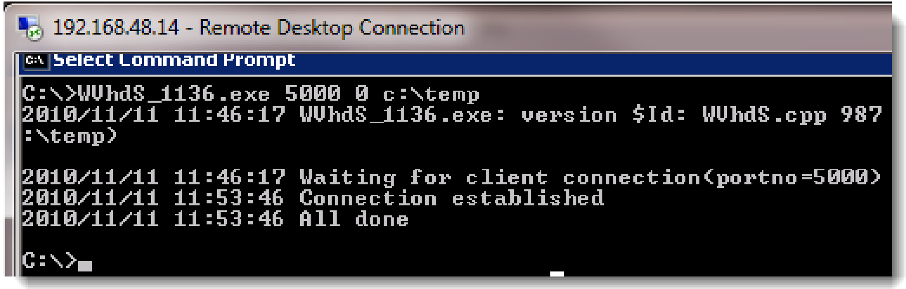
APPLIANCE CONFIG tab > **ADVANCED** button > **DOWNLOADS** subtab.

```
# cd <restore-location>
# wget http://<OnQ-IP-address>/onQFLRSelf.sh
# sh onQFLRSelf.sh
```

9. Begin the restoration. Click **START RESTORE**, then click **Yes** to confirm:

Note: Protection must be ON in order for the **START RESTORE** button to appear.

If you chose to restore to a PN:	 Start an immediate restore? pecify Restore Drive s Quoru ecified d estore to Yes No BACK START RESTORE

If you chose to restore to a Standalone Server:	 Please start 'WVhds.exe 5000 0 *restore_root*' on 10.20.18.172 before continuing. This can be found in the 'usr' directory of installed Quorum PN software (usually 'C:\Program Files\Quorum\') If this file does not exist, it can be downloaded via the ADVANCED button on the APPLIANCE CONFIG tab. The DOWNLOADS tab on this dialog will include the WVhds_xxxx.exe file. Scroll to bottom of tab, after selecting file, and click the DOWNLOAD button. Start an immediate restore? Yes No
	If restore completes, output indicates `All` **done**:  192.168.48.14 - Remote Desktop Connection Select Command Prompt C:\>WVhdS_1136.exe 5000 0 c:\temp 2010/11/11 11:46:17 WVhdS_1136.exe: version $Id: WVhdS.cpp 987 :\temp) 2010/11/11 11:46:17 Waiting for client connection(portno=5000) 2010/11/11 11:53:46 Connection established 2010/11/11 11:53:46 All done C:\>

Afterward, the onQ Portal returns you to the main **RESTORE** page.

10. Verify that your restore completed successfully:

a. Observe Snapshot status (**RESTORE** tab > **FILES** page > **Recovery Status** pane > **Status** column):

- The left pane (**Available Snapshots**) shows available snapshots, as folders, listed in a hierarchical structure by node, date, and time.
- The right pane (**Recovery Status**) shows your previous efforts at retrieving files from snapshots. The carat to the right symbolizes the result of each restore attempt.
- A **RESTART** button appears for any status other than `Completed OK`. Click the **RESTART** button to restart the FLR.

The restart process does not recreate the manifest file.

Status	**Completed OK** ∧ carat is green and points upward	Restore finished successfully. If you roll your cursor over the icon, hover-over help displays the message.
	Incomplete(NetworkErr) ∨ carat is red and points downward	Restore failed. The Status icon’s hover-over help displays the reason for the failure. This error can occur if the Netcat (`nc`) utility is not installed on the target Linux node as outlined in (Agent-based Linux PNs) Enroll protected nodes. Also, if this utility is missing, your `var/log/messages` indicate: `/opt/quorum/bin/./FLR.sh: line 44: /usr/bin/nc: No such file or directory`.
	Incomplete Client: Unable to connect to FLR server ∨ carat is red and points downward	Restore failed. The Status icon’s hover-over help displays the reason for the failure.
	Incomplete ∨ carat is red and points downward	Restore failed. The Status icon’s hover-over help displays the reason for the failure; this message is common when you type the incorrect credentials for the PN.
	Incomplete(ReplyError) ∨ carat is red and points downward	Restore failed. The Status icon’s hover-over help displays the reason for the failure.
	Completed with errors ∧ carat is yellow and points upward	The restore process didn't report that the FLR completed and didn't result in an abort. An error that cannot be attributed to the other errors in this table are categorized as `Completed with errors`. Whether FLR or QUARK-based, a restore involves a pair of processes: `R2V` and `WVHSDS`. To view the specific errors, browse the target’s quorum `wvhds.log` and the onQ Appliance’s `/var/log/r2v.log`.

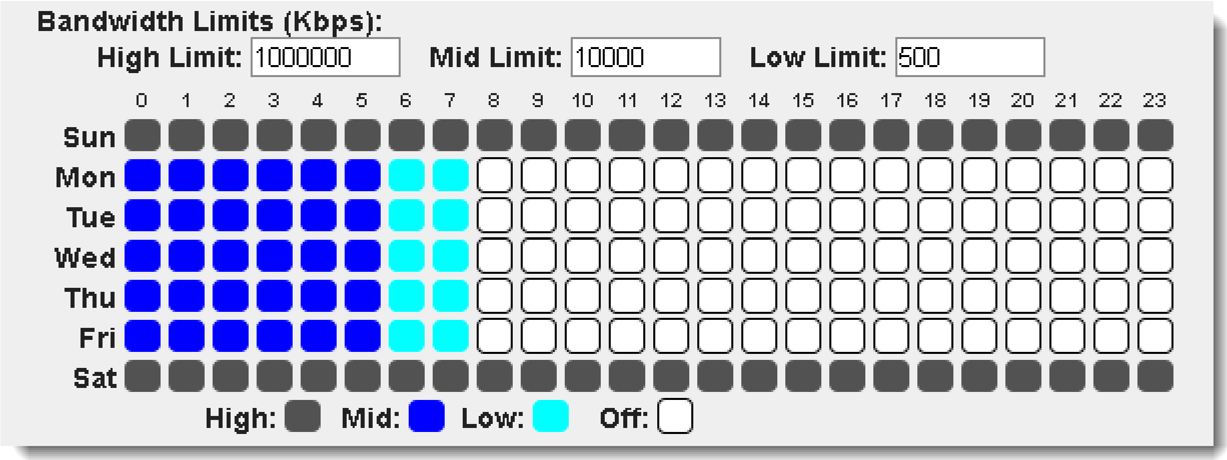
Incomplete: Unexpected Disconnect ^	Restore was interrupted, probably due to a timeout.

b. (Standalone Server) Verify that the restored files appear in the expected destination.

9.11 Adjust bandwidth throttling

Bandwidth throttling on the WAN connection between the HA and the DR Appliance is set by default to the maximum bandwidth available. If you have a DR Mirror, you can also adjust bandwidth throttling between the DR Appliance and the DR Mirror.

Bandwidth throttling can prevent a single transfer operation from swamping the network, node crashes, or other processing bottlenecks. You might need to adjust bandwidth throttling downward if the replication process places too much of a burden on your network.



Bandwidth Limits (Kbps):

High Limit: 1000000 **Mid Limit:** 10000 **Low Limit:** 500

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
Mon	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Tue	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Wed	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Thu	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Fri	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Sat	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛

High: ⬛ **Mid:** 🟦 **Low:** ▨ **Off:** □

To adjust bandwidth throttling between HA and DR Appliance:

1. Log on to the HA's onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **onQ (REMOTE)** page, then **MODIFY**.
3. Change the value (Kbps) in the **High Limit**, **Mid Limit**, and **Low Limit** fields.
4. Use the grid by clicking on the boxes to cycle through the bandwidth settings to select the limit for each day and hour, then **SAVE**.

To adjust bandwidth throttling between DR Appliance and DR Mirror:

1. Log on to the DR Appliance's onQ Portal.

2. Go to **APPLIANCE CONFIG** tab > **onQ (REMOTE)** page, then **MODIFY**.
3. Change the value (Kbps) in the **High Limit**, **Mid Limit**, and **Low Limit** fields.
4. Use the grid by clicking on the boxes to cycle through the bandwidth settings to select the limit for each day and hour, then **SAVE**.

Related Topics

Limit resource utilization on PNs

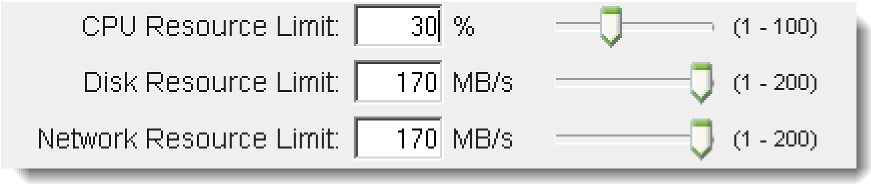
9.12 Limit resource utilization on PNs

When onQ Manager performs certain tasks, such as backing up protected nodes, it uses resources on those hosts. onQ Manager is always aware of the resource utilization on your hosts.

Your HA is pre-configured to use normal resource utilization by default, but you can further limit the CPU, disk, and network resources that onQ Manager uses. These controls can provide you assurance that your end users receive the highest priority during peak application usage.

To set resource limitations:

1. Log on to the HA's onQ Portal.
2. Stop protection.
3. From the **PROTECTION CONFIG** tab, select the protected node from the table, then **MODIFY** > **ADVANCED**.
4. Specify the resource limits using either the slider or the text boxes provided. Go more information on these limits, go to Protected Node Parameters.



CPU Resource Limit: 30 % (1 - 100)

Disk Resource Limit: 170 MB/s (1 - 200)

Network Resource Limit: 170 MB/s (1 - 200)

Related Topics

Adjust bandwidth throttling

9.13 Run custom backup scripts

onQ supports to ability to run custom backup scripts. You can use custom backup scripts to automate any number of tasks, including the ability to quiesce an application or database for backup.

(Agent-based PNs) To quiesce an application or database for backup**:**

To quiesce an application or database for backup without manual intervention, simply use `pre-snap` and `post-snap` scripts:

- For Windows PNs, you can define batch file scripts that run automatically before and after the HA creates a VSS snapshot.
- For Linux PNs, you can define shell scripts that run automatically before and after the HA creates a backup. If, for example, your pre-snap script shuts down your database so as to back up the database, the database remains down until the post-snap script executes the startup process.

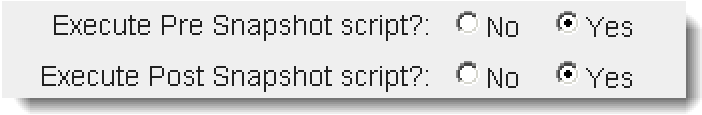
You can do so on a per-protected-node basis by saving your scripts to the PN, then registering them with the HA.

If you want to run these same scripts on all protected nodes, you must repeat the procedure below for each protected node.

1. Create two scripts with the following names, specifying the commands that you want executed.
   - **`pre_snap.bat`** and **`post_snap.bat`**. For Windows, click here to download `.bat` placeholder files to quiesce a DB2 database. In this example, each of the batch files in turn executes `.clp` scripts. These `.clp` scripts quiesce the DB2 database before the snapshot starts and again after the snapshot completes. After you create/install these scripts, they are not overwritten during a PN upgrade.
   - **`pre_snap.sh`** and **`post_snap.sh`**: For Linux, these placeholder files were saved to the destination you chose during the installation. The default location is `/opt/quorum/bin`. These scripts are not overwritten during a PN upgrade.

2. **Log on to the PN and save these scripts to:**
    - (Windows) `\Program Files\Quorum\usr` folder.
    - (Linux) the destination you chose during the installation. Usually, `/opt/quorum/bin/` is the preferred directory.
3. [Log on](#) to the HA’s onQ Portal.
4. [Stop protection](#).
5. From the **PROTECTION CONFIG** tab, select the protected node from the table, then **MODIFY** > **ADVANCED**.
6. Enable the pre and post snapshot scripts on that node:
    - Select the **Execute Pre Snapshot script?: Yes** radio button.
    - Select the **Execute Post Snapshot script?: Yes** radio button.

    The pre-snapshot script is `pre_snap`, and the post snapshot script is `post_snap`.



Execute Pre Snapshot script?: ○ No ● Yes

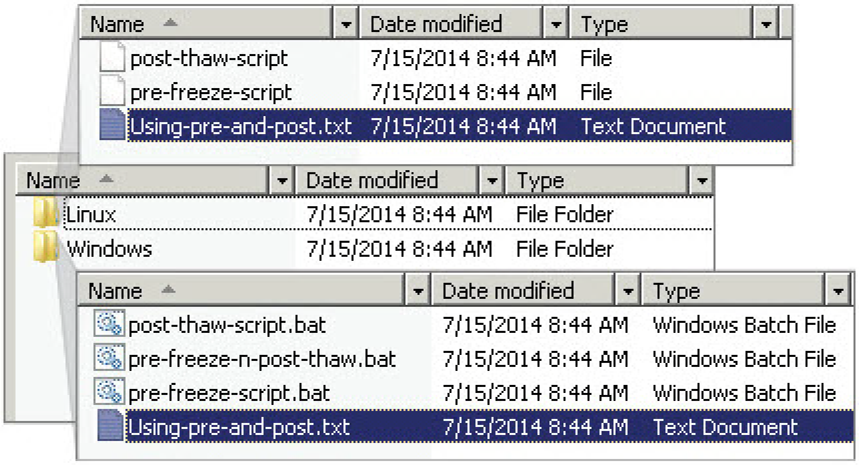
Execute Post Snapshot script?: ○ No ● Yes

7. Initiate a backup of the PN from the onQ Portal and verify the results.

(Agent-less PNs) To quiesce an application or database for backup**:**

To quiesce an application or database for backup without manual intervention, simply use `pre-freeze` and `post-thaw` scripts:

1. Download and unzip the example scripts. There are two folders, one for Windows and another for Linux. Each folder contains sample scripts.



Name	Date modified	Type
post-thaw-script	7/15/2014 8:44 AM	File
pre-freeze-script	7/15/2014 8:44 AM	File
Using-pre-and-post.txt	7/15/2014 8:44 AM	Text Document

Name	Date modified	Type
Linux	7/15/2014 8:44 AM	File Folder
Windows	7/15/2014 8:44 AM	File Folder

Name	Date modified	Type
post-thaw-script.bat	7/15/2014 8:44 AM	Windows Batch File
pre-freeze-n-post-thaw.bat	7/15/2014 8:44 AM	Windows Batch File
pre-freeze-script.bat	7/15/2014 8:44 AM	Windows Batch File
Using-pre-and-post.txt	7/15/2014 8:44 AM	Text Document

2. Create `pre-freeze-script.bat` and `post-thaw-script.bat` files, specify the commands that you want executed.
3. Do one of the following, depending on the PN's operating system:
   - (Windows) Save the `pre-freeze-script.bat` and the `post-thaw-script.bat` files under one of the following locations:
     - `C:\Program Files\VMware\VMwaretools\backupscript.d\` folder. When using this path, both the pre and the post scripts can be combined as in the `pre-freeze-n-post-thaw.bat` example script.
     - `C:\WINDOWS` folder on the Protected Node.
   - (Linux):
     - Save the `pre-freeze-script.bat` and the `post-thaw-script.bat` files under `/usr/sbin` of the Protected Node.
     - Make scripts executable (**chmod +x** <*script*>).
4. Initiate a backup of the PN from the onQ Portal to verify the results.

(Agent-less PNs) To make dynamic disks available for backup:

VMware doesn't support dynamic disks: the VSS Writers metadata on which onQ depends isn't available from the ESXi host. Therefore, to ensure that onQ can back up the dynamic disks, use a freeze and thaw script to install `VSSWriterData.exe`.

1. Download the example script (`vmwQuorum.bat`).

2. Log on to the PN and save `vmwQuorum.bat` to `C:\Program Files\VMware\VMware tools\backupscripts.d\`.
3. From the onQ Portal, initiate a backup of the PN to verify the results.

Related Topics

Back up and restore Oracle 11g database on Linux
Back up and restore Oracle 10g+ database on Windows

9.14 (Agent-based PNs) Methods of Performing Incremental Backups

After onQ performs an initial snapshot of your protected nodes, onQ performs incremental updates from that point forward. onQ can employ one of two scan solutions to achieve this goal: Filter Driver or Non-Filter. The onQ Filter Driver is supported for agent-based PN enrollment only.

During enrollment, the Protect Me wizard installs the onQ Filter Driver, but it is disabled by default. If you want to choose this solution you must enable it.

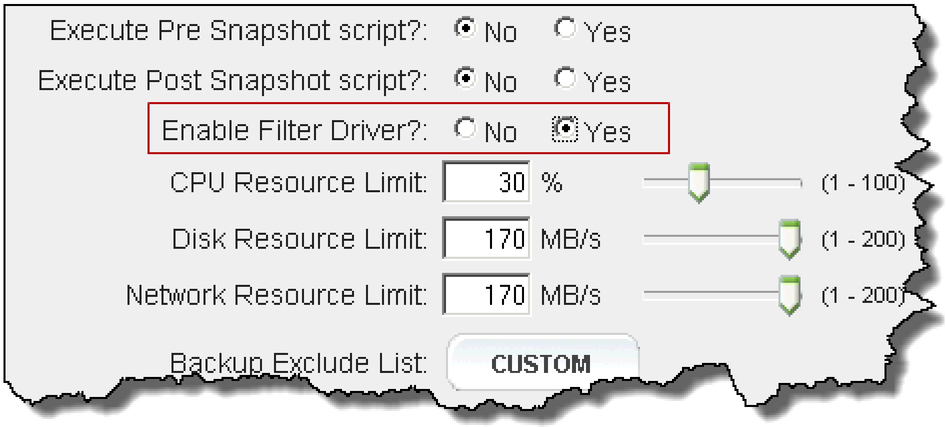
onQ Filter Driver enables faster and more efficient incremental updates. The onQ Filter Driver is no different than the filter drivers that Windows backup products use. The major difference between the onQ Filter Driver and Non-Filter is that the onQ Filter Driver installs as a service on the protected node, using some system resources.

Though you don’t need to know the “ins and outs” of each solution, you do need to understand when each performs optimally, so that you can choose the right solution for your organization:

Circumstance	**Recommendation**	
	onQ Filter Driver (Optional)	**Non-Filter (Default)**
PN stores a large number (millions) of files	✓	
PN stores large files that change frequently	✓	
PN files don’t change frequently		✓
PN stores a small number of files		✓
PN has resource constraints (memory, CPU, disk space)		✓

To enable the onQ Filter Driver:

1. Log on to the HA’s onQ Portal.
2. Stop protection.
3. Go to **PROTECTION CONFIG** tab, select the protected node, then click **MODIFY** > **ADVANCED**.
4. Select the **Enable Filter Driver? Yes** radio button, then **SAVE**.



Execute Pre Snapshot script?: ● No ○ Yes

Execute Post Snapshot script?: ● No ○ Yes

Enable Filter Driver?: ○ No ● Yes

CPU Resource Limit: 30 % (1 - 100)

Disk Resource Limit: 170 MB/s (1 - 200)

Network Resource Limit: 170 MB/s (1 - 200)

Backup Exclude List:

Related Topics

Configure automatic testing of RNs

9.15 Perform full rescan on PN

In most cases, you will not need to perform a full rescan of the node that you are protecting because the onQ handles all the changes based on the backup schedule that you configured. However, you might want to perform a rescan if:

- you are not comfortable with the delta
- a lot of changes occurred and you don’t want to wait for the next scheduled backup

To initiate full rescan:

1. Log on to the HA’s onQ Portal.
2. Go to **DASHBOARD** tab > **PROTECTED NODES** page.
3. Unlock the page.
4. In the Protected Node column, click on the node name button for the protected node that you want to rescan.
5. When asked if you want to **Force a Full Rescan on next backup?**, click **CONFIRM**.

9.16 Enable onQ to back up shared volumes

Aside from specifying the shared volume (mount point) at that time that you enroll the PN, in order for onQ to back up shared volumes, these shared drives need to include the required privileges. This requirement does not apply to fixed drives.

To set these privileges:

1. If your PN is a Win2k8 system, apply the hotfix 270891 as described in Microsoft's KB article 973278 to be able to back up NAS volumes:
   - 64-bit Win2K8
   - 32-bit Win2K8
2. Configure the onQ Service service to run as one of the following:
   - the same administrator that is currently logged on to the PN
   - Local administrator
   - Domain administrator

Warning: The onQ Service is designed to automatically map the drive for backup. To avoid conflicts, ensure that the user that runs the onQ Service does not have the same share mapped to the same drive letter as you define in Recovery Node Configuration and in Step 4 below. Otherwise, the backup will fail.

3. Ensure that the CIFS-enabled shares are mapped to the protected nodes with either Local administrator or a Domain administrator.
4. Specify the shared volume (mount point) at that time that you enroll the PN. If already enrolled, modify the PN's configuration.

Troubleshooting

If the backup failed with an `invalid drive` error and the `sq.log` indicates that `The local device name has a remembered connection to another network resource`, the onQ Service is trying to map the drive but can't because the user that the onQ Service is running as is logged in to the server, and already has the drive mapped (see details in Step 2 above). To resolve this issue:

1. Log off from the server.
2. Disconnect the drive for the user running the onQ Service.
3. Change the drive letter for the mapping.

10

Security and Communications

10.1 Test HA-to-DR Link

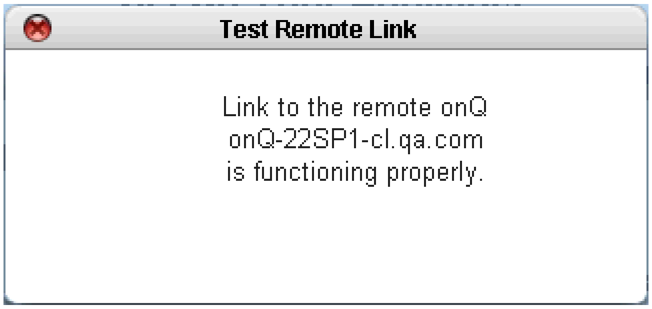
Use this procedure to:

- test the trust relationship between the Appliances.
- test inter-Appliance communications on port 81. This test does not test remote ssh communication.

To test your HA-to-DR link:

1. Go to **APPLIANCE CONFIG** tab > **onQ (REMOTE)** page.
2. Click **Test Remote Link**.

   If successful, you see a page similar to this:



Test Remote Link

Link to the remote onQ
onQ-22SP1-cl.qa.com
is functioning properly.

Related Topics

Monitor DR Appliance
Network and Firewall Requirements

10.2 Set up trust relationships

Before your Appliances will work in production, you need to set up the trust relationship between the HA and the DR Appliance. Moreover, if you have a DR Mirror, you must set up the trust relationship between the DR Appliance and the DR Mirror.

Also, you need to re-establish this trust relationship between the HA and DR Appliance if you change their roles, which is required in the event of a disaster (see (Workflow) Fail over HA to DR Appliance).

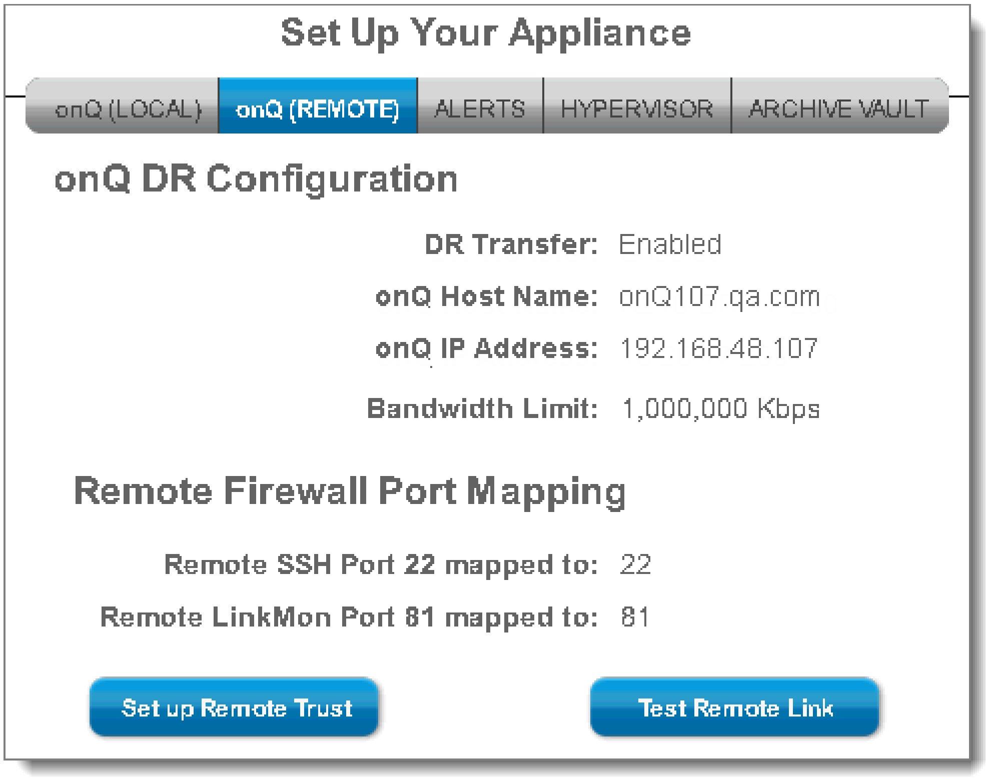
Therefore, just in case you have a disaster, it's best practice to set up the trust relationship in advance so that it's immediately available when you need it. As such, consider performing the following procedure on both the HA and, if you have a DR Mirror, the DR Appliance.

To set up the trust relationship between HA and DR Appliance:

1. Log on to the HA's onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **onQ (REMOTE)** page.

   Simply click on the **Set Up Remote Trust** button.

Example of HA:



onQ DR Configuration

DR Transfer: Enabled

onQ Host Name: onQ107.qa.com

onQ IP Address: 192.168.48.107

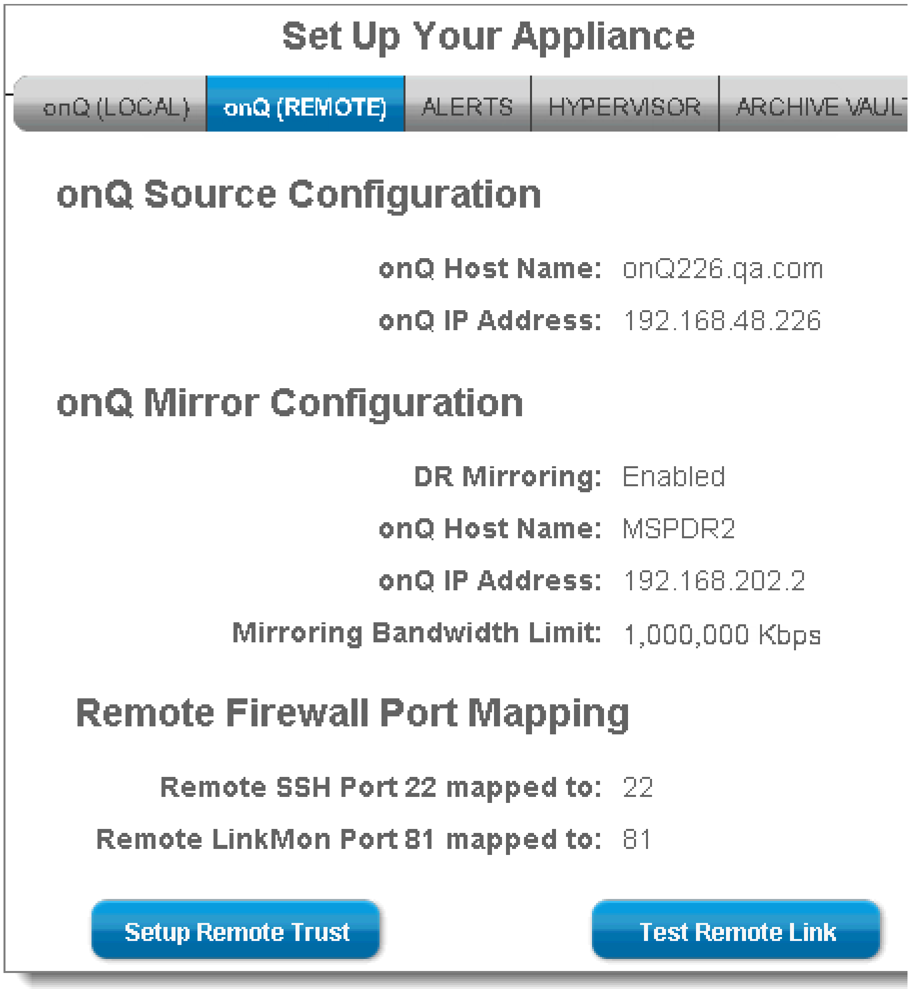
Bandwidth Limit: 1,000,000 Kbps

Remote Firewall Port Mapping

Remote SSH Port 22 mapped to: 22

Remote LinkMon Port 81 mapped to: 81

Example of DR Appliance:



Set Up Your Appliance

onQ Source Configuration

onQ Host Name: onQ226.qa.com

onQ IP Address: 192.168.48.226

onQ Mirror Configuration

DR Mirroring: Enabled

onQ Host Name: MSPDR2

onQ IP Address: 192.168.202.2

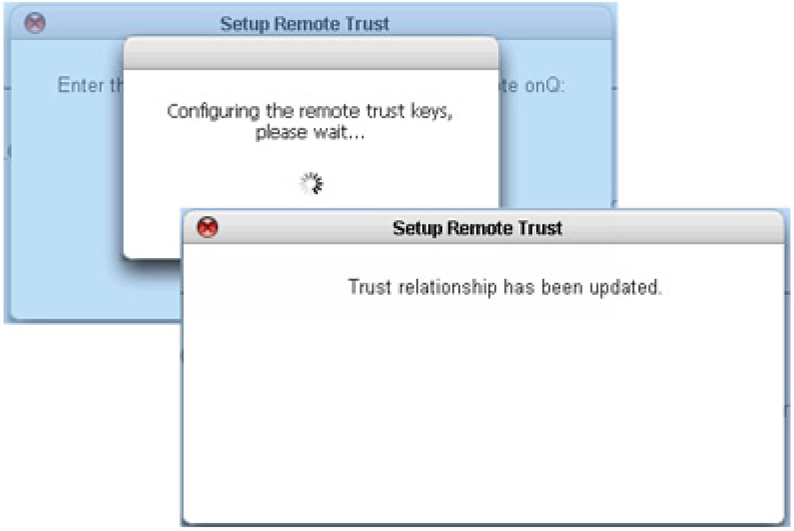
Mirroring Bandwidth Limit: 1,000,000 Kbps

Remote Firewall Port Mapping

Remote SSH Port 22 mapped to: 22

Remote LinkMon Port 81 mapped to: 81

3. Type the VARAdmin password for the *other* onQ Appliance, then **Update Trust**.



Configuring the remote trust keys, please wait...

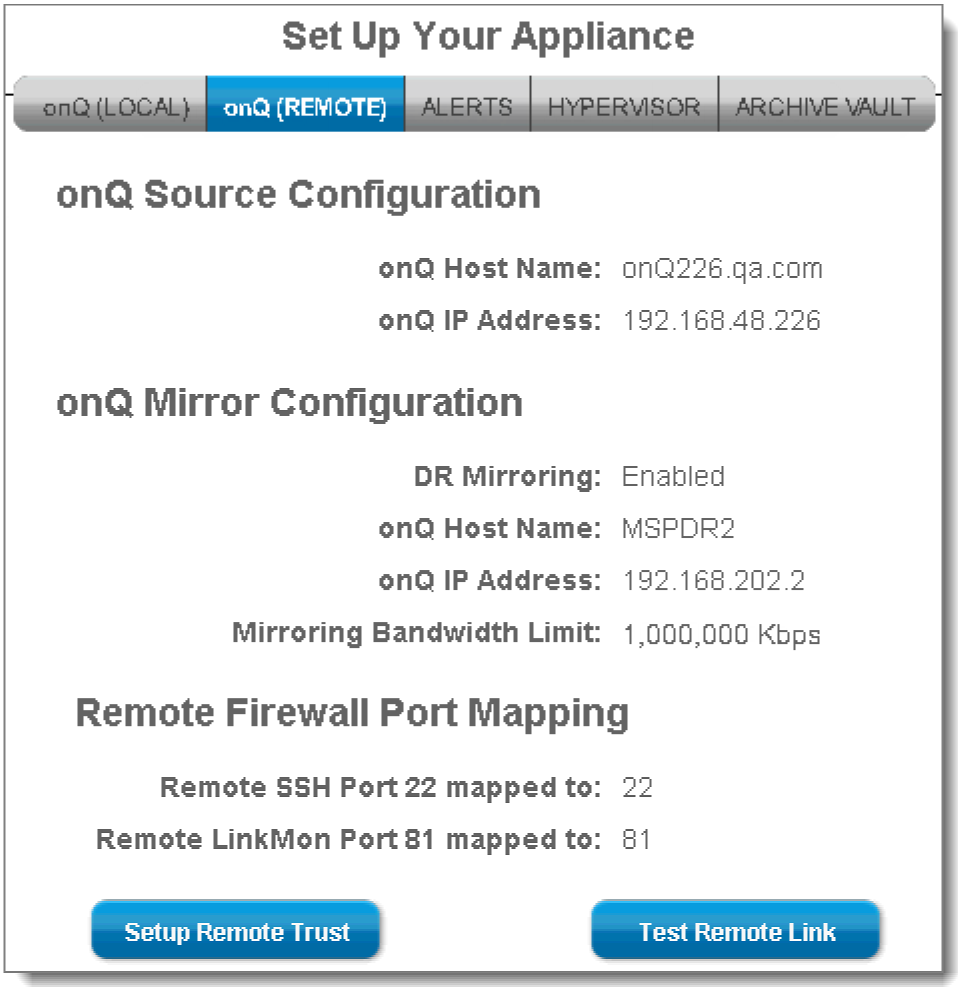
Trust relationship has been updated.

4. Test the link.

To set up the trust relationship between DR Appliance and DR Mirror:

1. Log on to the DR Appliance's onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **onQ (REMOTE)** page.

Example of DR Appliance:



Set Up Your Appliance

onQ Source Configuration

onQ Host Name: onQ226.qa.com
onQ IP Address: 192.168.48.226

onQ Mirror Configuration

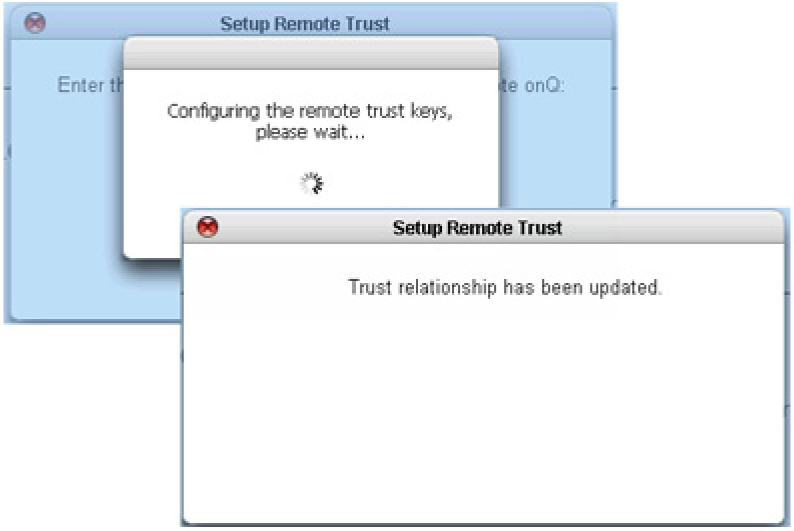
DR Mirroring: Enabled
onQ Host Name: MSPDR2
onQ IP Address: 192.168.202.2
Mirroring Bandwidth Limit: 1,000,000 Kbps

Remote Firewall Port Mapping

Remote SSH Port 22 mapped to: 22
Remote LinkMon Port 81 mapped to: 81

3. Simply click on the **Set Up Remote Trust** button. These buttons are inactive if you have not yet enabled DR mirroring.

4. Type the VARAdmin password for the *other* onQ Appliance, then **Update Trust**.



Setup Remote Trust

Enter th... ...te onQ:

Configuring the remote trust keys, please wait...

Setup Remote Trust

Trust relationship has been updated.

5. Test the link.

10.3 Create Custom Networks for RNs

If you currently segment your traffic using VLANs (virtual networks), you will want to replicate this configuration on your onQ. For example, your traffic might be segmented by internal and external (DMZ) traffic, by department, or iSCSI vs. SAN.

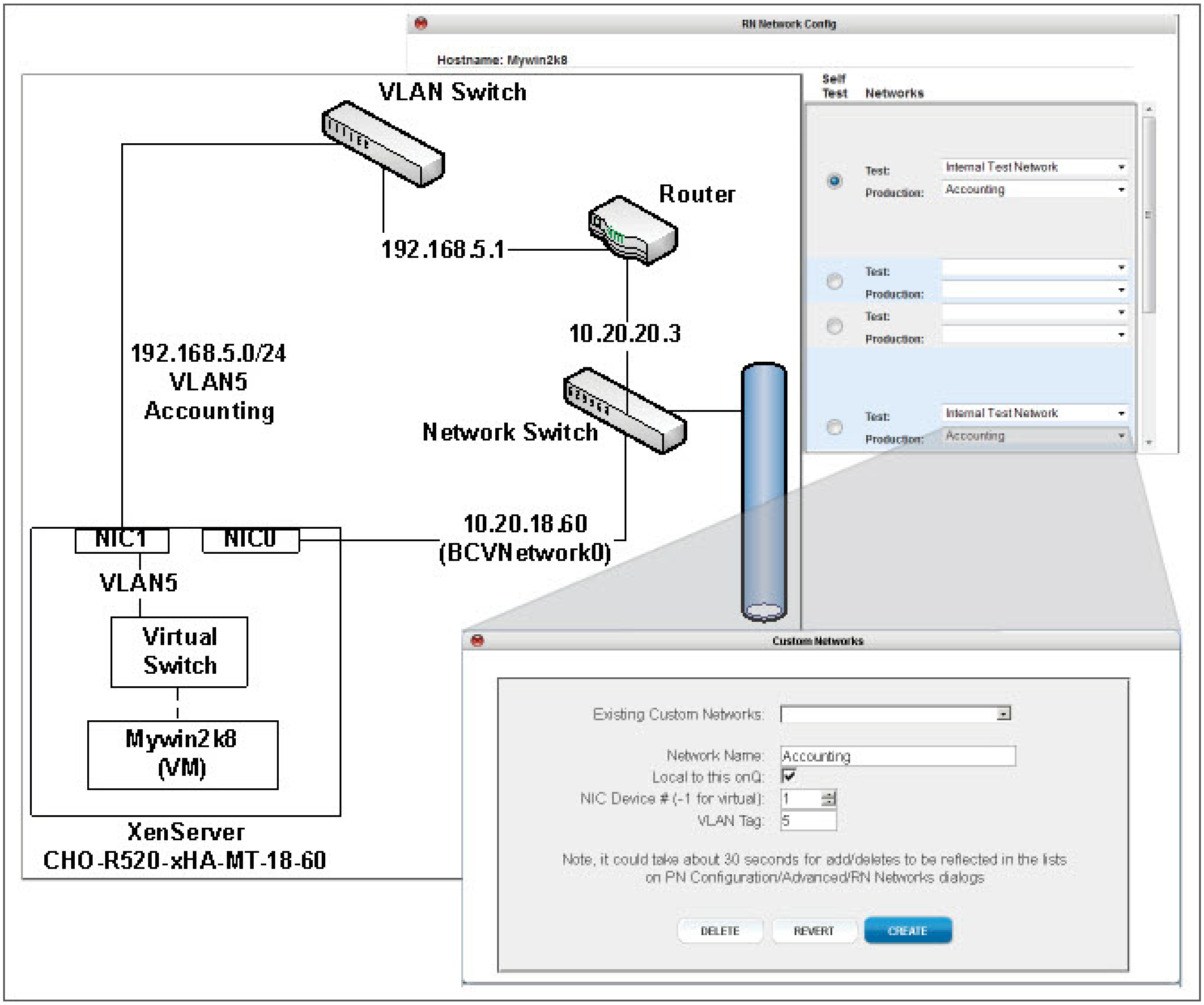
Quorum recommends that you set up these custom networks using the onQ Portal. Do not set up these custom networks on the onQ hypervisor directly. The onQ Portal provides all the bells and whistles to help you emulate your network easily and safely.

To create virtual networks:

1. Identify your broadcast domains (aka VLAN IDs or VLAN tag), the ports that they comprise, and the PNs that reside in each network.
2. Log on to the onQ Appliance's onQ Portal. You must log on as `varadmin` user. When you create a network on the HA, it does not automatically appear on the DR. You must make such changes on both onQ Appliances.

3. Click the **APPLIANCE CONFIG** tab > **HYPERVISOR** page.
4. Click the **CUSTOM NETS** button. The Modify Custom Networks dialog appears.
5. Specify the custom network parameters, click **CREATE**, then **SAVE**.
   - **Existing Custom Networks**. If you've previously defined a custom network using the onQ Portal, it appears in this list; however, if you previously configured custom networks on the onQ hypervisor directly, the onQ Portal does not present these networks.
   - **Network Name**. Specify a descriptive name that helps you identify this VLAN (or the type of traffic on this virtual network). For example, `DMZ Traffic` or `Accounting Traffic`. After you define your custom network, this network name appears in the **Existing Custom Networks** drop-down list. Any virtual network that you create will be available as a test network or a production network.
   - **Local to this onQ**. Checking this check box means that the network is only available to RNs of this onQ instance. Clearing the check box allows the network that you're defining to be available to the RNs that belong to all onQ instances on the onQ Appliance.
   - **NIC Device # (-1 for virtual)**. Specify either `-1` for virtual NIC or `1-4094` for a physical NIC. You cannot leave this field blank.
   - **VLAN Tag**. Specify the unique identifier (aka VLAN ID or broadcast domain) for the virtual network. An identifier is inserted into a packet header in order to identify which VLAN the packet belongs to. Switches use the VLAN Tag to determine which port(s) or interface(s) to send a broadcast packet to. This tagging allows you to create multiple VLANs on the same physical interface.

Example: *Separate VLAN for Accounting Traffic*



Hostname: Mywin2k8

Test: Internal Test Network
Production: Accounting

Test:
Production:

Test:
Production:

Test: Internal Test Network
Production: Accounting

Existing Custom Networks:
Network Name: Accounting
Local to this onQ: ☑
NIC Device # (-1 for virtual): 1
VLAN Tag: 5

Note, it could take about 30 seconds for add/deletes to be reflected in the lists on PN Configuration/Advanced/RN Networks dialogs

6. Now that you’ve created the networks, assign your RNs to those networks as outlined in Assign RNs to Networks.

10.4 Assign RNs to Networks

If you have Windows PNs that are on different subnets, you'll want to configure multiple networks so that those RNs have a pathway outside the onQ Appliance. (Linux PNs are not yet supported.) Additionally, you can create complex test networks to test your RNs.

Quorum recommends that you set up multiple networks using the onQ Portal. Do not set up these networks on the onQ hypervisor directly. The onQ Portal provides all the bells and whistles to help you emulate your network safely and easily.

Your supported Windows RNs (see Platform Support) can run in either production mode or test mode on multiple networks using virtual NICs. An RN's IP address changes during an RN build to accommodate these different networks.

The RN build process injects a default virtual NIC with the IP settings that onQ currently uses to communicate with the PN; You can use these default network settings to test the RN functionality without any modifications. However, if you need to, Windows RNs can be assigned to build with different network and IPs.

When an RN starts in production mode or test mode, it will connect to the pre-configured network. If you do not configure for multiple networks, the RN connects to the `BCV Network 0` (default) or `Internal Test Network` respectively; if you have PNs on different subnets, they will not have a pathway outside the onQ Appliance.

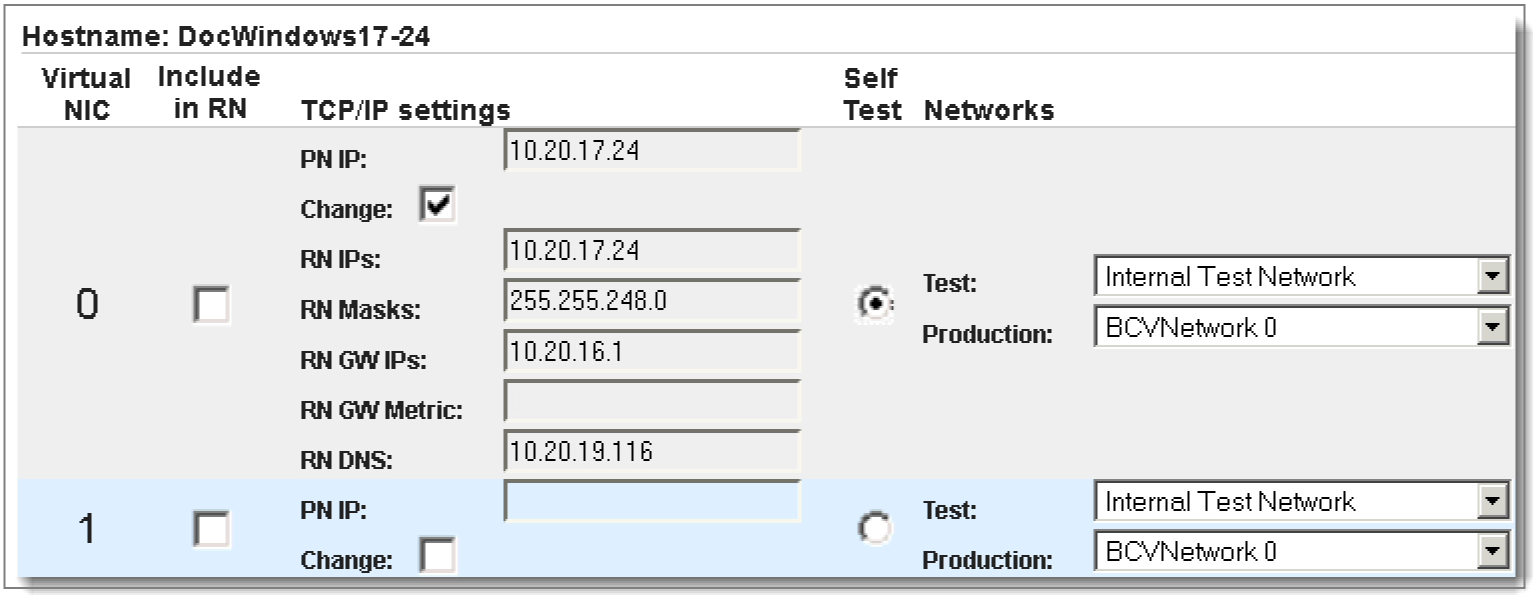
Your RNs can also be assigned to virtual networks, but you must set up these virtual networks in advance as outlined in Create Custom Networks for RNs.

If you want to attach an RN directly to a physical NIC, you do not need to create a custom network. Simply choose either the existing `BCVNetwork 0` (production only) network or one of the `Pool-wide` networks that is associated with `eth`*`X`*.

To assign RNs to networks:

1. Log on to the onQ Appliance's onQ Portal.
2. Click the **PROTECTION CONFIG** tab.

3. Select the node, then **MODIFY** button > **ADVANCED** button.
4. In the **RN Networks** field, click **Default** button.

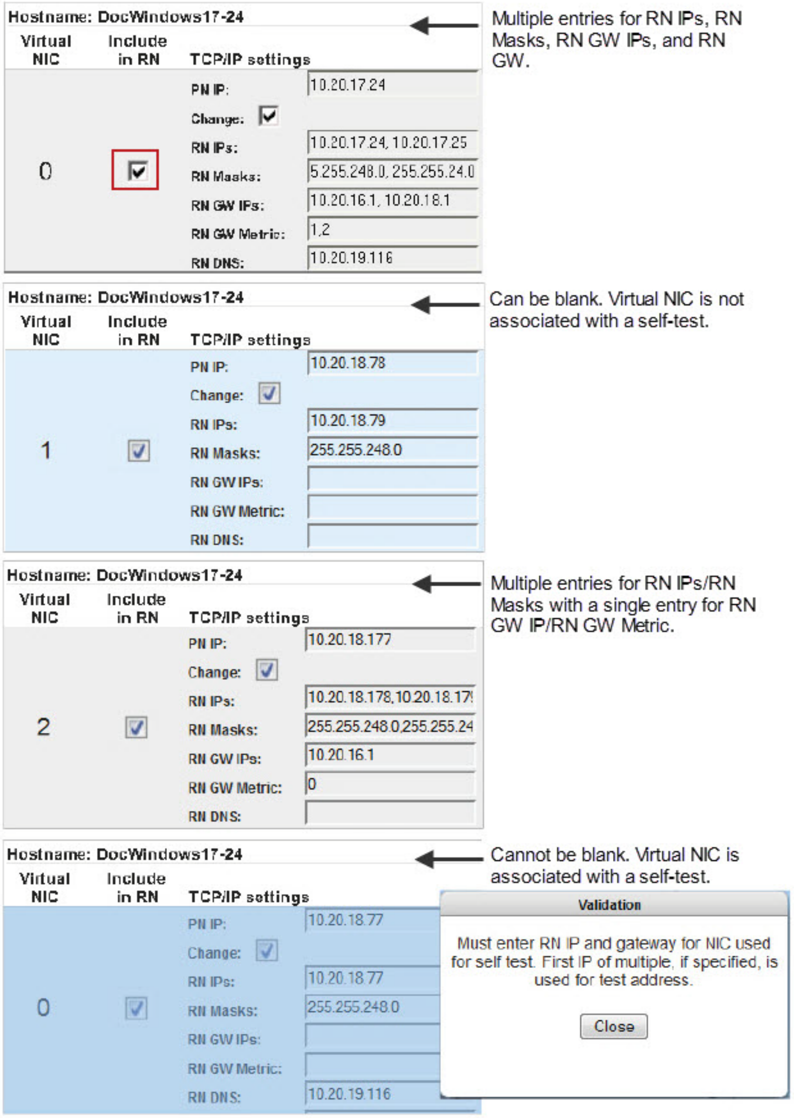


Hostname: DocWindows17-24

Virtual NIC	Include in RN	TCP/IP settings		Self Test	Networks	
0	□	PN IP:	10.20.17.24	●	Test:	Internal Test Network
		Change:	☑		Production:	BCVNetwork 0
		RN IPs:	10.20.17.24			
		RN Masks:	255.255.248.0			
		RN GW IPs:	10.20.16.1			
		RN GW Metric:				
		RN DNS:	10.20.19.116			
1	□	PN IP:		○	Test:	Internal Test Network
		Change:	□		Production:	BCVNetwork 0

5. Configure the RN’s network(s): Click the **Change** check box to display the RN defaults, which represents the PN’s networking information, make your chances, then **SAVE**.
    - **Virtual NIC**. Define your virtual NICs. The hypervisor supports up to 7 virtual NICs (NIC 0-6). NIC 0 defaults to the PN’s pre-configured TCP/IP settings. Use the **Include in RN** check box to make them available to the RN.
    - **Include in RN**. Select the check box for each Virtual NIC that you want to make available to the RN.
    - **TCP/IP settings**. Specify the networking information for each Virtual NIC that you want to make available to the RN. Select the **Include in RN** check box; otherwise, the onQ Portal will not save the networking information. You can set different IPs for the HA and DR, enabling RNs to boot up with different IPs per location. You can specify comma-separated entries for RN IPs, RN Masks, RN Gateway (GW) IPs, RN Gateway (GW) Metrics, and RN DNS, and onQ uses the first entry that you specify. You must: (1) Type the same number of RN GW Metrics as RN GW; and (2) Type the same number of RN IPs as RN Masks. RN GW metric is a 32-bit integer; as expected, the route that onQ chooses will be the available gateway with the lowest metric. RN GW IP/RN GW Metrics fields can be blank, if the virtual NIC is not associated with

a self-test.



Hostname: DocWindows17-24

Multiple entries for RN IPs, RN Masks, RN GW IPs, and RN GW.

Virtual NIC	Include in RN	TCP/IP settings	
0	☑	PN IP:	10.20.17.24
		Change: ☑	
		RN IPs:	10.20.17.24, 10.20.17.25
		RN Masks:	5.255.248.0, 255.255.24.0
		RN GW IPs:	10.20.16.1, 10.20.18.1
		RN GW Metric:	1,2
		RN DNS:	10.20.19.116

Hostname: DocWindows17-24

Can be blank. Virtual NIC is not associated with a self-test.

Virtual NIC	Include in RN	TCP/IP settings	
1	☑	PN IP:	10.20.18.78
		Change: ☑	
		RN IPs:	10.20.18.79
		RN Masks:	255.255.248.0
		RN GW IPs:	
		RN GW Metric:	
		RN DNS:	

Hostname: DocWindows17-24

Multiple entries for RN IPs/RN Masks with a single entry for RN GW IP/RN GW Metric.

Virtual NIC	Include in RN	TCP/IP settings	
2	☑	PN IP:	10.20.18.177
		Change: ☑	
		RN IPs:	10.20.18.178,10.20.18.17
		RN Masks:	255.255.248.0,255.255.24
		RN GW IPs:	10.20.16.1
		RN GW Metric:	0
		RN DNS:	

Hostname: DocWindows17-24

Cannot be blank. Virtual NIC is associated with a self-test.

Virtual NIC	Include in RN	TCP/IP settings	
0	☑	PN IP:	10.20.18.77
		Change: ☑	
		RN IPs:	10.20.18.77
		RN Masks:	255.255.248.0
		RN GW IPs:	
		RN GW Metric:	
		RN DNS:	10.20.19.116

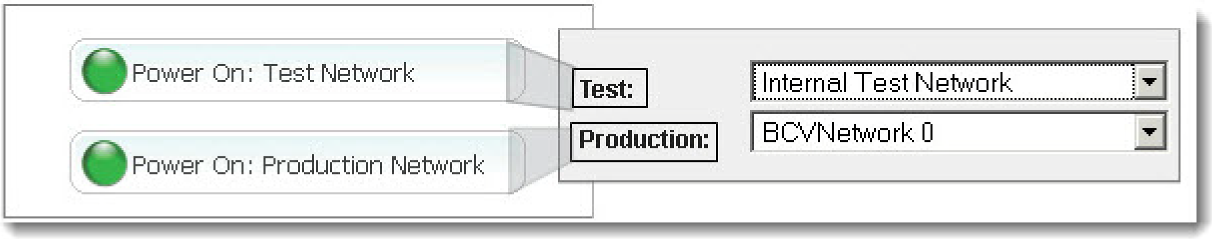
Validation

Must enter RN IP and gateway for NIC used for self test. First IP of multiple, if specified, is used for test address.

- **Self Test**. Select the Self Test radio button that corresponds to Virtual NIC and TCP/IP settings that you want the onQ to use for all Self Tests.
- **Networks**. Select the test network and production network that you want onQ to use when running an RN in either mode. Networks include:

Network Name	Description

Internal Test Network	Virtual adaptor for running RN in test mode. The Internal Test Network is not used for running RN self-tests: onQ uses the self-test network, which is not exposed during the RN build process, for self-tests.
BCVNetwork 0	Bridge attached to physical NIC0. This network is for production only; it is not available as a test network.
Pool-wide network associated with eth1	NIC1 on the onQ Appliance. Xen Server automatically creates this network, and is available to all VMs on that onQ Appliance.
Pool-wide network associated with eth2	NIC2 on the onQ Appliance. Xen Server automatically creates this network, and is available to all VMs on that onQ Appliance.



Test: Internal Test Network

Production: BCVNetwork 0

10.5 Modify TCP Ports for HA-DR Communications

You might need to modify the TCP port numbers used for communications between the local and remote onQ Appliances if inter-Appliance communications traverse a firewall that does network address translation (NAT) on the onQ Manager IP addresses.

- **Port 22** (ssh) — the default port for securely transmitting data. It's highly unlikely that you'd ever need to change this port.
- **Port 81** — the default port that each onQ Appliance uses to verify that the other is "alive"; no data is transmitted via this port.

To modify the TCP port numbers:

1. Stop protection.
2. Go to **APPLIANCE CONFIG** tab > **onQ (REMOTE)** page.
3. Click **MODIFY**.

   The **Modify Remote onQ Setup** page appears.
4. In the **Remote Firewall Port Mapping** section, make your changes, then **SAVE**.
5. Test the link.
6. Restart protection.

Related Topics

Network and Firewall Requirements

10.6 Synchronize system time

The HA uses an NTP Server for its system time (for more information, go to Configure Appliance's hypervisor settings).

The HA and the protected nodes must not be out of sync by more than 3 minutes (180 seconds) during installation or 5 minutes (300 seconds) after installation. If they are out of sync, a secure connection cannot be established.

Symptoms of an unsecure connection are outlined in (Agent-based PNs) Connection Problems.

To verify the system time on the onQ Appliance:

1. Log on to either HA’s onQ Portal or the DR Appliance’s onQ Portal.
2. Go to **DASHBOARD** tab > **onQ STATUS** page. The time appears as a header on the page.

To synchronize the clocks:

If the clock on the onQ Appliance is not synchronized with the protected nodes, you have a few choices:

- **(Best)** Enable NTP on the protected nodes or the Domain Controller.
- **(Better)** If your protected node is acquiring its time from your Domain Controller, update the time on that server.
- **(Not Recommended)** Update the system time on each individual protected node to be in sync with the onQ Appliance. This process is tedious, but it works.

10.7 Create secure connection to PNs

The network connection between the HA and the PN is generally over a trusted LAN. In some cases, though, it might be desirable to provide strong authentication between the HA and the PN.

The onQ Appliance uses an X.509 certificate for security. Your onQ Appliance ships with a unique certificate already installed. onQ automatically copies over this certificate to the PNs when you enroll protected nodes and again when you upgrade them, establishing a secure connection between the onQ Appliance and the PNs. The onQ portal’s Connection Status column uses a green padlock icon to indicate a secure connection as outlined in Monitor protected nodes. The certificate has a long expiration.

You can regenerate and/or reinstall a new certificate at any time. There are a couple of scenarios where you might want to do so:

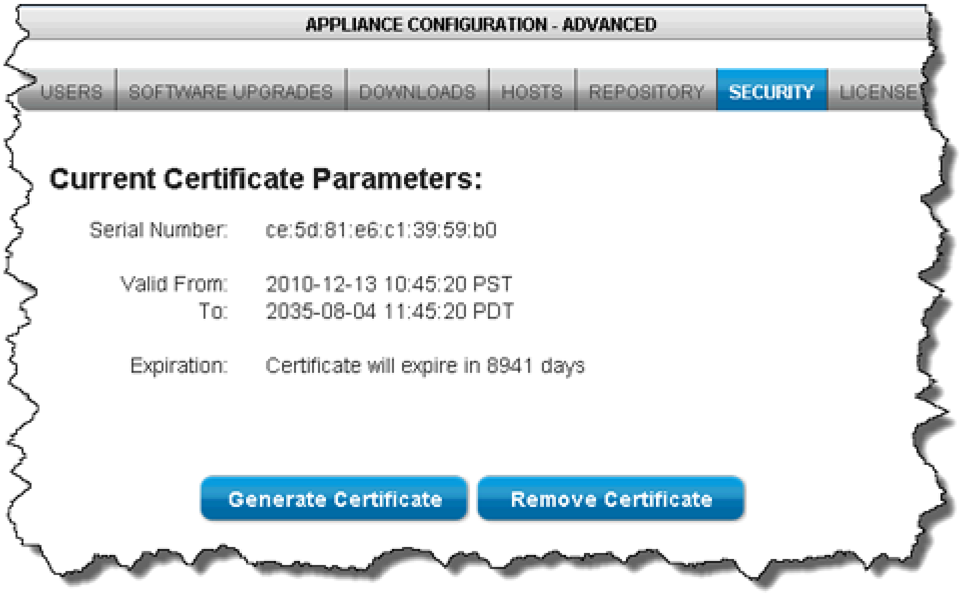
- Your HA’s certificate is corrupt; therefore, so too is the certificate on your PNs.

- You experienced a disaster scenario that resulted in you having to change the role of the DR Appliance to HA. In order for the RNs to establish a connection to that DR Appliance, you need to install the DR Appliance's certificate on those RNs.

To fix a corrupt certificate:

Fixing a corrupt certificate on requires that you regenerate and reinstall a new certificate. This procedure assumes that the HA's certificate is corrupt, but you can extrapolate.

1. Log on to the HA's onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **SECURITY** page.
3. Click **Remove Certificate**, then **Yes** to remove the existing certificate on the onQ Appliance. An example certificate is as follows:



Current Certificate Parameters:

Serial Number: ce:5d:81:e6:c1:39:59:b0

Valid From: 2010-12-13 10:45:20 PST
To: 2035-08-04 11:45:20 PDT

Expiration: Certificate will expire in 8941 days

4. Click **Generate Cerfticate**.
5. For each PN, re-install the HA Appliance certificate on the PNs by launching the HA's onQ Portal from each PN and re-enrolling the protected nodes using the **Protect Me** button.

To establish a secure connection between RNs and a DR Appliance:

Let's assume that you experienced a disaster scenario that resulted in you having to change the role of the DR Appliance to HA. (If you're performing a failback, extrapolate). In order for the RNs to establish a connection to that DR Appliance, you need to install the DR Appliance’s certificate on those RNs because the certificate that was originally installed on the PNs is specific to the HA Appliance, which has a different hostname than the DR Appliance, the current acting HA.

To do so, simply launch the DR Appliance’s onQ Portal from the PNs, then re-enroll the protected nodes using the **Protect Me** button.

To manually install the certificate:

onQ automatically installs the certificate that you generate when you enroll protected nodes and again when you upgrade them. However, you can manually install the certificate, if you desire.

1. Log on to the HA’s onQ Portal.
2. RDP to the protected node.
3. From that PN, launch the HA’s onQ Portal.
4. Go to **PROTECTION CONFIG** tab, then click on the **Update PN Security** button.
5. Click **Yes** to download the file to the protected node. Your browser saves the file to its default location.
6. Move the `*onQApplianceName*.cert` file to **C:\Program Files\Quorum\QuorumDCRM-NODE\security\**.
7. Restart the onQ Service.
8. Restart protection.

11

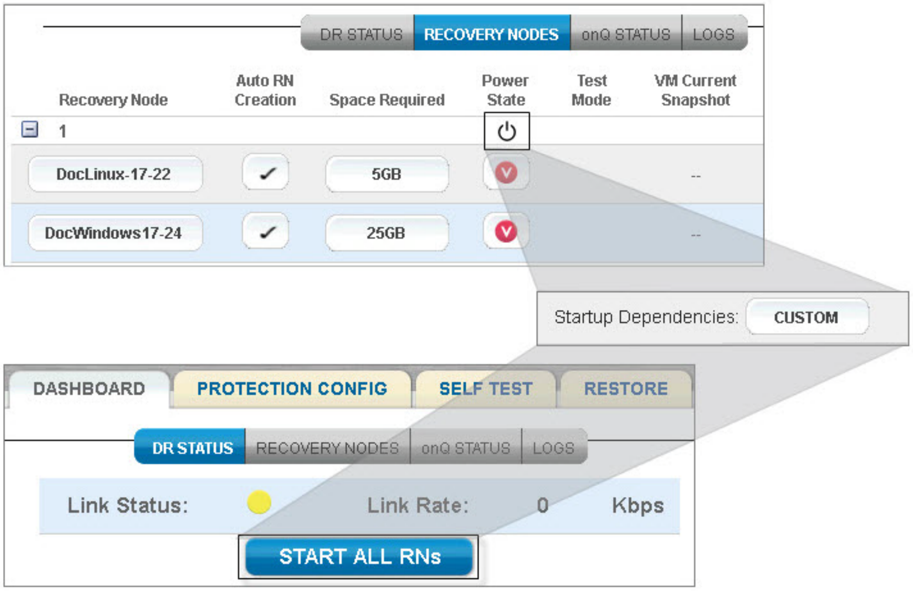
Disaster Recovery and DR Preparedness

11.1 Configure startup dependencies

If an RN depends on one or more RNs, or server outside your HA’s control, (for example, your Exchange Server depends on a Domain Controller), configure these dependencies in advance by adding RNs to groups. You can start all your recovery nodes individually, if you desire, taking into account the necessary boot order, but onQ automates all this work for you.

onQ will start a given RN after the RNs on which it depends are up and running. Startup dependencies do not apply to RNs in test mode (or automatic testing); startup dependencies apply in production mode.

onQ uses startup dependencies when a group of RNs is started on the HA Appliance or a group, or all, RNs are started on the DR Appliance or DR Mirror.

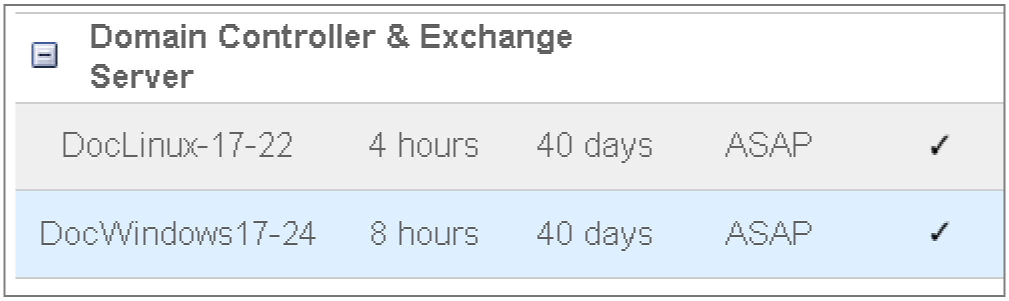


To configure an RN’s startup dependencies:

There is no limit to the number of dependencies that you can create for each RN. All dependencies in the list are executed in parallel.

All dependencies are configured on the HA. After you save that configuration, onQ transfers that information to the DR Appliances and DR Mirrors.

1. Log on to the HA’s onQ Portal.
2. Create a group to contain each dependency. For example, create a `Domain Controller & Mail Server` group and assign both the Exchange Server and the Domain Controller to that group.
   a. Click the **PROTECTION CONFIG** tab.
   b. Select the node, then **MODIFY** button.
   c. In the **Group Name** field type the name of the group, then **SAVE**.



⊟ Domain Controller & Exchange Server				
DocLinux-17-22	4 hours	40 days	ASAP	✓
DocWindows17-24	8 hours	40 days	ASAP	✓

3. Specify the startup dependencies for the RN:
   a. Click the **PROTECTION CONFIG** tab.
   b. Select the node, then **MODIFY** button > **ADVANCED** button.
   c. In the Startup Dependencies field, click the **NONE** button. If this isn’t your first time setting up a dependency, the **CUSTOM** button appears instead.
   d. Click the plus button (**+**). A default entry appears in the Startup Dependencies List.
   e. Define the **Dependent Server**. In the Dependent Server field, select the RN from the drop-down list or specify the IP address or hostname of the server that is not protected by (external to) this HA and on which the RN depends. If the dependent server is an external server, you must define it in the hosts file, unless you specify the IP address. Leave this field blank to specify a delay policy instead of a server dependency (see “**Delay**” in Step f).
   f. Specify the following information:

      Timeout – Indicate how long you want the onQ to wait for the **Dependent Server** to respond to a ping request. The default value is 5 minutes, but base the value on the typical boot time for your server. Ensure that the firewall allows ping requests. If you specify a Dependent Server, you must also specify a timeout value.

Timeout Action – Indicate what you want onQ to do with the RN if the **Dependent Server** does not respond to the ping command within the timeout period. onQ can start the RN (`Start Anyway`) without honoring the dependent server, or you can instruct onQ to refrain from starting the RN (`Abort Start`), regardless of whether all other dependencies are met, because the dependent server is critical to the RN's availability.

Delay – Specify a delay policy along with or instead of a server dependency.

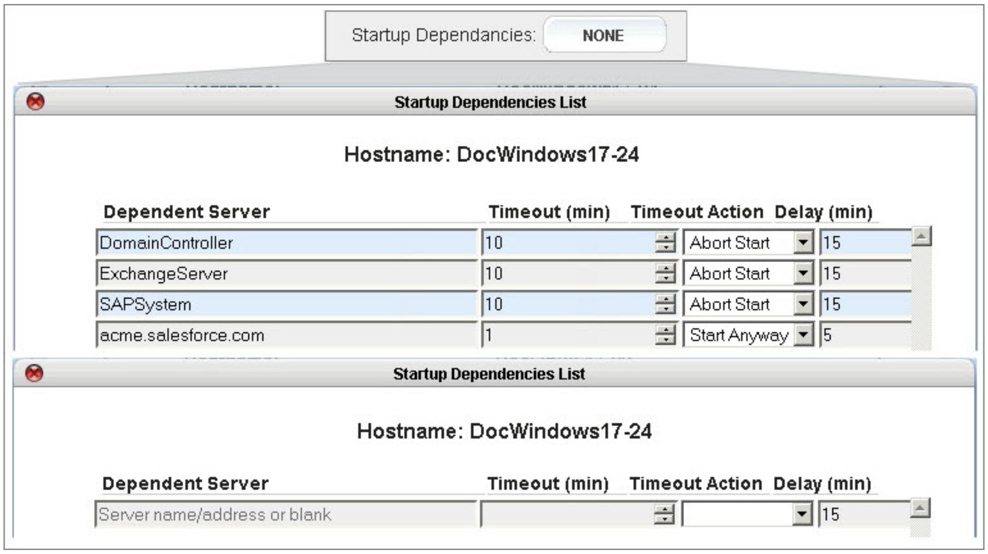
– **Delay policy *in addition* to a server dependency**. Indicate how long you want onQ to delay the RN startup after onQ detects that the dependent server is up. The default value is 1 minute, but base the value that you specify on the typical time needed for your dependent server's *applications* to respond to user requests.

– **Delay policy *instead of* a server dependency**. If a dependent RN is not configured to respond to the ping command on which **Timeout** depends, or you know that a dependent server will take a long time to boot, do not specify a server dependency; instead, create a delay policy: leave the **Dependent Server** field blank and specify a **Delay** time that accounts for the typical time needed for your dependent server's *applications* to respond to user requests. In this case, the delay option ignores values for **Timeout Action** and **Timeout**. You can only specify one such delay policy; if you try to specify two policies, the onQ Portal returns an error: `Only one row may have a blank server entry for a delay only specification`.

Example:

In the following example, all the internal dependent servers typically require 5 minutes to respond to ping requests, but this example provides an additional 5 minutes just in case. In most cases, the dependent server's applications are available within 15 minutes; therefore, in this example, the applications will have more than enough time (10-min timeout plus a 15-min delay) to become available. All dependent servers are critical to the RN's availability, with the exception of the "optional" Salesforce application.

Alternatively, a simple 15-minute (or 20) delay policy can encompass all the dependencies in the list.



Startup Dependancies: NONE

Startup Dependencies List

Hostname: DocWindows17-24

Dependent Server	Timeout (min)	Timeout Action	Delay (min)
DomainController	10	Abort Start	15
ExchangeServer	10	Abort Start	15
SAPSystem	10	Abort Start	15
acme.salesforce.com	1	Start Anyway	5

Startup Dependencies List

Hostname: DocWindows17-24

Dependent Server	Timeout (min)	Timeout Action	Delay (min)
Server name/address or blank			15

4. Click **SAVE**.
   - To revert to the last saved values, click **REVERT**.
   - To clear all data and start over, click **CLEAR**. Default values repopulate the fields provided.

   As the RN starts and if that RN has dependencies configured, the onQ Portal displays messages as the dependencies are met.

Related Topics

Cancel or override RN startup process

Start recovery nodes on HA

11.2 (Workflow) Fail over HA to DR Appliance

Use this procedure, in conjunction with your business continuity plan, in the event of a site disaster at the HA site or if you’ve experienced an onQ Appliance failure. The following table lists some of the most common failure scenarios. The table also discusses *seeding*; for information the seeding process, go to Seed the DR Repository.

Failure Scenario	**Disaster Recovery (DR) Solution**	
	DRaaS (Hybrid Cloud)	**onQ Appliance (on-Premises)**
Hardware component failure on HA	Run DR Appliance in HA role while Quorum replaces the FRU, or sells/loans you an HA replacement, followed by a pre-seeded box to synchronize the onQ Appliances.	Run DR Appliance in HA role, Quorum can employ one the following solutions: • Replace the FRU (Field Replaceable Unit) on HA. • Sell/loan you an HA replacement, followed by a seed box for the DR site, if WAN synchronization isn't possible, to synchronize the onQ Appliances. • Moves the DR to the HA site, then proceed with seeding.
Site power outage at HA site	Request that Quorum Support run DR in HA role while you fix the power outage. Afterward, Quorum can loan you a pre-seeded box to synchronize the onQ Appliances.	Run DR Appliance in HA role while you fix the power outage. Afterward, Quorum can loan you a seed box if WAN synchronization isn't possible for the DR site, to synchronize the onQ Appliances.
Software corruption on HA	Request that Quorum Support run DR in HA role while Quorum reimages/rebuilds the HA. Afterward, Quorum can loan you a pre-seeded box to synchronize the onQ Appliances.	Run DR Appliance in HA role while Quorum reimages/rebuilds the HA. Afterward, Quorum can loan you a seed box for the DR site, if WAN synchronization isn't possible, to synchronize the onQ Appliances.

Only an HA (local) can back up recovery nodes. Because your HA is unavailable, the DR Appliance (remote), whether DRaaS or on-premises, must take on this role; otherwise, your recovery nodes, which are now acting as the protected nodes, will not be backed up.

Therefore, a failover involves the DR Appliance taking on the HA role and running the recovery nodes.

As soon as your HA/local site is available, you must fail back.

To fail over to remote onQ Appliance:

1. Ensure that the local onQ Appliance is down (powered off) or that protection is off.

   When an onQ Appliance boots, protection is automatically off. Protection on an HA instructs the HA to perform backups. Given that the HA (local) still has its role set to HA, protection on that HA must be off until the failback completes.

2. Log on to the DR Appliance's onQ Portal.
3. Start all the recovery nodes on the DR Appliance (remote onQ Appliance). The boot order must take into account any interdependencies.
4. If applicable, restore the Oracle database:
   - Back up and restore Oracle 11g database on Linux
   - Back up and restore Oracle 10g+ database on Windows
5. Add a host entry for each protected node, if you haven't already done so.
6. Change the DR Appliance's role to HA.

   The recovery nodes on the remote onQ Appliance become the protected nodes; the remote onQ Appliance backs up these recovery nodes.

7. Establish a secure connection between the RNs and the DR Appliance. Go to Create secure connection to PNs.

Related Topics

(Workflow) Fail back DR to HA

11.3 (Workflow) Fail back DR to HA

You've been running your PNs on the DR Appliance; therefore, it has the most recent data. Now that you've either fixed or replaced the HA Appliance or the root cause of the site failure, use this procedure to synchronize the two onQ Appliances and fail back to the HA Appliance.

To fail back to local onQ Appliance:

1. Work with Quorum to determine the best option available to synchronize the local onQ Appliance's repository with the remote onQ Appliance's repository, which has the most recent data.

   Whether you have a Hybrid Cloud DR Appliance or on-premises DR Appliance, if WAN synchronization is not practical, Quorum loans you a seed box; in the case of DRaaS, the seed box has your seed data pre-loaded. If you were sent a seed box, connect this NAS device to your network.

2. Schedule downtime based on the time needed to synchronize the repositories.

3. During the scheduled downtime (for estimates, go to Seed the DR Repository), log on to the *remote* onQ Appliance's onQ Portal and do the following:

   a. Stop all the recovery nodes, which are acting as protected nodes.

   b. Stop protection.

4. Power on the *local* onQ Appliance, if it isn't already.

5. Change the local onQ Appliance's role to HA, if it isn't already.

6. Observe the repositories as they synchronize:

   Whether you chose to use WAN synchronization or the seed box in Step 1, that process takes place as soon as the local onQ Appliance boots up.

   As the synchronization is in progress, proceed to Step 7.

7. Log on to the *local* onQ Appliance's onQ Portal, and do the following to address failures to the protected nodes, if applicable.

   a. Disable the protected nodes, so that the onQ Appliance does not perform backups during a restore.

   b. Start protection. A restore requires protection.
   c. Restore the protected nodes using one of the following methods:
      - bare metal restore (BMR) or incremental/reversion restore
      - file level restore (FLR)
      - Windows Share Restore (WSR)
8. On the *local* onQ Appliance, bring up all the protected nodes. The boot order must take into account any interdependencies.
9. Change the remote onQ Appliance's role to DR.
10. Restart protection.
11. Establish a secure connection between the PNs and the HA. Go to Create secure connection to PNs.

Related Topics

(Workflow) Fail over HA to DR Appliance

11.4 (Workflow) Fail over a PN to an RN

When you start an RN, whether agent-based or agent-less, you are indirectly shutting down the PN and PN proxy (VM) respectively and disabling backups for that PN.

To fail over a PN to an RN *on the HA Appliance*:

1. Log on to the HA's onQ Portal.
2. Start the recovery node or, if the PN has a Build-on-Demand RN build policy, create the on-demand RN.

   If the RN is agent-less, the Backup Mode switches from `Agentless` to `Recovery Node`.
3. If applicable, restore the Oracle database:
   - Back up and restore Oracle 11g database on Linux
   - Back up and restore Oracle 10g+ database on Windows
4. Fix the PN's server.

When you're ready to fail back to the PN, go to To fail back an agent-based RN to a PN on the HA Appliance:

To fail over an *agent-less* PN to an RN *on the DR Appliance*:

If you start an agent-less PN's RN in production mode on the DR Appliance, you must perform the following steps so that the HA Appliance can back up the RN in production mode on the DR Appliance. This procedure enables onQ to back up the RN on the HA Appliance as a standard agent-based PN.

1. Start the RN in production mode on the DR Appliance.
2. RDP to the RN, then, from a browser window, launch the HA Appliance's onQ Portal.
3. Click the **Protect Me** button to install the onQ Monitor service on the RN.

   In the **Modify a Protected Node** page, switch the RN's Backup Mode from `Agentless` to `Recovery Node`, then **SAVE** the configuration.

When you're ready to fail back to the PN, go to To fail back an agent-less RN to a PN on the DR Appliance:

Related Topics

(Workflow) Fail back an RN to a PN

11.5 (Workflow) Fail back an RN to a PN

This workflow assumes that your enrolled PN went down for some reason, and that you failed over the PN to an RN as outlined in (Workflow) Fail over a PN to an RN. Now that you've fixed your original PN, use the failback procedure that pertains to your PN's enrollment method to restore the original PN:

To fail back an *agent-based* RN to a PN *on the HA Appliance*:

1. Log on to the onQ Appliance's onQ Portal.
2. Change the onQ Proxy address of the PN, if you specified an RN network configuration different than the original PN as part of multi-network support.
3. Schedule some downtime. Prevent any further changes to the RN.
4. Perform a backup of the RN in production mode.
5. Shut down the RN in production mode.
6. Perform an incremental restore of the PN, choosing the latest snapshot that you initiated in Step 4.

   onQ resumes backups of this agent-based PN.

To fail back an *agent-less* RN to a PN *on the HA Appliance*:

1. Log on to the onQ Appliance's onQ Portal.
2. Manually install the agent-based node software package on the RN. You can uninstall this software after the failback.
3. Change the onQ Proxy address of the PN, if you specified an RN network configuration different than the original PN as part of multi-network support.
4. Schedule some downtime.
5. Perform a backup of the RN in production mode.
6. Shut down the RN in production mode.

   The Backup Mode switches from `Recovery Node` to `Agentless`.
7. Boot the original PN using QUARK.

8. Perform an incremental restore, choosing the latest snapshot that you initiated in Step 5.

   onQ resumes backups of this agent-less PN. You can now uninstall the agent-based software that you installed in Step 2.

To fail back an *agent-less* RN to a PN *on the DR Appliance*:

1. Launch the DR Appliance’s onQ Portal.
2. Shut down the RN in production mode on the DR Appliance.
3. Restart the original PN in production mode on the DR Appliance.
4. Re-enable backups of the PN:
   a. Go to **APPLIANCE CONFIG** tab > **Modify a Protected Node** page.
   b. Select the PN, then **MODIFY**.
   c. Switch the PN’s Backup Mode from `Recovery Node` to `Agentless`, then **SAVE** the configuration.

11.6 Change Appliance’s role

An onQ Appliance can have one of two roles: **HA** (for high availability) or **DR** (for disaster recovery). For a new onQ Appliance, the default is `HA`.

You’ll need to change the role on the on-premises DR Appliance to HA if you experience a failure as outlined in (Workflow) Fail over HA to DR Appliance, and only if there’s a failure that warrants such a change.

If, for example, you set the onQ Appliance’s role to `HA`, then **onQ role: HA** displays at the top of each UI page on that onQ Appliance. Until you change the other onQ Appliance’s role to DR, both Appliances indicate `HA`.

To change an onQ Appliance’s role:

1. Log on to the onQ Appliance’s onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **onQ (LOCAL)** page.

   You will see a variety of settings for this onQ Appliance.
3. Click **MODIFY**.
4. In the **onQ Role** drop-down list, choose the role you want to assign.

A window appears, asking you to reboot the onQ Appliance.

5. Reboot onQ.

Related Topics

Create secure connection to PNs

11.7 Start recovery nodes on HA

In the event of a disaster, you might need to start an individual recovery node or a group of recovery nodes on HA.

Use this procedure in conjunction with the appropriate failover or failback procedures.

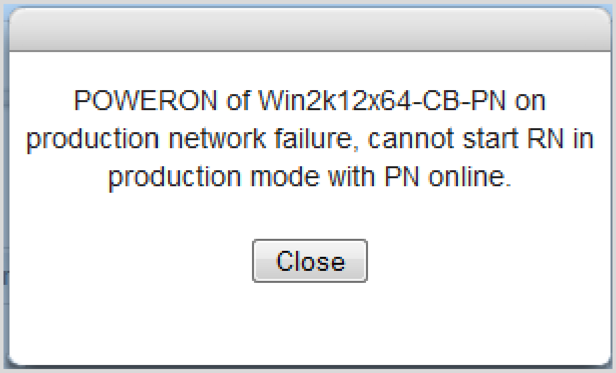
- (Workflow) Fail over HA to DR Appliance
- (Workflow) Fail back DR to HA
- (Workflow) Fail over a PN to an RN
- (Workflow) Fail back an RN to a PN

When you start an RN, whether agent-based or agent-less, you are indirectly shutting down the PN and PN proxy (VM) respectively and disabling backups for that PN.

On an HA there are two ways to start *individual* recovery nodes or a *group* of recovery nodes:

- **in production mode** — use this mode if your primary protected node failed and you want to immediately start the recovery nodes in your production environment. After you fix the PN, don't forget to stop the recovery node before bringing the PN online; otherwise, there will be network conflicts.

- **in** test mode — use this mode if you simply want to verify that the recovery node will run in the event of a disaster or to test a host running new server updates.

> **Note:** So as to avoid network conflicts, if the corresponding PN is already running in production, the onQ Portal will not let you start the RN in production. In that case, the onQ Portal displays the following error message:
>
> 
>
> POWERON of Win2k12x64-CB-PN on production network failure, cannot start RN in production mode with PN online.
>
>

You may be prompted to install application-specific software licenses upon startup of recovery nodes.

If you want to start *all DR* recovery nodes, go to Start recovery nodes on DR Appliance or DR Mirror.

(From RN tab) To start a *group* of recovery nodes in *production mode* or *test mode*:

1. From the HA, go to **DASHBOARD** tab > **RECOVERY NODES** page.
2. Unlock the page.
3. For the group, click the **Power State** (⏻) button.
4. Select either **Power On: Test Network** or **Power On: Production Network**.

   When you start in production mode, the startup order will take into account the order you specified in "Configure startup dependencies" on page 328.

(From RN tab) To start an *individual* recovery node in *production mode*:

1. (Optional) Consider suspending RN tests to "free up" resources.

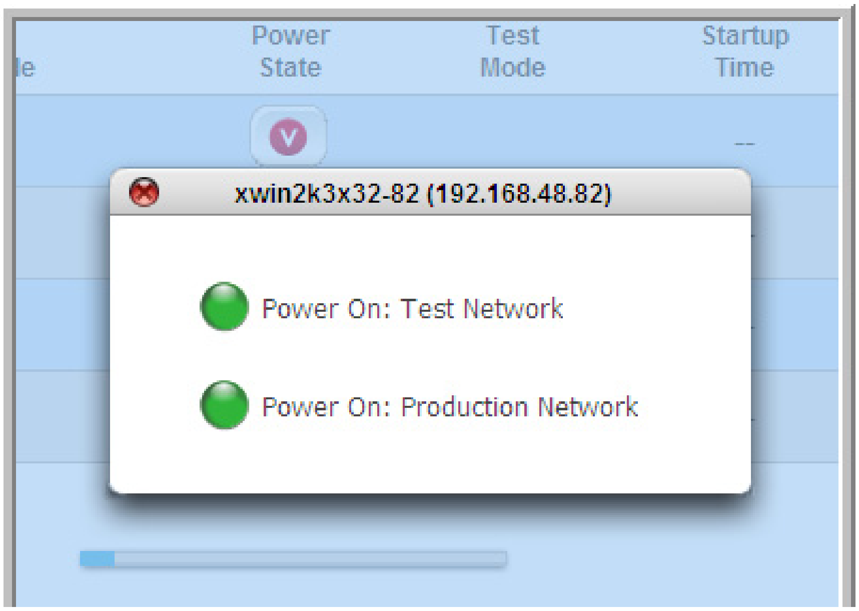
2. (Redhat 5.x RNs) Install kernel-xen RPM package, if you haven’t already.
3. Shut down the corresponding PN, if it’s online.
4. From the HA, go to **DASHBOARD** tab > **RECOVERY NODES** page.
5. Unlock the page.
6. Click the button in the **Power State** column, then choose to enable or disable backups.

   A dialog box appears that offers you a choice to disable backups for the RN (aka Recovery PN).

   - If you’re trying to recover from a failed PN, it’s important that backups continue.
   - If you are testing an RN in production after applying server updates, you might want to disable backups.

   Another dialog box appears that offers you a choice between the following two alternatives: **Power On: Test Network** or **Power On: Production Network**.

7. Choose the **Power On: Production Network** power option.



8. If you have an Oracle database, you must restore it now. Go to:
   - Back up and restore Oracle 11g database on Linux.
   - Back up and restore Oracle 10g+ database on Windows

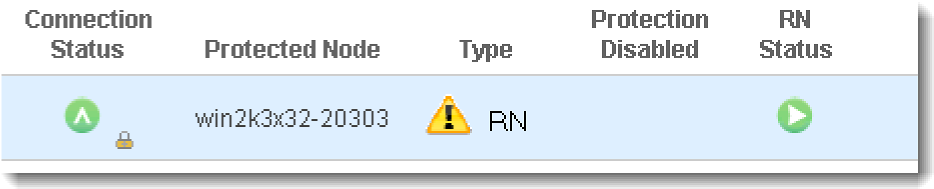
(From PN tab) To start an *individual* recovery node in *production mode*:

1. (Optional) Consider suspending RN tests to “free up” resources.
2. (Redhat 5.x RNs) Install kernel-xen RPM package, if you haven’t already.
3. Go to **DASHBOARD** tab > **PROTECTED NODES** page.
4. Unlock the page.
5. Click on the **Connection Status** button for the recovery node that you want to start.

   An information box appears that offers you this option: **Power ON the Recovery Node on the Production Network**.
6. Click **Continue**, to start the recovery node. If the recovery node has already started, this request does nothing.

   During the start up of the RN, the power indicator turns yellow with a green arrow:

Soon after, an exclamation icon appears to the right of the protected node and the **Type** field changes to **RN**, indicating that the recovery node is now running.



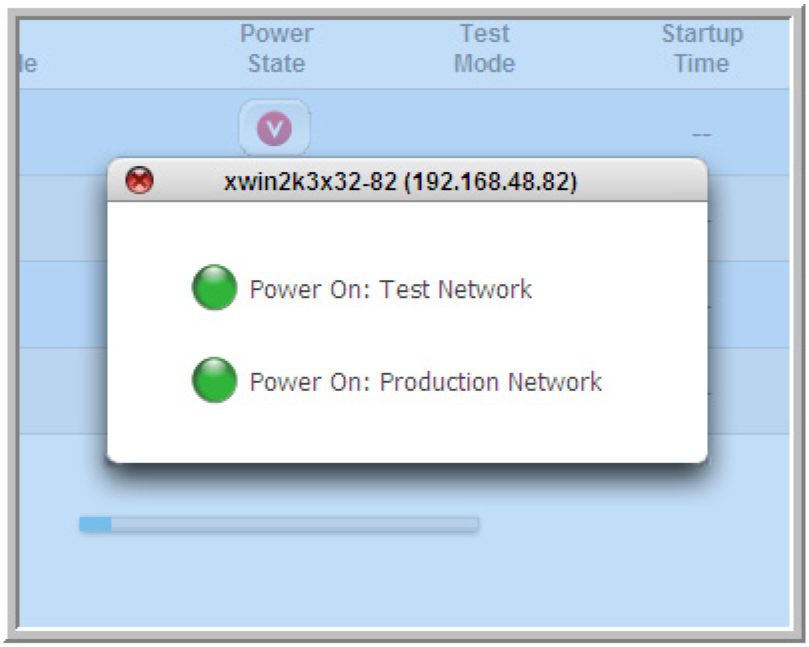
Connection Status	Protected Node	Type	Protection Disabled	RN Status
●	win2k3x32-20303	⚠ RN		●

7. if you have an Oracle database, you must restore it now. Go to:
   - Back up and restore Oracle 11g database on Linux.
   - Back up and restore Oracle 10g+ database on Windows

To start an *individual* recovery node in *test mode*:

1. Go to **DASHBOARD** tab > **RECOVERY NODES** page.
2. Unlock the page.
3. Click the button in the **Power State** column.

   A box appears that offers you a choice between the following two alternatives: **Power On: Test Network** or **Power On: Production Network**.
4. Click on the **Power On: Test Network** power option.



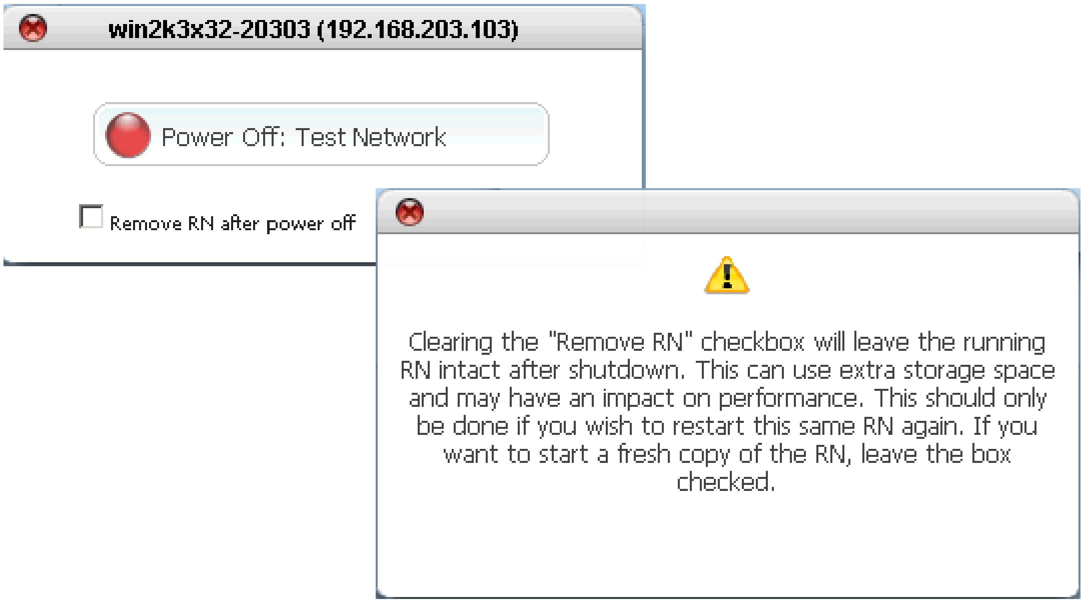
xwin2k3x32-82 (192.168.48.82)

● Power On: Test Network

● Power On: Production Network

A check mark appears in the **Test Mode** column of the appropriate status page, indicating that the recovery mode is running in test mode.

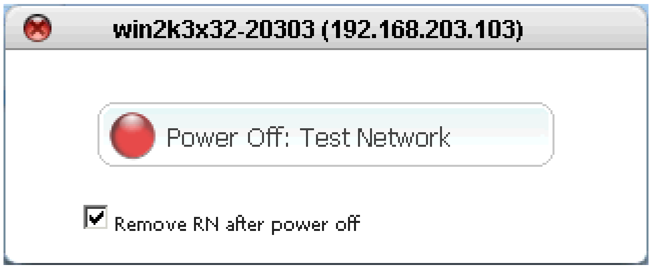
5. Launch the host’s console.
6. Perform your testing.
7. After you test the node, return it to production:
    a. Click the button in the **Power State** column.
    b. (Optional) Clear the **Remove RN after power off** check box if you want to retain this RN, keeping in mind that it is outdated.



□ Remove RN after power off

Clearing the "Remove RN" checkbox will leave the running RN intact after shutdown. This can use extra storage space and may have an impact on performance. This should only be done if you wish to restart this same RN again. If you want to start a fresh copy of the RN, leave the box checked.

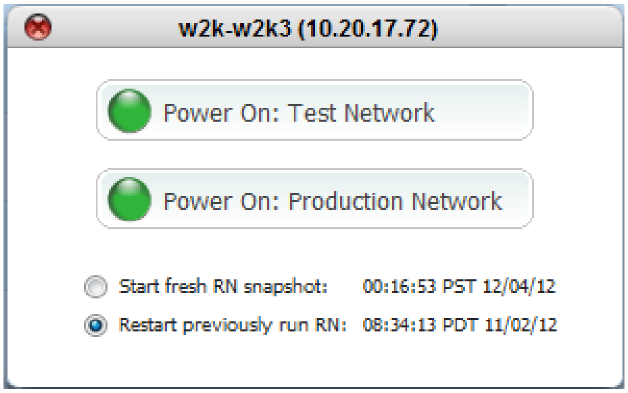
    c. Click **Power Off: Test Network** option.



☑ Remove RN after power off

The icon in the **Power State** column changes color and orientation. There might be a delay of several seconds or minutes before the icon shows a change.

If you cleared the **Remove RN after power off** check box, then the following dialog will open the next time the RN is started.



w2k-w2k3 (10.20.17.72)

○ Start fresh RN snapshot: 00:16:53 PST 12/04/12

● Restart previously run RN: 08:34:13 PDT 11/02/12

8. Choose **Start fresh RN snapshot** or **Restart previously run RN** as appropriate.

Related Topics

Self-Test Alerts

Cancel or override RN startup process

(onQ Flex) Build recovery nodes

11.8 Start recovery nodes on DR Appliance or DR Mirror

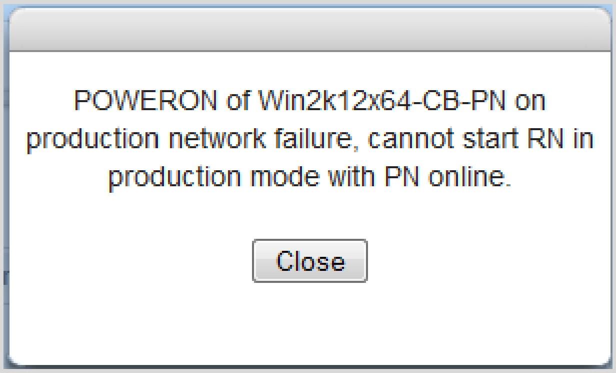
In the event of a disaster, you might need to start an individual recovery node, a group of recovery nodes, or all the recovery nodes on the DR Appliance.

Use this procedure in conjunction with the appropriate failover or failback procedures.

- (Workflow) Fail over HA to DR Appliance
- (Workflow) Fail back DR to HA
- (Workflow) Fail over a PN to an RN
- (Workflow) Fail back an RN to a PN

When you start an RN, whether agent-based or agent-less, you are indirectly shutting down the PN and PN proxy (VM) respectively and disabling backups for that PN.

Note: So as to avoid network conflicts, if the corresponding PN is already running in production, the onQ Portal will not let you start the RN in production. In that case, the onQ Portal displays the following error message:



POWERON of Win2k12x64-CB-PN on production network failure, cannot start RN in production mode with PN online.

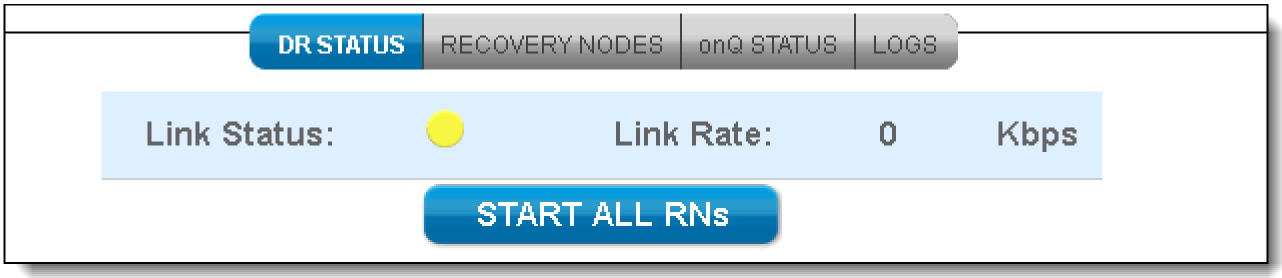
It’s possible to allocate resources to recovery nodes beyond what is physically available on the onQ Appliance. If you don’t have enough memory to start all the recovery nodes, you have two choices:

- You can change the memory allocation of PNs so that the total is less than the memory on the onQ Appliance.

- You can start your recovery nodes individually. The boot order must take into account any interdependencies.

To start *all* recovery nodes in *production mode*:

1. (Optional) Consider suspending RN tests to “free up” resources.
2. (Redhat 5.x RNs) Install kernel-xen RPM package, if you haven’t already.
3. From the DR Appliance, go to **DASHBOARD** tab > **DR STATUS** page.
4. Unlock the page.
5. Click on the **START All RNs** button.



6. Click **Apply** to start all the DR recovery nodes.

   When you start in production mode, the startup order will take into account the order you specified in “Configure startup dependencies” on page 328.

To start a *group* of recovery nodes in *production mode* or *test mode*:

1. From the DR Appliance, go to **DASHBOARD** tab > **RECOVERY NODES** page.
2. Unlock the page.
3. For the group, click the **Power State** (⏻) button.
4. Select either **Power On: Test Network** or **Power On: Production Network**.

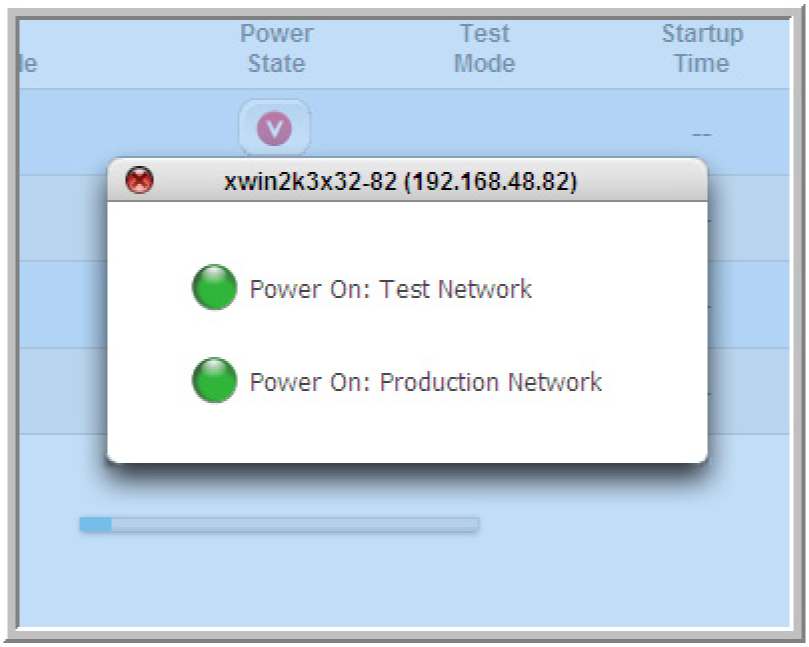
   The startup order will take into account the order you specified in “Configure startup dependencies” on page 328.

To start an *individual* recovery node in *production mode*:

You might be prompted to install application-specific software licenses upon startup of recovery nodes.

1. (Optional) Consider suspending RN tests to “free up” resources.
2. (Redhat 5.x RNs) Install kernel-xen RPM package, if you haven’t already.
3. From the DR Appliance, go to **DASHBOARD** tab > **RECOVERY NODES** page.
4. Locate the **Power State** column.

   When you click the button in the **Power State** column, a box appears that offers you a choice between the following two alternatives: **Power On: Test Network** or **Power On: Production Network**.
5. Choose the **Power On: Production Network** power option.



Related Topics

Cancel or override RN startup process

11.9 (On-Site/Prime/Plus) Build recovery nodes

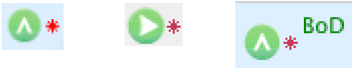
onQ creates recovery nodes (RNs) automatically if you chose the Ready-to-Run build policy, or you can manually build them if you chose the Build-on-Demand policy. You can build RNs in the following ways:

- **Update**. Apply deltas since last RN update.
- **Reinitialize**. Delete existing RN and create a new one from scratch.
- **Build**. Build an RN using a specific snapshot or an initial RN for a PN with a Build-on-Demand policy.

To update an existing RN:

Use this procedure if you want to update an existing RN with any changes since the last RN update/build. You might need to do so if you have a disaster and the RN is outdated.

You know an RN is not up-to-date if the RN Status(HA)/RN Ready Status(DR) icon is accompanied by a red asterisk:

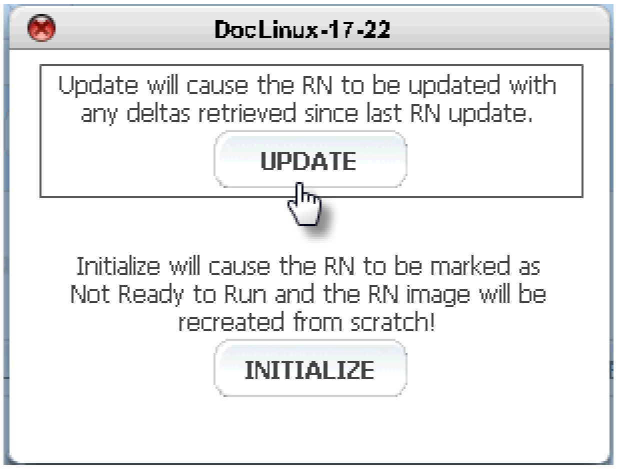


For an RN with a Build-on-Demand policy, but where onQ previously built the RN and was not instructed to delete it, a simple update is sufficient to get to the most recent state. For an RN with a Ready-to-Run policy, onQ with auto-update the RN; however, if you need an updated RN immediately, simply initiate an update rather than wait for the scheduler.

1. Log on to the HA’s or the DR Appliance’s onQ Portal.
2. Do one of the following, depending on the appliance that’s available:
   - (*HA Appliance*) Go to **DASHBOARD** tab > **PROTECTED NODES** page.
   - (*DR Appliance*) Go to **DASHBOARD** tab > **DR STATUS** page.
3. Unlock the page.
4. Do one of the following, depending on the appliance that’s available:
   - (*HA Appliance*) Click on the **RN Status** button next to the recovery node.
   - (*DR Appliance*) Click on the **RN Ready Status** button next to the recovery node.

Hover-over help for the button shows a summary of the status for that recovery node as well as the date and time the latest recovery node was generated.

5. Click the **UPDATE** button.



Update will cause the RN to be updated with any deltas retrieved since last RN update.

Initialize will cause the RN to be marked as Not Ready to Run and the RN image will be recreated from scratch!

The onQ Appliance begins to update the RN as opposed to a complete rebuild.

To reinitialize an existing RN:

Use this procedure if you want to delete the existing RN and create a new one from scratch. You might want to do so if:

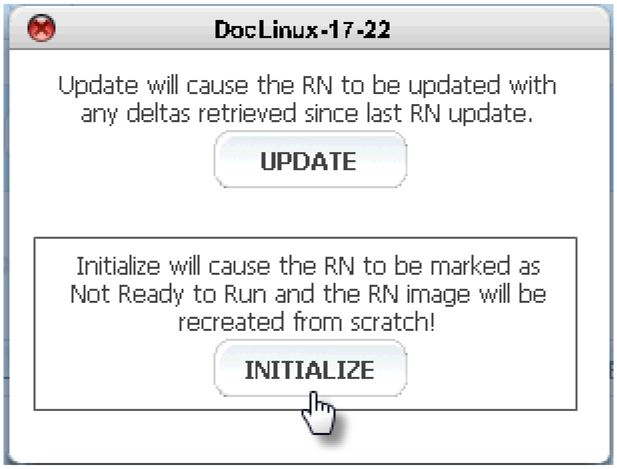
- You need a new recovery node to replace a corrupt recovery node.
- You need to build a recovery node to test, for example, new Windows Server updates.

1. Log on to the HA's or the DR Appliance's onQ Portal.
2. Do one of the following, depending on the appliance that's available:
   - (*HA Appliance*) Go to **DASHBOARD** tab > **PROTECTED NODES** page.
   - (*DR Appliance*) Go to **DASHBOARD** tab > **DR STATUS** page.
3. Unlock the page.
4. Do one of the following, depending on the appliance that's available:
   - (*HA Appliance*) Click on the **RN Status** button next to the recovery node.
   - (*DR Appliance*) Click on the **RN Ready Status** button next to the

recovery node.

Hover-over help for the button shows a summary of the status for that recovery node as well as the date and time the latest recovery node was generated.

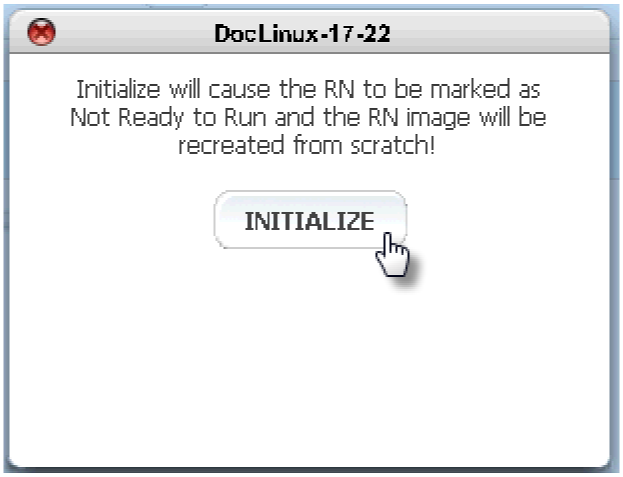
5. Click the **INITIALIZE** button.



DocLinux-17-22

Update will cause the RN to be updated with any deltas retrieved since last RN update.

Initialize will cause the RN to be marked as Not Ready to Run and the RN image will be recreated from scratch!



DocLinux-17-22

Initialize will cause the RN to be marked as Not Ready to Run and the RN image will be recreated from scratch!

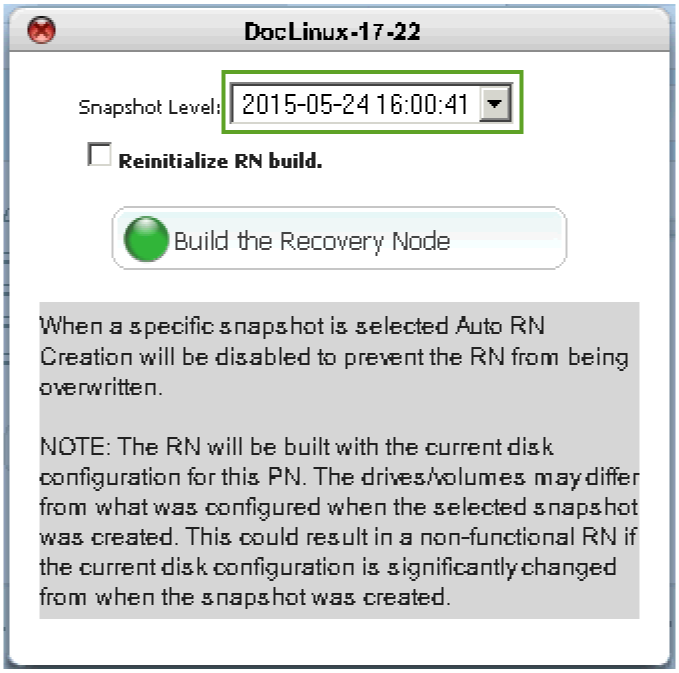
The onQ Appliance begins the process of rebuilding the RN. The RN is immediately labeled as `Not Ready to Run` and the recovery image is recreated from scratch. The

RN Status(HA)/RN Ready Status(DR) icon also briefly turns solid red during this process.

To build a point-in-time RN:

Use this procedure if you want to build an RN from a specific point in time because the latest backup is corrupt.

1. Log on to the HA's or the DR Appliance's onQ Portal.
2. Go to **DASHBOARD** tab > **RECOVERY NODES** page.
3. Unlock the page.
4. Click on the Protected Node button for the PN that you want to recreate.
5. From the drop-down list, choose a specific snapshot, then **Build the Recovery Node**. Optionally, you can select the **Reinitialize RN build** check box to build the RN from scratch instead of updating the RN with incremental data (deltas). If there are no snapshots available, this dialog does not appear.



DocLinux-17-22

Snapshot Level: 2015-05-24 16:00:41

□ Reinitialize RN build.

When a specific snapshot is selected Auto RN Creation will be disabled to prevent the RN from being overwritten.

NOTE: The RN will be built with the current disk configuration for this PN. The drives/volumes may differ from what was configured when the selected snapshot was created. This could result in a non-functional RN if the current disk configuration is significantly changed from when the snapshot was created.

onQ builds the RN to the chosen snapshot and disables `Auto RN Creation` to preserve the RN state: Ready-to-Run build policy (see About RN Build Policies) is always tied to the `MOST RECENT` snapshot; therefore, onQ disables `Auto RN Creation` so that onQ does not default to `MOST RECENT` after the next backup. The RN will be built with the current disk configuration for this PN. If the PN's current disk configuration changed significantly (for example, you added a disk/volume) from that of the selected snapshot, the RN won't be functional (might not boot); in this unlikely case, reconfigure the RN to match the PN's current disk configuration.

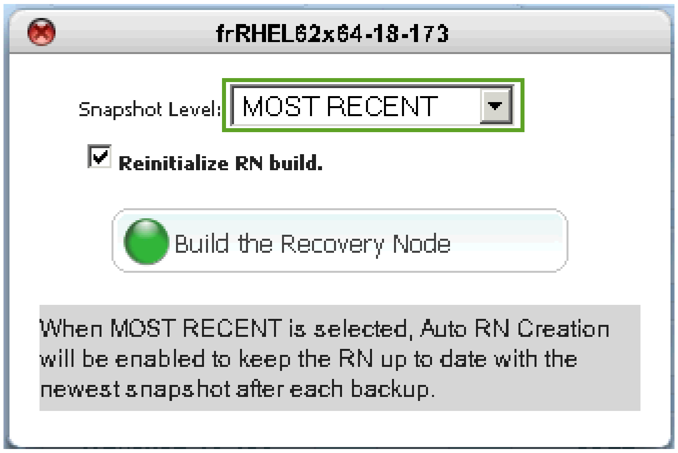
To build an initial RN:

If you chose the Build-on-Demand policy, you must manually create recovery nodes (RNs). This process can take 20 minutes to several hours depending on the size of the RN.

1. Log on to the HA's or the DR Appliance's onQ Portal.
2. Go to **DASHBOARD** tab > **RECOVERY NODES** page.
3. Unlock the page.

   The amount of space required appears in the **Space Required** column. The **RN Space Available** is shown just above the Unlock button.
4. Click on the Protected Node button for the PN that you want to recreate.
5. From the drop-down list, choose `MOST RECENT` snapshot, then **Build the Recovery Node**. The **Reinitialize RN build** check box is selected by default because this step is required to create the necessary disks.

If there are no snapshots available, the following dialog does not appear.



When MOST RECENT is selected, Auto RN Creation will be enabled to keep the RN up to date with the newest snapshot after each backup.

onQ builds the RN using the most recent snapshot and enables `Auto RN Creation`.

If you don’t, have enough disk space, onQ states that there’s `insufficient disk space`. Go to Remove recovery nodes.

Related Topics

Remove recovery nodes

11.10 (onQ Flex) Build recovery nodes

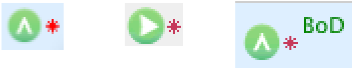
onQ creates recovery nodes (RNs) automatically if you chose the Ready-to-Run build policy, or you can manually build them if you chose the Build-on-Demand policy. You can build RNs in the following ways:

- **Update**. Apply deltas since last RN update.
- **Reinitialize**. Delete existing RN and create a new one from scratch.
- **Build**. Build an RN using a specific snapshot or an initial RN for a PN with a Build-on-Demand policy.

To update an existing RN:

Use this procedure if you want to update an existing RN with any changes since the last RN update/build. You might need to do so if you have a disaster and the RN is outdated.

You know an RN is not up-to-date if the
RN Status(HA)/RN Ready Status(DR) icon is accompanied by a red asterisk:

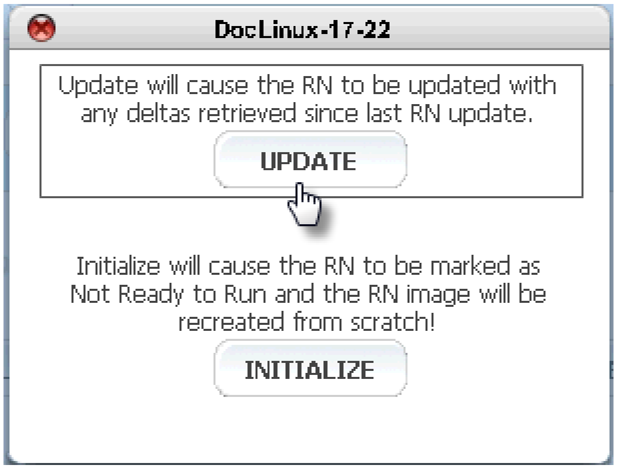


For an RN with a Build-on-Demand policy, but where onQ previously built the RN and was not instructed to delete it, a simple update is sufficient to get to the most recent state. For an RN with a Ready-to-Run policy, onQ with auto-update the RN; however, if you need an updated RN immediately, simply initiate an update rather than wait for the scheduler.

1. Log on to the HA's or the DR Appliance's onQ Portal.
2. Do one of the following, depending on the appliance that's available:
   - (*HA Appliance*) Go to **DASHBOARD** tab > **PROTECTED NODES** page.
   - (*DR Appliance*) Go to **DASHBOARD** tab > **DR STATUS** page.
3. Unlock the page.
4. Do one of the following, depending on the appliance that's available:
   - (*HA Appliance*) Click on the **RN Status** button next to the recovery node.
   - (*DR Appliance*) Click on the **RN Ready Status** button next to the recovery node.

Hover-over help for the button shows a summary of the status for that recovery node as well as the date and time the latest recovery node was generated.

5. Click the **UPDATE** button.



DocLinux-17-22

Update will cause the RN to be updated with any deltas retrieved since last RN update.

Initialize will cause the RN to be marked as Not Ready to Run and the RN image will be recreated from scratch!

The onQ Appliance begins to update the RN as opposed to a complete rebuild.

To reinitialize an existing RN:

Use this procedure if you want to delete the existing RN and create a new one from scratch. You might want to do so if:

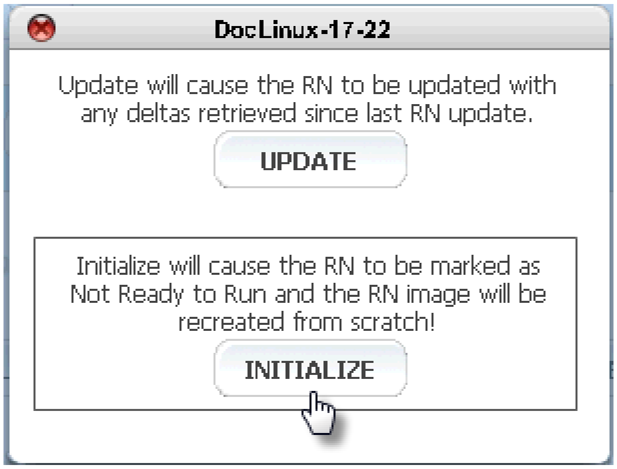
- You need a new recovery node to replace a corrupt recovery node.
- You need to build a recovery node to test, for example, new Windows Server updates.

1. Log on to the HA’s or the DR Appliance’s onQ Portal.
2. Do one of the following, depending on the appliance that’s available:
   - (*HA Appliance*) Go to **DASHBOARD** tab > **PROTECTED NODES** page.
   - (*DR Appliance*) Go to **DASHBOARD** tab > **DR STATUS** page.
3. Unlock the page.
4. Do one of the following, depending on the appliance that’s available:
   - (*HA Appliance*) Click on the **RN Status** button next to the recovery node.
   - (*DR Appliance*) Click on the **RN Ready Status** button next to the

recovery node.

Hover-over help for the button shows a summary of the status for that recovery node as well as the date and time the latest recovery node was generated.

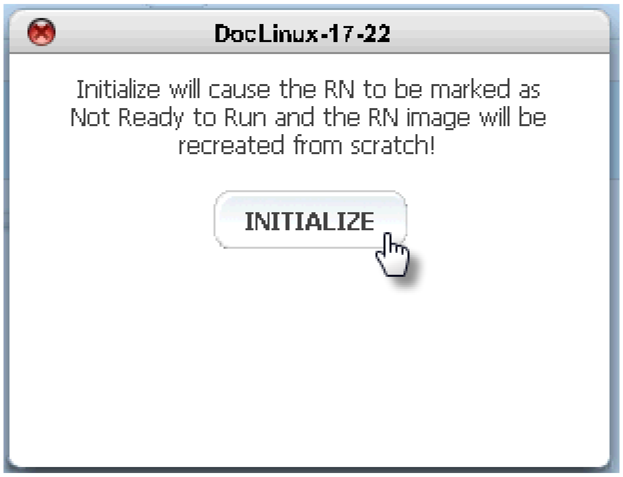
5. Click the **INITIALIZE** button.



DocLinux-17-22

Update will cause the RN to be updated with any deltas retrieved since last RN update.

Initialize will cause the RN to be marked as Not Ready to Run and the RN image will be recreated from scratch!



DocLinux-17-22

Initialize will cause the RN to be marked as Not Ready to Run and the RN image will be recreated from scratch!

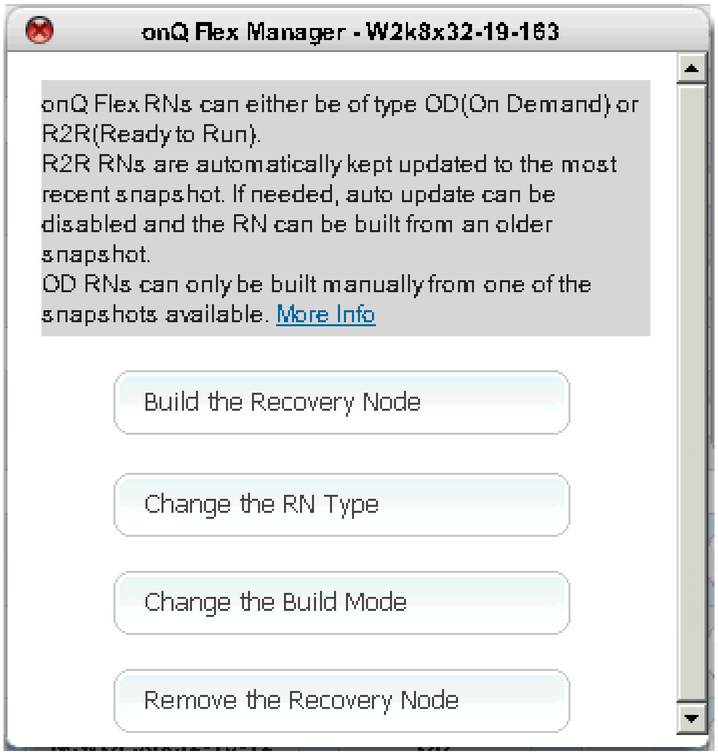
The onQ Appliance begins the process of rebuilding the RN. The RN is immediately labeled as `Not Ready to Run` and the recovery image is recreated from scratch. The

RN Status(HA)/RN Ready Status(DR) icon also briefly turns solid red during this process.

To build a point-in-time RN:

Use this procedure if you want to build an RN from a specific point in time because the latest backup is corrupt.

1. Launch the onQ Flex Manager.
2. From the onQ Flex Manager, click the **Build the Recovery Node** button.

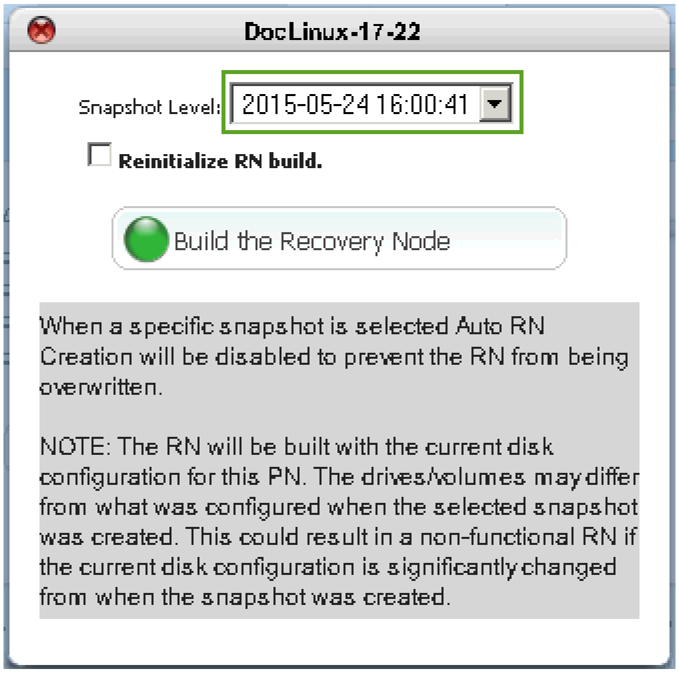


onQ Flex Manager - W2k8x32-19-163

onQ Flex RNs can either be of type OD(On Demand) or R2R(Ready to Run).
R2R RNs are automatically kept updated to the most recent snapshot. If needed, auto update can be disabled and the RN can be built from an older snapshot.
OD RNs can only be built manually from one of the snapshots available. More Info

3. From the drop-down list, choose a specific snapshot, then **Build the Recovery Node**. Optionally, you can select the **Reinitialize RN build** check box to build the RN from scratch instead of updating the RN

with incremental data (deltas). If there are no snapshots available, this dialog does not appear.



Snapshot Level: 2015-05-24 16:00:41

□ Reinitialize RN build.

When a specific snapshot is selected Auto RN Creation will be disabled to prevent the RN from being overwritten.

NOTE: The RN will be built with the current disk configuration for this PN. The drives/volumes may differ from what was configured when the selected snapshot was created. This could result in a non-functional RN if the current disk configuration is significantly changed from when the snapshot was created.

onQ builds the RN to the chosen snapshot and disables `Auto RN Creation` to preserve the RN state: Ready-to-Run build policy (see About RN Build Policies) is always tied to the `MOST RECENT` snapshot; therefore, onQ disables `Auto RN Creation` so that onQ does not default to `MOST RECENT` after the next backup. The RN will be built with the current disk configuration for this PN. If the PN's current disk configuration changed significantly (for example, you added a disk/volume) from that of the selected snapshot, the RN won't be functional (might not boot); in this unlikely case, reconfigure the RN to match the PN's current disk configuration.

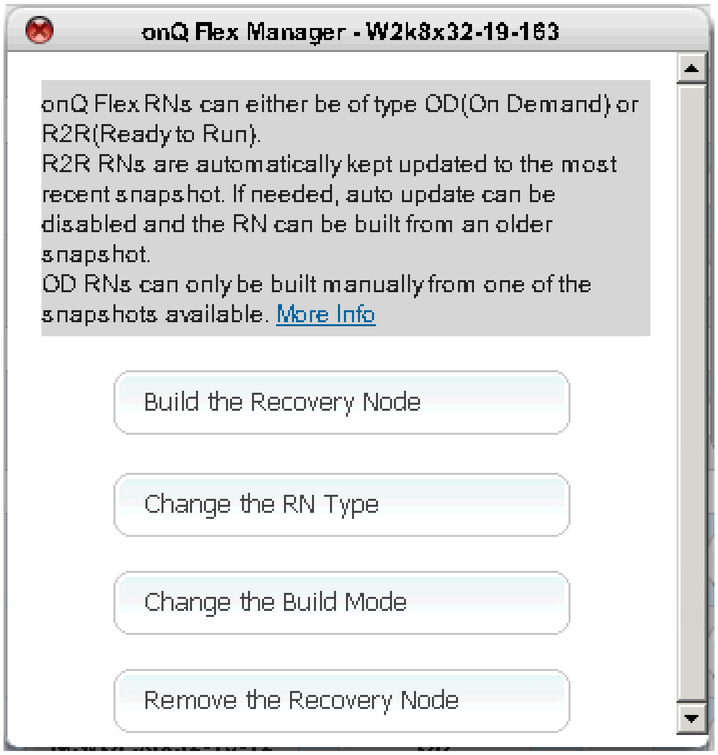
To build an initial RN:

Before you begin, learn about the charges that you may incur.

1. Launch the onQ Flex Manager.

   The amount of space required appears in the **Space Required** column. The **RN Space Available** is shown just above the Unlock button.

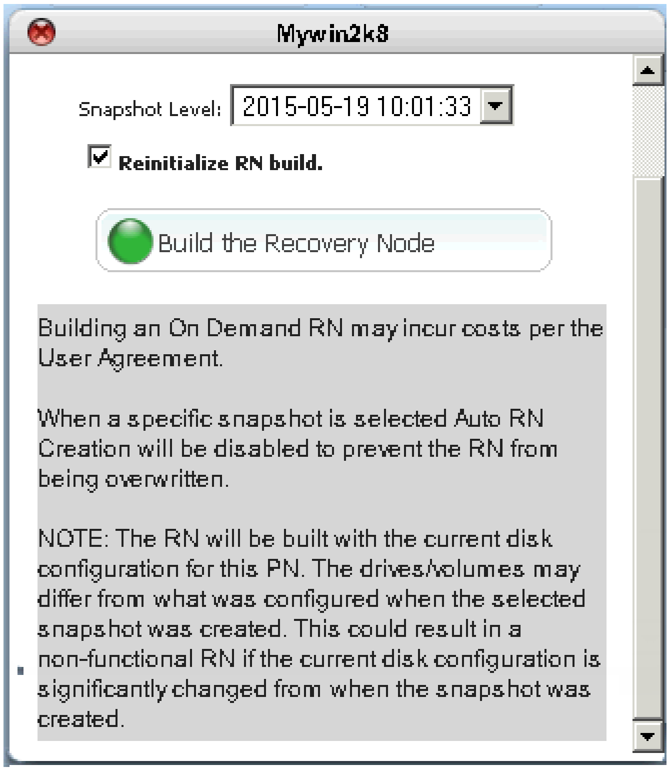
2. From the onQ Flex Manager, click the **Build the Recovery Node** button.



onQ Flex Manager - W2k8x32-19-163

onQ Flex RNs can either be of type OD(On Demand) or R2R(Ready to Run).
R2R RNs are automatically kept updated to the most recent snapshot. If needed, auto update can be disabled and the RN can be built from an older snapshot.
OD RNs can only be built manually from one of the snapshots available. More Info

If you have an onQ Flex configuration where the RN type is `OD`, and you have *never* built this RN before (aka *initial build*), the following dialog appears, with the **Reinitialize RN build** check box selected by default; however, the **Reinitialize RN build** check box is unchecked by default for all future attempts to build that RN so as to instruct onQ to retain the existing disk and build the RN from deltas, resulting in a faster recovery.



Mywin2k8

Snapshot Level: 2015-05-19 10:01:33

☑ **Reinitialize RN build.**

Build the Recovery Node

Building an On Demand RN may incur costs per the User Agreement.

When a specific snapshot is selected Auto RN Creation will be disabled to prevent the RN from being overwritten.

NOTE: The RN will be built with the current disk configuration for this PN. The drives/volumes may differ from what was configured when the selected snapshot was created. This could result in a non-functional RN if the current disk configuration is significantly changed from when the snapshot was created.

3. From the drop-down list, choose among the snapshots listed, then **Build the Recovery Node**. The **Reinitialize RN build** check box is selected by default so as to build the RN from scratch instead of updating the RN with incremental data (deltas).

   If you don't, have enough disk space, onQ states that there's `insufficient disk space`. Go to Remove recovery nodes.

Related Topics

(On-Site/Prime/Plus) Modify RN build policy

Remove recovery nodes

About onQ Flex

11.11 Remove recovery nodes

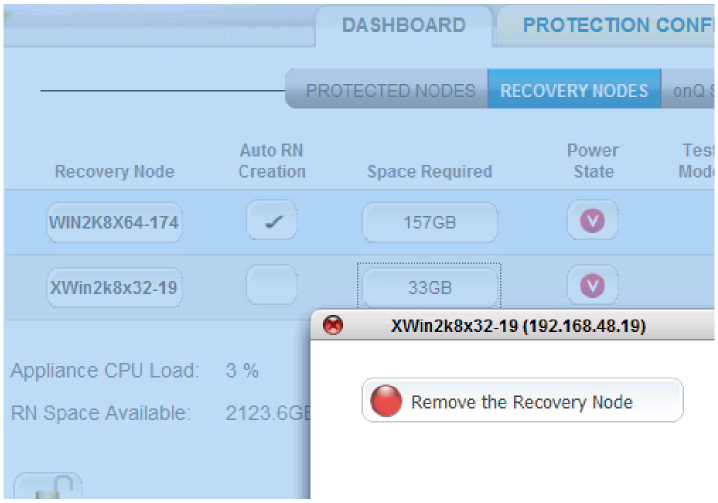
You might need to remove (aka delete) a Build-on-Demand RNs to free up disk space. Each RN uses nearly the same amount of disk space on the onQ Appliance as is used on the PN.

If there is not enough disk space on the onQ Appliance for an RN that you want to build, you must remove one or more existing BoD RNs. (You cannot add disk space at this time without reinstalling.)

Deleting the RN does not affect the corresponding PN.

(onQ On-Site/onQ Prime/onQ Plus) To remove a recovery node:

1. Log on to the HA's onQ Portal.
2. Go to **DASHBOARD** tab > **RECOVERY NODES** page.
3. Click on the **Space Required** button for the recovery node that you want to delete.
4. Click the **Remove the Recovery Node** button.



Recovery Node	Auto RN Creation	Space Required	Power State	Tes Mod
WIN2K8X64-174	✓	157GB	V	
XWin2k8x32-19		33GB	V	

Appliance CPU Load: 3 %

RN Space Available: 2123.6GE

Related Topics

(onQ Flex) Build recovery nodes

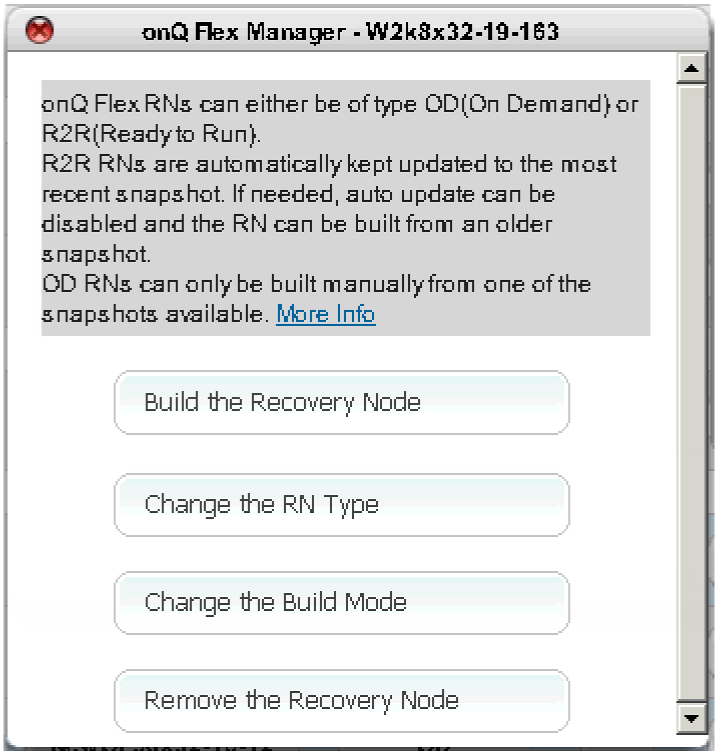
(On-Site/Prime/Plus) Modify RN build policy

(onQ Flex) Modify RN type and/or RN build policy

(onQ Flex) To remove a recovery node:

1. Launch the onQ Flex Manager.

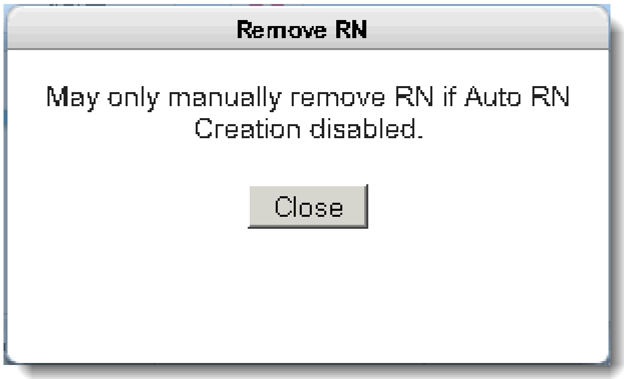
2. From the onQ Flex Manager, click the **Build the Recovery Node** button. The following dialog appears.



onQ Flex RNs can either be of type OD(On Demand) or R2R(Ready to Run).
R2R RNs are automatically kept updated to the most recent snapshot. If needed, auto update can be disabled and the RN can be built from an older snapshot.
OD RNs can only be built manually from one of the snapshots available. More Info

You might see one of the following messages:

Error: `May only manually remove RN if Auto RN Creation disabled`:

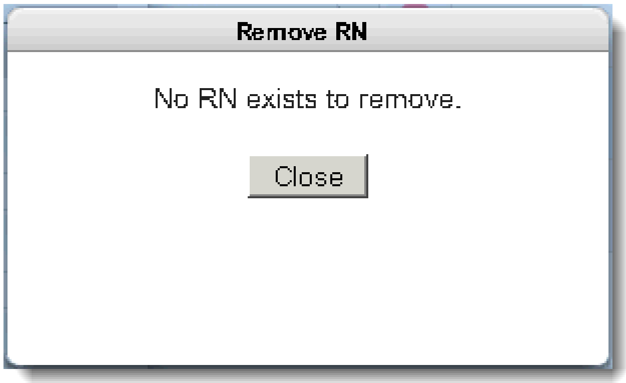


Remove RN

May only manually remove RN if Auto RN Creation disabled.

Your RN's build policy instructs onQ to make the RN immediately available upon request. onQ cannot do so if you delete the RN. To eliminate this contradiction, you must change the build policy.

Error: `No RN exists to remove`:

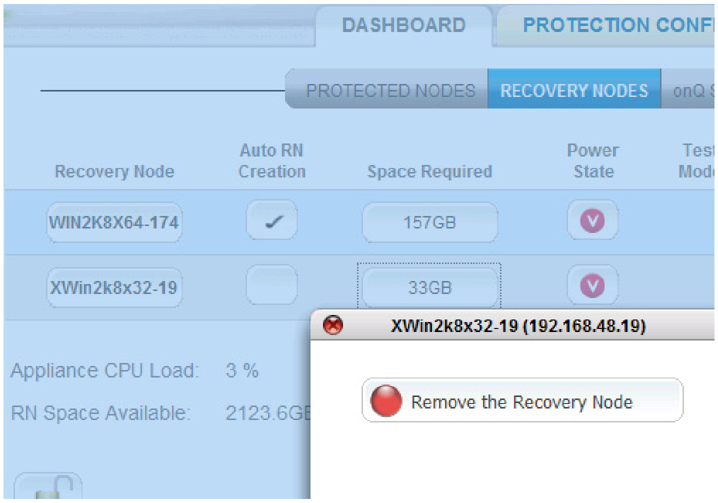


Remove RN

No RN exists to remove.

In an onQ Flex configuration where the RN type is `OD` and was never formerly `R2R`, you will never have RNs.

3. Click the **Remove the Recovery Node** button.



Related Topics

[(onQ Flex) Build recovery nodes]

[(On-Site/Prime/Plus) Modify RN build policy]

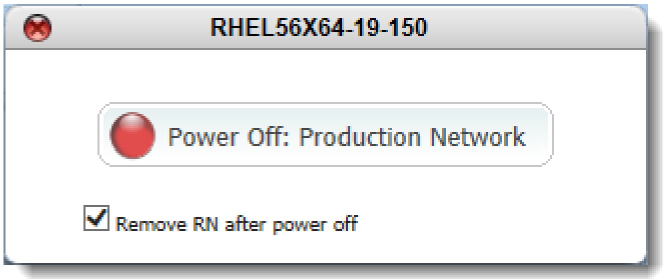
[(onQ Flex) Modify RN type and/or RN build policy]

11.12 Stop recovery nodes

Use this procedure if you are recovering from a failed PN. After you fix the PN, you must stop the recovery node before bringing the PN online; otherwise, there will be network conflicts.

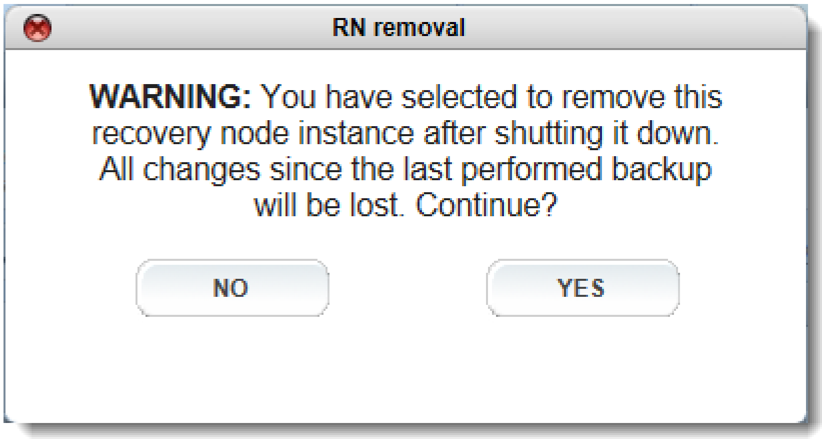
To stop an individual recovery node in *production mode:*

1. Log on to the HA's onQ Portal. In the event of a site failure, this HA was formerly your DR Appliance before you changed its role.
2. Go to **DASHBOARD** tab > **RECOVERY NODES** page.
3. Unlock the page.
4. Click the button in the **Power State** column, then **Power Off: Production Network** button, leaving the **Remove RN after power off** check box selected.



☑ Remove RN after power off

5. If you receive the following warning, click **Yes**, then perform an immediate backup.



WARNING: You have selected to remove this recovery node instance after shutting it down. All changes since the last performed backup will be lost. Continue?

This warning means that changes to the RN since the last performed back have not been written to the Repository.

Note: If you were testing an RN in production, you'd want to clear the **Remove RN after power off** check box so as to save the RN for future use. However, you're trying to recover from a failed PN, and so it's not important that you keep this RN.

6. Do one of the following:

- If you are performing this procedure as part of a site disaster, return to (Workflow) Fail back DR to HA.
- Otherwise, perform a BMR using QUARK to restore to this RN (aka Recovery PN) as outlined in (Workflow) Fail back an RN to a PN.

11.13 Back up and restore Oracle 11g database on Linux

Oracle recommends that you use RMAN to perform backups and restores of your databases.

Presumably you’re already running RMAN scripts to back up and restore your Oracle databases in production—a best practice for any business continuity plan. This procedure walks you how to back up and restore using Quorum’s example scripts. Feel free to insert hooks into these backup and restore scripts so as to execute the scripts you’re already using.

Quorum’s `pre_snap.sh` script is optional; for example, you might prefer to use cron jobs or other scheduler; as such, discuss these options with your Linux Oracle Database Administrator.

You should not have any difficulties using your existing scripts in an onQ environment because backup and restore operations are independent of onQ. However, before you use your scripts in an onQ environment, ensure that they are performing database backups and restores as expected.

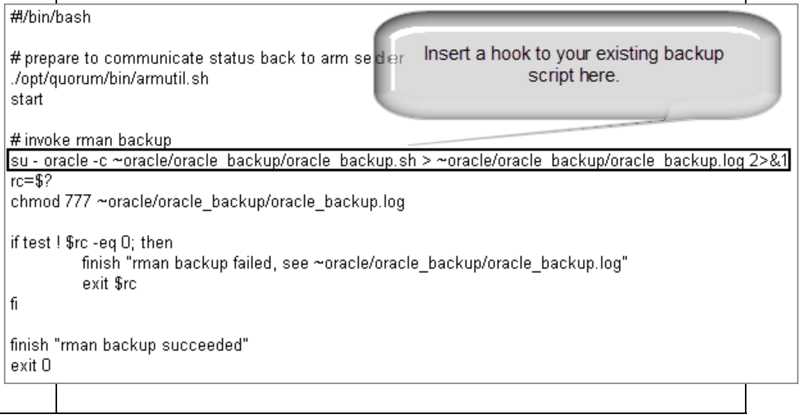
If you do not currently have a backup and restore strategy in place, involve an experienced Linux Oracle Database Administrator before you deploy onQ. onQ is one component of your backup and restore strategy.

(Step 1) To install and modify example RMAN scripts:

This procedure works for Linux 6.2 RNs, though this procedure should also work on other os versions. Quorum’s example RMAN scripts use RMAN to back up and restore a single DB instance and uses onQ to activate the backup script. Modify these scripts as needed. The following example is a basic proof-of-concept.

1. Download Quorum's example scripts, then modify these scripts to fit your Oracle environment (RMAN version):

`pre_snap.sh`	Performs the database backup by calling `oracle_backup.sh`. There are many ways to trigger DB backup script: cron jobs, third-party scheduler, or application, for example; however, onQ Portal provides a way to trigger this `pre_snap.sh` script before it backs up the protected volumes (see Step 5). This script can be modified to simply call an existing backup script that you're currently using in your environment:



```
#!/bin/bash

# prepare to communicate status back to arm se der
./opt/quorum/bin/armutil.sh
start

# invoke rman backup
su - oracle -c ~oracle/oracle_backup/oracle_backup.sh > ~oracle/oracle_backup/oracle_backup.log 2>&1
rc=$?
chmod 777 ~oracle/oracle_backup/oracle_backup.log

if test ! $rc -eq 0; then
            finish "rman backup failed, see ~oracle/oracle_backup/oracle_backup.log"
            exit $rc
fi

finish "rman backup succeeded"
exit 0
```

Insert a hook to your existing backup script here.

oracle_backup.sh	Coordinates rman backup of the Oracle database.The onQ Service runs this script before the Quorum backup process.
	Modify this script to specify the details of your Oracle installation:
	ORACLE_BASE=**/opt/oracle**
	ORACLE_HOME=**$ORACLE_BASE/product/11.2.0/db_1**
	Change the parameters for your database:
	BACKUP_BASE=**/backup01**
	BACKUP_AREA=**${BACKUP_BASE}/rdbms/physical/orcl**
	BACKUP_LOG_DIR=**~/oracle_backup**
	Modify for your Oracle SID:
	db=**orcl**
	This script can be replaced with an existing database backup script that you’re currently using in your environment.

oracle_restore.sh	Coordinates rman restore/recovery of the Oracle database. Use this script to restore and recover the Oracle database if automated crash recovery fails.
	Modify this script to specify the details of your Oracle installation:
	ORACLE_BASE=**/opt/oracle**
	ORACLE_HOME=**$ORACLE_BASE/product/11.2.0/db_1**
	Change the parameters for your database:
	BACKUP_BASE=**/backup01**
	BACKUP_AREA=**${BACKUP_BASE}/rdbms/physical/orcl**
	BACKUP_LOG_DIR=**~/oracle_backup**
	Modify for your Oracle SID:
	db=**orcl**
	This script can be replaced with an existing database backup script that you're currently using in your environment. This script should be available in advance of your need to recover: as a best practice, always test a recovery before the need arises.

armutil.sh armSender vmmonCtl	Communicates pre_snap.sh execution status to onQ, and depends on armSender and vmmonCtl executables in x64 or i386 folder.

2. Log on to the PN as oracle user (for example, **su - oracle**) and create a /home/oracle/oracle_backup directory.
3. Now that you've modified oracle_backup.sh and oracle_restore.sh, copy them to /home/oracle/oracle_backup on the PN.
4. As root user, copy armutil.sh and armSender and vmmonCtl from x64 or i386 folder, depending on the PN's architecture, to /opt/quorum/bin on the Linux PN that's running the Oracle database.

The armSender and vmmonCtl are tools to communicate status to the onQ Manager.

5. As root user, copy pre_snap.sh to /opt/quorum/bin/ on the PN, then activate this script on the onQ Portal.
   - a. Log on to the HA's onQ Portal.
   - b. From the **PROTECTION CONFIG** tab, select the PN that's running the Oracle 11g database, then **MODIFY** > **ADVANCED**.
   - c. Enable the pre snapshot script on that PN by selecting the **Execute Pre Snapshot script?: Yes** radio button.

That's it! Now you're ready to test the backup process.

(Step 2) To back up the Oracle database:

This procedure works for Linux 6.2 RNs, though this procedure should also work on other os versions.

1. Load some known data into the Oracle database (for example in ORCL catalog).
2. Initiate a backup, or wait for a scheduled backup, of the protected node.

   The PN's Event Log displays the following messages as onQ builds the RN. These messages also appear in oracle_backup.log on the PN:

   - Pre-snapshot command returned: rman backup succeeded (as coded in pre_snap.sh), if rman backup passes. For example:

   ```
   RHEL62x64-19-87: system: 2014-12-30 13:34:19: Pre-
   snapshot command returned: rman backup succeeded
   ```

   - Pre-snapshot command returned: rman backup failed (as coded in pre_snap.sh), if rman backup fails. For example:

   ```
   RHEL62x64-19-87: system: 2014-12-30 13:11:37: Pre-
   snapshot command returned: rman backup failed, see
   ~oracle/oracle_backup/oracle_backup.log
   ```

   If the RMAN backup fails, consult Oracle's RMAN documentation to fix the problem. The RMAN backup must succeed before you proceed with the restore.

If the backup succeeded, you're ready to test the restore process.

(Step 3) To restore the Oracle database:

This procedure works for Linux 6.2 RNs, though this procedure should also work on other os versions.

1. Start the Recovery Node in test mode, after the RN build completes.

   After the RN boots, the Oracle database should perform crash recovery automatically. The database either opens successfully or it doesn't:

   - (Case A) The database opens successfully and is ready for connection with no need for recovery, as shown in the following output; therefore, skip to Step 4.

```
[root@RHEL62x64-19-87 oracle_backup]# su - oracle
[oracle@RHEL62x64-19-87 ~]$ sqlplus / as sysdba
SQL*Plus: Release 11.2.0.1.0 Production on Tue Dec
23 09:22:06 2014
Copyright (c) 1982, 2009, Oracle.  All rights
reserved.

Connected to an idle instance.
SQL> startup;
ORACLE instance started.

Total System Global Area 1603411968 bytes
Fixed Size                  2213776 bytes
Variable Size            1124075632 bytes
Database Buffers          469762048 bytes
Redo Buffers                7360512 bytes
Database mounted.
Database opened.
SQL> connect SCOTT/<password>
Connected.
SQL> select count(*) from qa_test;
   COUNT(*)
   ----------
   27472
```

   - (Case B) The Oracle database does not open successfully, as shown in the following output. You need to perform the recovery procedure; therefore, proceed to the next step:

```
[root@RHEL62x64-19-87 oracle_backup]# su - oracle
[oracle@RHEL62x64-19-87 ~]$ sqlplus / as sysdba
SQL*Plus: Release 11.2.0.1.0 Production on Tue Dec
23 09:22:06 2014
Copyright (c) 1982, 2009, Oracle.  All rights
reserved.

Connected to an idle instance.
SQL> startup;
ORACLE instance started.

Total System Global Area 1603411968 bytes
Fixed Size                  2213776 bytes
Variable Size            1124075632 bytes
Database Buffers          469762048 bytes
Redo Buffers                7360512 bytes
Database mounted.
ORA-03113: en-of-life on communication channel
Process ID: 2235
Session ID: 1 Serial number:
```

2. On the RN, run the restore/recovery script to restore the Oracle database onto the RN:

```
# cd /home/oracle/oracle_backup
# ./oracle_restore.sh
```

Optionally, you can run the commands manually as shown in the following example output:

Invoke the restore/recovery script:

```
[oracle@RHEL62x64-19-87 ~]$ cd
/home/oracle/oracle_backup
[oracle@RHEL62x64-19-87 oracle_backup]$
./oracle_restore.sh
Recovery Manager: Release 11.2.0.1.0 - Production on
Tue Dec 23 09:32:15 2014

Copyright (c) 1982, 2009, Oracle and/or its
affiliates.  All rights reserved.

RMAN>         set echo on;
2>         connect target *;
3>         shutdown immediate;
4>         startup mount;
5>         restore database;
6>         shutdown immediate;
7>         startup mount;
8>         recover database;
9>         alter database open;
10>         exit;
echo set on

connected to target database: ORCL (not mounted)

using target database control file instead of
recovery catalog
Oracle instance shut down

connected to target database (not started)
Oracle instance started
database mounted

Total System Global Area    1603411968 bytes
Fixed Size                     2213776 bytes
Variable Size               1124075632 bytes
Database Buffers             469762048 bytes
Redo Buffers                   7360512 bytes
...
```

Restore/recovery begins and completes:

```
Starting restore at 23-DEC-14
allocated channel: ORA_DISK_1
...
restore from backup set
...
channel ORA_DISK_1: restore complete, elapsed time:
00:02:45

Finished restore at 23-DEC-14
database dismounted
Oracle instance shut down

connected to target database (not started)
Oracle instance started
database mounted

Total System Global Area    1603411968 bytes
Fixed Size                     2213776 bytes
Variable Size               1124075632 bytes
Database Buffers             469762048 bytes
Redo Buffers                   7360512 bytes
Starting recover at 23-DEC-14
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=18 device type=DISK

starting media recovery
media recovery complete, elapsed time: 00:00:03
Finished recover at 23-DEC-14
database opened
Recovery Manager complete.
```

3. Verify that the RN's Oracle database is up and running and in a usable state, and that it shows the expected data:

```
[oracle@RHEL62x64-19-87 oracle_backup]$ sqlplus /
as sysdba

SQL*Plus: Release 11.2.0.1.0 Production on Tue Dec
23 09:44:55 2014
Copyright (c) 1982, 2009, Oracle.  All rights
reserved.

Connected to:
Oracle Database 11g Enterprise Edition Release
11.2.0.1.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real
Application Testing options

SQL> connect SCOTT/<password> ' Able to connect to
DB after restore and recovery
Connected.
SQL> select count(*) from qa_test;
COUNT(*)
--------
   27472

SQL>EXIT;
```

4. Start the Recovery Node in production mode; when prompted, do not remove the RN.

Related Topics

Run custom backup scripts

Back up and restore Oracle 10g+ database on Windows

11.14 Back up and restore Oracle 10g+ database on Windows

The following procedures walks you through how to back up and restore an Oracle 10g+ database on a Windows Recovery Node. These procedures assume that you are knowledgeable and comfortable with Oracle databases.

Restoring and recovering an Oracle database, after you have booted the recovery node (RN), is a unique process from that of other databases. These procedures cover the prerequisites for hot backups with Volume Shadow Copy, and the required tools developed by Quorum to recover and open your Oracle Database on your recovery node.

These procedures outline the steps to recover an Oracle database with `ARCHIVELOG` mode enabled and the Oracle VSS Writer service installed. Hot backups are not possible with an Oracle database using `NOARCHIVELOG` mode. Databases using `NOARCHIVELOG` mode must be put in a consistent (shutdown) state in order to perform a backup.

Recovery, maintenance and troubleshooting of Oracle databases on the protected node (PN) will not be covered in these procedures.

These procedures might not work with your specific configuration; as such, discuss your configuration with Quorum Support before you perform this procedure.

(Step 1) To prepare your environment:

1. Verify that your RN is running:
   - Windows 2003 or greater
   - Oracle Database 10g or greater
2. Ensure that you have your archive logs stored on a separate volume from your database (DBF) files.

   Oracle requires that you put archive logs on a separate volume when performing backups with the Oracle VSS Writer service.

   Quorum cannot recommend an architecture that violates Oracle's specifications. However, it should be noted that Quorum did not observe any adverse effects when putting the database and archive logs on the same volume while performing VSS backups and restores.

3. From the onQ Portal’s **Protection Config** tab, verify that you have the following volumes protected.
   - The volume that contains your database files.
   - The volume that contains the archive logs.

4. For the protected node on which you want to perform hot backups and for every Oracle database instance, install the Oracle VSS Writer service (`service.msc`).

   The Oracle VSS Writer service is installed by default with Oracle Database 11g. Oracle Database 10g releases require a manual installation of the Oracle VSS Writer service. The installation instructions for the Oracle VSS Writer service can be found here.

5. Configure the Oracle services:

   a. Make sure Oracle is in `ARCHIVELOG` mode.

   b. Configure **Oracle VSS Writer** service with the `SYSDBA` user, mode `Automatic`; then, test that the user account has `SYSDBA` set correctly:

   ```
   > sqlplus user_account as SYSDBA
   ```

   For example:

   Where `sysadm_amy` is the *user_account*.

   ```
   > sqlplus sysadm_amy as SYSDBA
   ```

   c. Configure the **Volume Shadow Copy Service** with `Local Service` account, mode `Automatic`.

   d. Configure the **Microsoft Software Shadow Copy Provider** service with `Local Service` account, mode `Automatic`.

(Step 2) To back up the Oracle database:

Perform the following procedure on the PN and for each database that you want to restore.

1. Verify that the Oracle VSS Writer service is `running`.

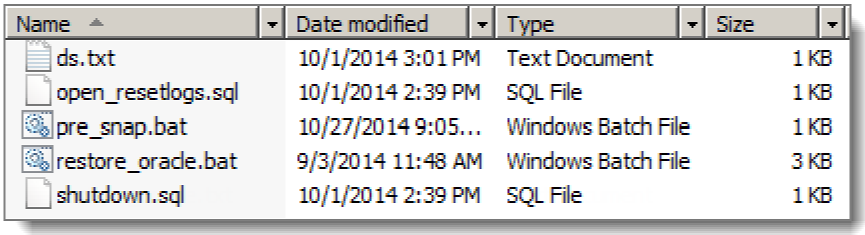
   ```
   > oravssw /q /status
   OracleVssWriterORCL - The service is running.
   ```

2. On the PN, verify that the VSS writers are `Stable`.

```
> vssadmin list writers
...
Writer name: 'Task Scheduler Writer'...
   State: [1] Stable
   Last error: No error
Writer name: 'VSS Metadata Store Writer'...
   State: [1] Stable
   Last error: No error
Writer name: 'Performance Counters Writer'...
   State: [1] Stable
   Last error: No error
Writer name: 'Oracle VSS Writer - ORCL'...
   State: [1] Stable
   Last error: No error
Writer name: 'System Writer'...
   State: [1] Stable
   Last error: No error
Writer name: 'ASR Writer'...
   State: [1] Stable
   Last error: No error
Writer name: 'Registry Writer'...
   State: [1] Stable
   Last error: No error
Writer name: 'COM+ REGDB Writer'...
   State: [1] Stable
   Last error: No error
Writer name: 'Shadow Copy Optimization Writer'...
   State: [1] Stable
   Last error: No error
Writer name: 'WMI Writer'...
   State: [1] Stable
   Last error: No error
```

3. On the PN, unzip the Quorum Oracle database recovery scripts in the `C:\Program Files\Quorum\usr` folder.

4. Modify the `restore_oracle.bat` batch file:



Name	Date modified	Type	Size
ds.txt	10/1/2014 3:01 PM	Text Document	1 KB
open_resetlogs.sql	10/1/2014 2:39 PM	SQL File	1 KB
pre_snap.bat	10/27/2014 9:05...	Windows Batch File	1 KB
restore_oracle.bat	9/3/2014 11:48 AM	Windows Batch File	3 KB
shutdown.sql	10/1/2014 2:39 PM	SQL File	1 KB

   a. Make a backup copy of the `restore_oracle.bat` batch file.

   b. Change the placeholder database names to match your Oracle database names. Each instance should be separated by a single space and encapsulated by parenthesis.

```
> set DB_INSTANCES=(database_instance_name)
```

   For example:

   Where there are three database instances: `orcl`, `orcl1`, and `orcl2`:

```
> set DB_INSTANCES=(orcl oracl1 oracl2)
```

   c. Save your changes.

5. Initiate a backup of the PN, or wait for a scheduled backup to complete.

6. Repeat Step 2: Verify that the VSS writers are `Stable`.

7. Verify that the backup completed successfully. Go to Monitor backups.

8. Check the PN's Event Log for VSS-related errors. If there are errors, resolve them. For troubleshooting information, see the appropriate return code in A0801.

(Step 3) To restore the Oracle database:

After the RN boots, you can now begin the Oracle Database recovery process. This process can be performed with an RN booted in test mode or production mode. Perform the following procedure on the RN and for each database instance that you want to restore. This procedure includes two ways to restore your database(s). Begin with the recommended solution.

(Recommended) Using restore_oracle.bat

This procedure uses Quorum’s `restore_oracle.bat` scripts. This solution is recommended.

1. With the RN, in test or production mode, navigate to the `C:\Program Files\Quorum\usr` folder, then run the `restore_oracle.bat` file completely.

   You will be prompted for your database password twice for each database instance: once for a shutdown command and once for an open **`resetlogs`** command.

2. Verify that your database(s) opens without any errors.
   - If the database(s) opens without error, you’ve successfully restored your database(s). You’re done!
   - If the database(s) fails to open successfully, the cause is the result of known bugs in Oracle’s VSS Writer. Perform the troubleshooting procedure outlined in (Step 4, if necessary) To fix an incomplete database recovery:.

Using “manual” process

This procedure uses a manual process to restore your database(s). This solution is not automated as is the case with using Quorum’s `restore_oracle.bat` scripts, which executes the same commands in the following manual process.

1. Shut down the database that you want to restore.

   ```
   > set ORACLE_SID=database_instance_name
   > sqlplus SYS as SYSDBA
   SQL> SHUTDOWN IMMEDIATE;
   SQL> EXIT;
   ```

   For example:

   Where `orcl` is the *database_instance_name* or Oracle System ID (SID).

   ```
   > set ORACLE_SID=orcl
   > sqlplus SYS as SYSDBA
   SQL> SHUTDOWN IMMEDIATE;
   SQL> EXIT;
   ```

2. Restore the Oracle VSS Writer's metadata and generate the required archive log, if any.

   ```
   > qvss.exe restore
   ```

3. Open the database for service and reset the redo logs.

   ```
   > sqlplus SYS as SYSDBA
   SQL> ALTER DATABASE open resetlogs;
   SQL> EXIT;
   ```

4. Compare the PN's and RN's row counts. They should match, if no changes were made after the backup.

   ```
   > sqlplus system@database_instance_name
   SQL> select count (*) from table_name;
   ```

   For example:

   Where `testtable` is the *table_name* and where `orcl` is the *database_instance_name* or Oracle System ID (SID).

   ```
   > sqlplus system@orcl
   SQL> select count (*) from testtable;
   ```

5. Check the PN's Event Log for VSS-related errors. If there are errors, resolve them. For troubleshooting information, see the appropriate return code in A0801.

6. Verify that your database(s) opens without any errors.
   - If the database(s) opens without error, you've successfully restored your database(s). You're done!
   - If the database(s) fails to open successfully, the cause is the result of known bugs in Oracle's VSS Writer. Perform the troubleshooting procedure outlined in (Step 4, if necessary) To fix an incomplete database recovery:.

(Step 4, if necessary) To fix an incomplete database recovery:

If you attempted to restore an Oracle database either manually or using `restore_oracle.bat` and your database(s) fails to open, you have an incomplete database recovery. This procedure includes two ways to fix an incomplete database recovery. Begin with the recommended solution.

(Recommended) Using "recover database until cancel" method

This solution uses Oracle's *recover database until cancel* recovery method to fix an incomplete database recovery. This procedure is the easiest way to fix such a problem, and is recommended before attempting any other incomplete database recovery method.

1. Restart a *fresh* RN, in test or production mode. If you're using `restore_oracle.bat`, execute that file now, but choose not to start the databases at the end of batch file.
2. Set the `ORACLE_SID` to the database SID. Where the SID is `ORCL`:

   ```
   C:\> SET ORACLE_SID=ORCL
   ```

3. Start the sqlplus shell:

   ```
   C:\> SQLPLUS / AS SYSDBA
   ```

4. Perform the following Oracle DB incomplete recovery procedure, which uses the *recover database until cancel* method:

   a. Execute the *recover database until cancel* method.

   b. Verify that the suggested log file is available or specify an available archived log file to be restored, then press **Enter**.

If the suggested log file is unavailable or there are no archive log files, type **CANCEL**.

```
SQL> RECOVER DATABASE UNTIL CANCEL USING BACKUP
CONTROLFILE;
ORA-00279: change 5619127 generated at 11/18/2014
13:03:07 needed for thread 1
ORA-00289: suggestion :
E:\LOGS\ARCH_863902564_1_81.ARC
ORA-00280: change 5619127 for thread 1 is in se-
quence #81


Specify log: {<RET>=suggested | filename | AUTO |
CANCEL}


++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++
Specify log: {<RET>=suggested | filename | AUTO |
CANCEL}
CANCEL
Media recovery cancelled.
SQL>
```

5. Open the database with resetlogs:

```
SQL> alter database open resetlogs;
```

6. Verify that the database opens successfully. The database has a new change number in the database view.

```
SQL> SELECT CURRENT_SCN FROM V$DATABASE;
```

If the database fails to open successfully, the cause is a known bug (race condition) in Oracle's VSS Writer. Perform the procedure outlined in Using point-in-time recovery method.

Using point-in-time recovery method

This solution uses Oracle's *point-in-time* recovery method to restore the database to the target time (or SCN) for recovery. This procedure is guaranteed to succeed, but is more complicated; for this reason, use it as a last resort. Perform the following procedure for each database instance.

1. Restart a *fresh* RN, in test or production mode. If you're using `restore_oracle.bat`, execute that file now, but choose not to start the databases at the end of batch file.
2. Set the `ORACLE_SID` to the database SID. Where the SID is `ORCL`:

   ```
   C:\> SET ORACLE_SID=ORCL
   ```

3. Start the sqlplus shell:

   ```
   C:\> SQLPLUS / AS SYSDBA
   ```

4. Perform the following Oracle DB incomplete recovery procedure, which uses the *point-in-time* recovery method*.*
   a. Determine the missing last change number and record the last `NEXT_CHANGE#` value:

   ```
   SQL> SELECT MAX(NEXT_CHANGE#) FROM V$LOG_HISTORY;
   ```

   Let's assume the last change value is `118009`.

   b. Recover to the last change number in the last archived redo log on the RN. This value is the last `NEXT_CHANGE#` value (see Step 4) minus 1. Where the last change value is `118009`, therefore, the value is `118008` (118009 -1).

   ```
   SQL> RECOVER DATABASE UNTIL CHANGE 118008 USING
   BACKUP CONTROLFILE;
   ```

5. Open the database with resetlogs:

   ```
   SQL> alter database open resetlogs;
   ```

6. Verify that the database opens successfully. The database has a new change number in database view.

   ```
   SQL> SELECT CURRENT_SCN FROM V$DATABASE;
   ```

   If your database still fails to open successfully, contact Quorum Support.

Related Topics

Run custom backup scripts

Back up and restore Oracle 11g database on Linux

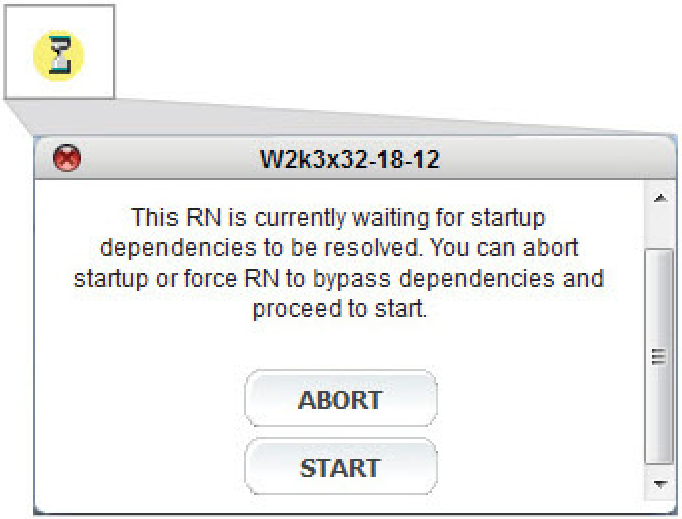
11.15 Cancel or override RN startup process

During the startup process for an RN configured with dependencies, onQ might be waiting for a dependency to become available or for the delay period.

If you are waiting for a dependent RN/server that has no chance of coming online and/or you never specified a timeout, you might need to force or cancel the startup process.

To cancel or override the process:

1. Log on to the onQ Appliance's onQ Portal.
2. Go to **DASHBOARD** tab > **RECOVERY NODES** page.
3. Unlock the page.
4. Click the button in the **Power State** column, then click:
   - **ABORT** - to cancel the startup process. Fix the dependency problem, then restart.
   - **START** - to override the dependencies and start the RN. Fix the dependency problem.



W2k3x32-18-12

This RN is currently waiting for startup dependencies to be resolved. You can abort startup or force RN to bypass dependencies and proceed to start.

11.16 Launch recovery node’s console

Use this procedure if you’d like to test a recovery node. The onQ Portal launches the recommended console—VNC console (aka *noVNC*), unless your browser cannot support websockets and the canvas element (see “User Interface Limitations” in onQ Release Notes); otherwise the onQ Portal launches the Java-based browser.

If you see unidentifiable characters when you use your keyboard, your browser version does not handle key events in the way that VNC console expects, although your browser does support websockets and the canvas element; in this case, exit the VNC console, then hold down the Ctrl key and select the **Console** icon to launch the Java-based console.

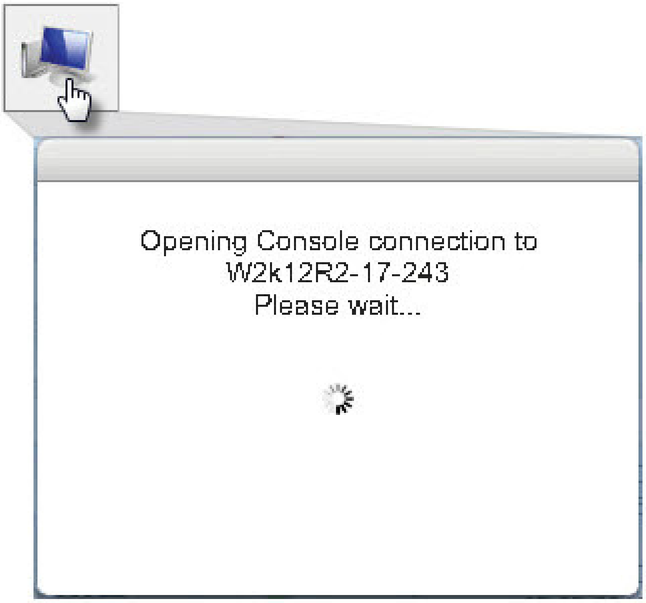
To launch a recovery node’s console:

1. If the RN is an HA recovery node, start it in test mode.

Note: You can use the console in either test mode or production mode.

2. Go to **DASHBOARD** tab > **RECOVERY NODES** page.

3. Click on the **Console** icon. The console launches as a HTML5 web-based VNC console or a Java-based console, depending on your browser version.



Opening Console connection to
W2k12R2-17-243
Please wait...

> If your browser supports websockets and the canvas element, a VNC console opens in a new browser window or tab; however, if you invoke the console in a browser that does not offer this support, the browser reverts to the Java-based console.

- **Web-based VNC Console**. Add an exception to the pop-up blocker as most browsers will block this new window by default.
- **Java Console**. Choose **Open with Java Web Start Launcher** to open the.`jnlp` file. If prompted, click **OK** to accept the security warning. If your desktop cannot recognize this file, then you don't have JRE (Java Runtime Environment) installed. Download the software from the Java site.

> **Note:** If the onQ portal returned the following message, the port required for the VNC session is not available from the hypervisor: `The VNC session is not currently available. Please try again`. During RN power, the port hasn't been assigned yet. During RN power down, the port has already been closed. Simply wait a few seconds, then try again.

4. From the **onQ RN Console**, click **Send Ctrl-Alt-Delete** in the main menu.

   Now you can log on using the host’s credentials.

Related Topics

Test Mode
RN Console Mouse Problems
Start recovery nodes on HA

11.17 Test Mode

When you start a recovery node, you have an opportunity to run the recovery node in test mode. Quorum recommends that you access the recovery node in test mode through the integrated console.

Running a recovery node in test mode means that it runs in a limited private network environment isolated from your production facilities.

The reason for running in test mode is to ensure, without risk to ongoing operations, that the recovery node is intact and will run in the event of a disaster. Keep in mind that this capability is in addition to automatic testing.

The onQ Appliance itself occasionally and briefly runs a recovery node in test mode as part of an internal quality-assurance process. However, best practice is to check your recovery nodes periodically, just as you would ordinary backups.

While an RN is running in test mode the corresponding PN also continues to run although the backup process is suspended. Backups (and subsequent rebuilds of the RN) resume according to current settings when the test mode has finished.

Related Topics

Configure automatic testing of RNs
Start node protection

11.18 Configure automatic testing of RNs

onQ can automatically test (also called *Self Test*) Ready-to-Build Recovery Nodes (RNs) on a predefined schedule after each RN build and for all the RNs that you add to the self-test list.

Self Test verifies connectivity inside an agent-based or agent-less RN (via TCP connection), testing that onQ can connect to the RN using the pre-configured IP address and, in the case of agent-based RNs, that the Quorum service is running on the RN.

Self Test works on both the HA and the DR Appliance and even when PNs are on different subnets. Upon completion, onQ sends the test results to all alert subscribers.

onQ can automatically test *individual* nodes, but not a *group* of nodes.

To configure an RN test for an *individual* recovery node:

1. From the HA or the DR Appliance, go to the **SELF TEST** tab > **ADD INDIVIDUAL** button.
2. In the RN Name drop-down list, choose the recovery node from the list.

   Build-on-Demand RNs can appear in this list, if the RN was formerly an Ready-to-Run RN. A self test of an outdated RN is possible, but the results will not reflect the RN’s resiliancy or vulnerability in the event of a disaster.
3. In the Test Schedule drop-down list, choose when you want the test to run, then **SAVE**.

   After Update – Choose this option if you want the test to run after each incremental update. This option is ideal when your backups are scheduled once every 24 hours.

   Hour – If you have multiple incremental backups in a day, choose this option to avoid getting multiple confirmations after each test. More than one test in a day does not provide any additional benefits.

Related Topics

Test Mode

(Agent-based PNs) Methods of Performing Incremental Backups

Initiate immediate backups

11.19 Suspend and resume RN tests

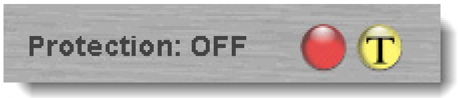
RN tests (aka *Self-Test*), when running, can reduce the memory pool and can interfere with RN testing. The onQ Portal enables you to suspend all RN tests that are currently running.

Suspending and resuming RN tests do not generate alert emails. Moreover, an alert email will not be generated on the next successful test after RN tests resume. However, an alert will be generated if an RN test failure occurs after RN tests resume.

To suspend all RN tests:

1. Do one of the following:
    - From the HA or the DR Appliance, go to the **SELF TEST** tab > **ADD INDIVIDUAL** button.
    - Go to **DASHBOARD** tab > **RECOVERY NODES** page, then unlock the page.
2. Click on the **Suspend Self Test** button, then **Suspend**.

    The Suspend icon appears in the page header to the right of the Protection On/Off display, and messages appear in the Self Test log:



`Suspend RN Self-Tests of ALL`	onQ instructs the scheduler to suspend all RN tests.
`Request to stop Self-Test for` <host>	Appears if an RN test is currently running.
`Self-Test stopped`	Appears when the scheduler successfully stops the RN test(s).

To restart all RN tests:

- From the HA or the DR Appliance, go to the **SELF TEST** tab > **ADD INDIVIDUAL** button.
- Go to **DASHBOARD** tab > **RECOVERY NODES** page, then

unlock the page.

3. Click on the **Resume Self Test** button, then **Resume**.

   The Self Test log indicates `Resume RN Self-Tests for ALL`.

11.20 Restore PNs Using QUARK

The following disaster recovery workflows prompt you to use Quorum Ultimate Automated Recovery Kit (QUARK):

- (Workflow) Fail over HA to DR Appliance
- (Workflow) Fail back DR to HA
- (Workflow) Fail over a PN to an RN
- (Workflow) Fail back an RN to a PN

QUARK is an easy-to-use wizard that walks you through two types of restores:

- **Bare Metal Restore (BMR)**. You have a server failure or site failure and you want to restore a Recovery PN from scratch.
- **Incremental/Reversion Restore**. You have a server failure and you want to restore to the latest snapshot, or you have a corruption problem and need to restore to a previous snapshot (aka *reversion*).

You can also restore PN data using two other methods: file level restore (FLR) and Windows Share Restore (WSR). These methods are commonly used in non-disaster recovery scenarios.

To learn more about BMR/QUARK support and limitations, go to:

- "Bare Metal Restore Limitations" in onQ Release Notes
- "Bare Metal Restore Support" in onQ Release Notes

(Step 1) To download the QUARK software:

QUARK supports two boot options:

- **USB**. This media is used for most installs. If for any reason QUARK cannot inject the necessary drivers, you can add drivers to this USB for use during the BMR without needing additional media.
- **ISO**. Burn this ISO to a CD-ROM or, in the case of virtualization, save this ISO to your network and point to it from your virtualization infrastructure.

  1. Log on to the onQ Portal.
  2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **SOFTWARE UPGRADES** page > **Check for Updates** button.

This step ensures that you have the most current version of QUARK for your onQ Appliance. However, if your disaster scenario is critical, skip this step so as not to add more complexity to your recovery in the event that your upgrade results in unusual complications.

3. Save the QUARK image. Later you will reconfigure the Recovery PN's BIOS to boot QUARK.
    a. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **DOWNLOADS**.
    b. Select the `Quark_BCV-<release>-<date>-<time>.iso`, click **Download**, then save the `.iso` file to your virtualization infrastructure, or burn it to a CD-ROM or USB flash drive.

Now you're ready to perform your BMR.

(Step 2) To restore data to your PN:

In this procedure, *Recovery PN* (also called *Recovery OS, BMR target*, *restore target*, or simply *target*) refers to the server to which you are restoring. This Recovery PN can be a physical or virtual machine.

If your Recovery PN is a virtual machine, QUARK requires a "shell" (and necessary disks and network cards) onto which QUARK can load its snapshot(s). You can retrieve this "shell" by building a new virtual machine from scratch, restoring to the original PN, using a snapshot of your virtual machine, or deploying a clone from a template. In any case, this virtual machine need not look like your Recovery PN. Simply reconfigure the machine's BIOS to boot QUARK, then QUARK will walk you through the BMR.

Note: Although QUARK attempts to inject the necessary drivers for your system, it's a best practice to have a copy of these drivers as part of your business continuity plan.

Your Recovery PN must have enough resources to accommodate the new data. To be safe, ensure that your Recovery PN has at least the same amount of disk space and memory as the failed PN.

Warning: Do Not Restart! In the event of a restore failure, QUARK provides you the opportunity to resume the restore (see Step 8 and Step 12). However, this capability will not be available if you:

- **Restart protection**. Therefore, do not stop, then start protection (aka restart) on the onQ.
- **Restart a BMR for a different PN from the same onQ**. Therefore, wait for the BMR to complete before beginning another from the same onQ.

1. Verify that your platform is supported. Go to “Support” in onQ Release Notes.
2. Configure Hardware RAID on the Recovery PN.

   If necessary, configure any hardware RAID controllers in the BIOS of the Recovery PN. For instructions, refer to the hardware manufacturer's documentation.
3. Launch the QUARK wizard:

   a. Configure the Recovery PN's BIOS to boot QUARK.

   b. Boot the Recovery PN to load the QUARK image.

   The **Start BMR** page appears.
4. From the **Start BMR** page, allow the QUARK wizard to check for basic network and disk controller drivers on which QUARK depends, then **Next**.

   If the QUARK wizard detects a missing driver, upload the missing network driver.

Note: To manually launch the **Add Drivers** utility, run the following command from the command prompt:

```
# QUARK_Wizard.exe AddDriver
```

5. (Optional) In the **Network Configuration** page, change the default network configuration, then **Next**:
   - If the wizard detects a DHCP server, the wizard displays the assigned default IP address and netmask.

- If DHCP is not enabled on the network, the wizard displays the assigned default Windows workgroup address.

a. Select a NIC from the **Interface** drop-down list.

b. Specify a *temporary* **IP address** for the restore target. DO NOT set the IP address to the PN's original IP address; doing so prevents onQ from communicating with the restore target. After onQ restores PN data, the restore target will automatically be set to the PN's original IP address. Select the **Set Static IP** check box to set the default IP address to a static IP.

The **Disk Cleanup / iSCSI Configure** page appears.

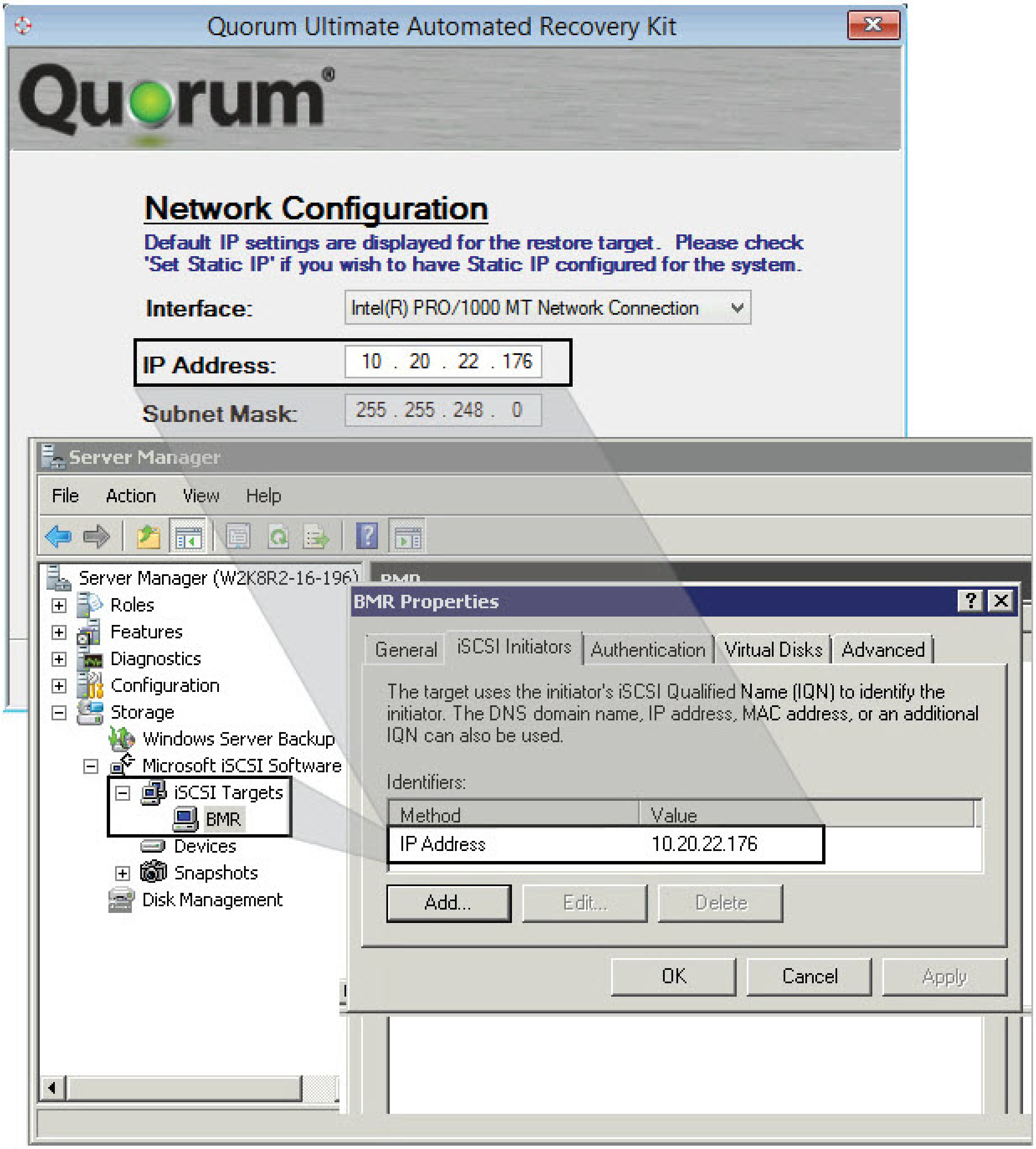
6. Do one of the following:

- **Reset all local disks**. Select this option if you intend to perform a BMR.

Note: Resetting the disks ensures that you do not write PN data on top of corrupted data. Reformatted and clean disks are ideal. However, if you’ve already created the disk partitions outside of QUARK using a disk partition tool, you can skip this task.

- **Skip disk reset**. Select this option if you intend to perform an Incremental/Reversion or your last restore interrupted prematurely.
- **Configure iSCSI disks**. Select this option if your Recovery PN has iSCSI disks. The **QUARK Disk Configuration** wizard launches. (1) Add QUARK (BMR target) to the iSCSI target’s initiator list, then (2) In **Disk Configuration** page, specify the

iSCSI target's IP address to attach the iSCSI devices to QUARK.



Quorum Ultimate Automated Recovery Kit

Network Configuration

Default IP settings are displayed for the restore target. Please check 'Set Static IP' if you wish to have Static IP configured for the system.

Interface: Intel(R) PRO/1000 MT Network Connection

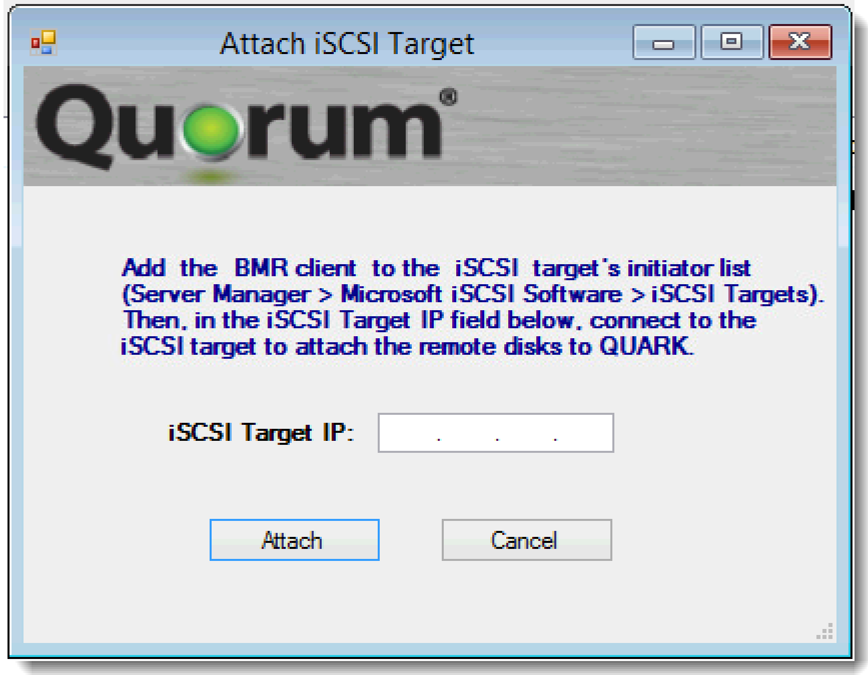
IP Address: 10 . 20 . 22 . 176

Subnet Mask: 255 . 255 . 248 . 0

The target uses the initiator's iSCSI Qualified Name (IQN) to identify the initiator. The DNS domain name, IP address, MAC address, or an additional IQN can also be used.

Identifiers:

Method	Value
IP Address	10.20.22.176



Add the BMR client to the iSCSI target's initiator list (Server Manager > Microsoft iSCSI Software > iSCSI Targets). Then, in the iSCSI Target IP field below, connect to the iSCSI target to attach the remote disks to QUARK.

iSCSI Target IP: . . .

The **Log on to onQ** page appears.

7. In the **Log on to onQ** page, type the IP Address and credentials of the onQ Appliance that manages the Recovery PN's snapshot to which you want to restore, then **Next**.

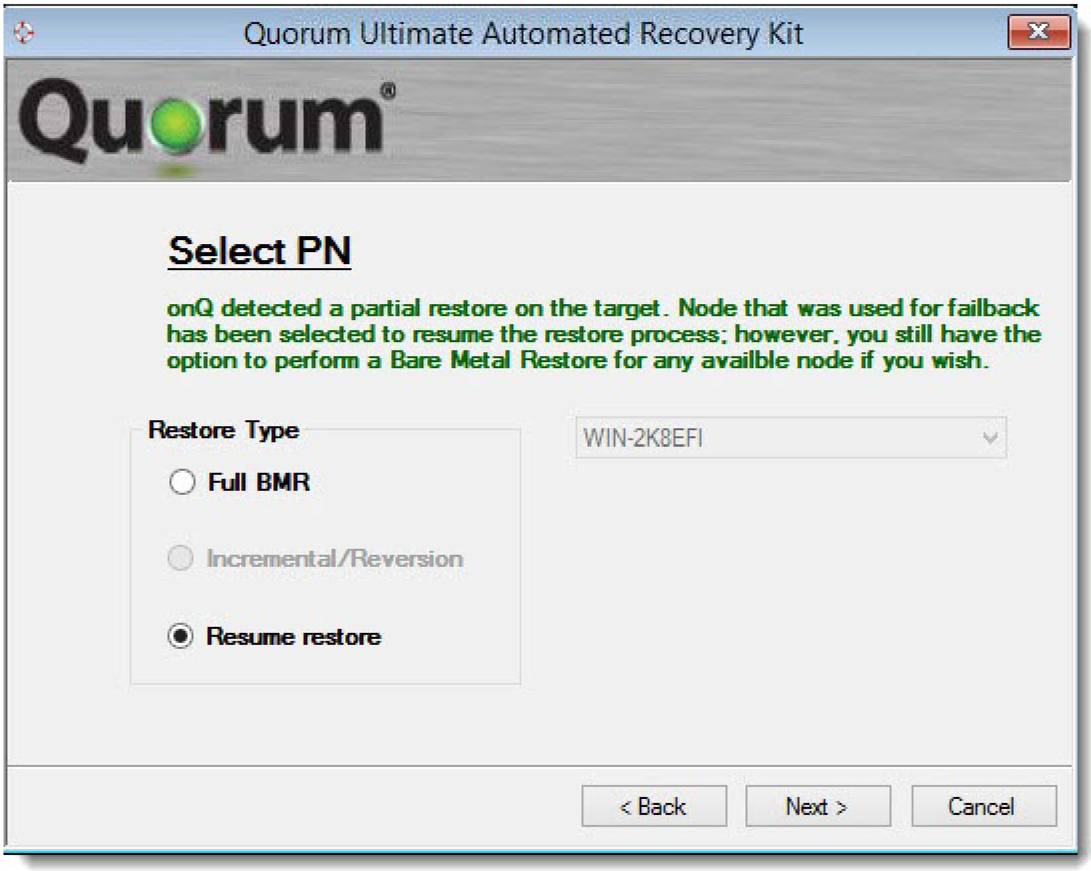
   The onQ Appliance analyzes the snapshots that belong to the Recovery PN, and determines the restore types (**Full BMR** or **Incremental**) that are available for this recovery, then displays the **Select PN** page.

   If this process fails, browse the list of error messages in (Step 4) To interpret QUARK Errors: to correct the problem.

8. In the **Select PN** page, select the restore type and the Recovery PN from the drop-down list of PNs that the onQ Appliance manages, then **Next**.
   - **Full BMR**. Restore a Recovery PN from scratch. If the onQ Appliance doesn't have the incremental backups that are needed to perform the Incremental/Reversion restore (that is, the PN is a new server and does not have any data on its disk), the wizard displays the Full BMR option only; otherwise, both options are available.
   - **Incremental/Reversion**. Use the **Incremental/Reversion** restore

type to: (1) Restore to the latest version; simply choose the latest snapshot, or (2) Revert to a previous version (also known as a *reversion*); simply select the snapshot that represents a point in time. This scenario is ideal when you know that the latest version is corrupt.

- **Resume restore**. Appears when onQ detects an incomplete restore (aka restore failure) on the target. An incomplete restore (see Step 12) may occur if a restore doesn't complete within 48 hours. Choose Resume restore to resume "beginning where QUARK left off." You also have the choice to start over.



Quorum Ultimate Automated Recovery Kit

Select PN

onQ detected a partial restore on the target. Node that was used for failback has been selected to resume the restore process; however, you still have the option to perform a Bare Metal Restore for any availble node if you wish.

Restore Type

○ Full BMR

○ Incremental/Reversion

● Resume restore

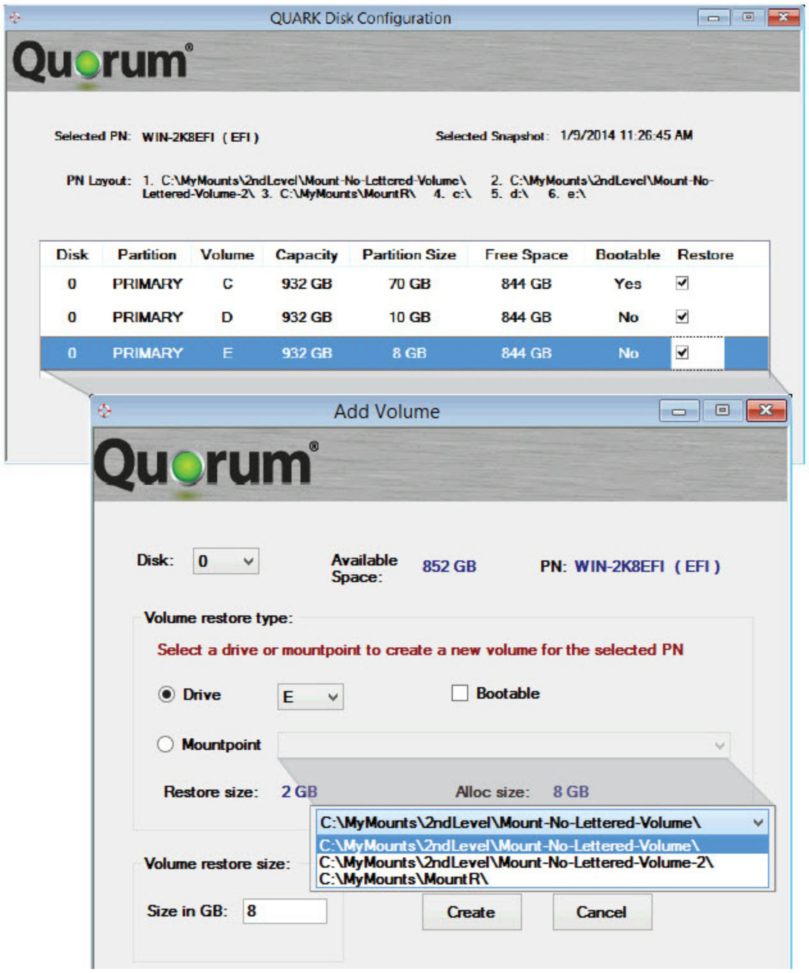
WIN-2K8EFI

9. In the **Select Snapshot** page, select the snapshot to which you want to restore the Recovery PN, then **Next**.
10. From the **Begin PN Restore** page, click **Next** to confirm your PN and snapshot selection. The **QUARK Disk Configuration** wizard launches.

11. Configure the Recovery PN with the same disk configuration as the original PN, then **Close**.

> **Note:** If a USB/CD-ROM takes a PN drive letter, QUARK automatically reassigns the USB/CD-ROM a different drive letter.

a. For every volume that appears in the PN Layout field, add a corresponding volume. The volume can be either a drive or a mountpoint. Optionally, you can change the **Volume restore size** of the drive or mountpoint; the default is the allocated size as shown in the onQ Portal.



Selected PN: WIN-2K8EFI (EFI)

Selected Snapshot: 1/9/2014 11:26:45 AM

PN Layout: 1. C:\MyMounts\2ndLevel\Mount-No-Lettered-Volume\ 2. C:\MyMounts\2ndLevel\Mount-No-Lettered-Volume-2\ 3. C:\MyMounts\MountR\ 4. c:\ 5. d:\ 6. e:\

Disk	Partition	Volume	Capacity	Partition Size	Free Space	Bootable	Restore
0	PRIMARY	C	932 GB	70 GB	844 GB	Yes	☑
0	PRIMARY	D	932 GB	10 GB	844 GB	No	☑
0	PRIMARY	E	932 GB	8 GB	844 GB	No	☑

Disk: 0

Available Space: 852 GB

PN: WIN-2K8EFI (EFI)

Volume restore type:

Select a drive or mountpoint to create a new volume for the selected PN

● Drive E

□ Bootable

○ Mountpoint

Restore size: 2 GB

Alloc size: 8 GB

C:\MyMounts\2ndLevel\Mount-No-Lettered-Volume\
C:\MyMounts\2ndLevel\Mount-No-Lettered-Volume\
C:\MyMounts\2ndLevel\Mount-No-Lettered-Volume-2\
C:\MyMounts\MountR\

Volume restore size:

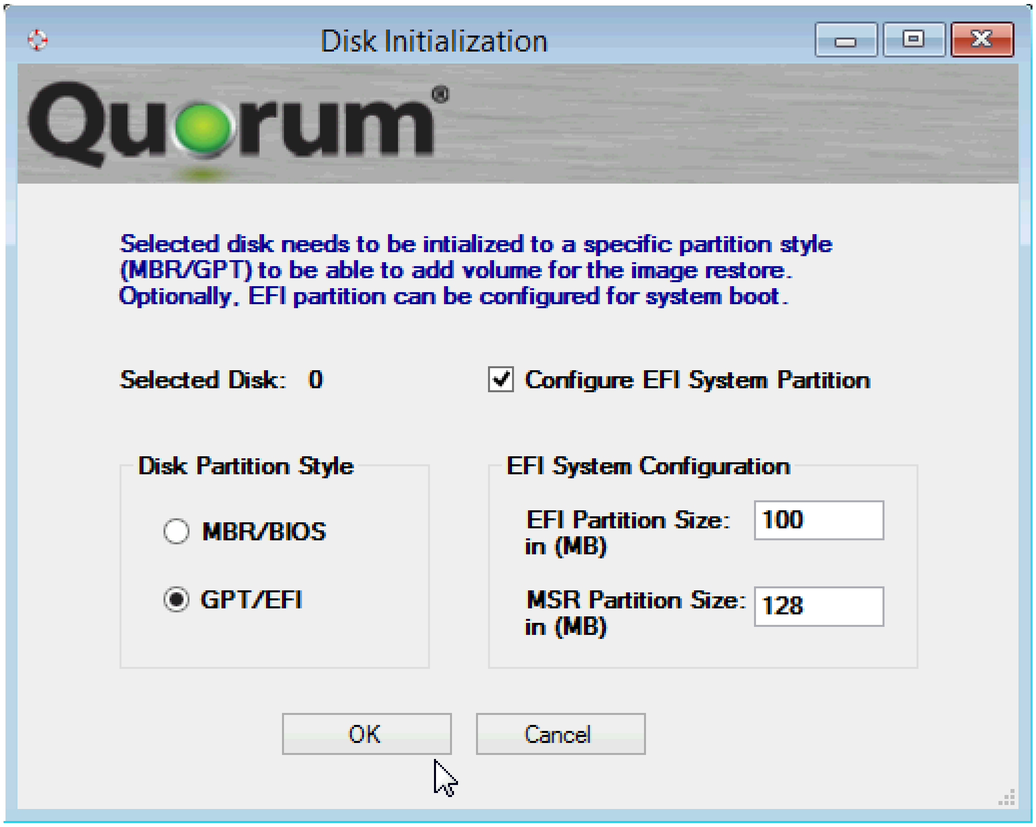
Size in GB: 8

b. If the drive is a boot drive, specify the partition style when the **QUARK Disk Configuration** wizard prompts you:

- If you want the PN to boot with BIOS, select **MBR/BIOS**.

- If want the PN to boot with UEFI, select **GPT/EFI**.

Optionally, change the partition size.



Selected disk needs to be intialized to a specific partition style (MBR/GPT) to be able to add volume for the image restore. Optionally, EFI partition can be configured for system boot.

Selected Disk: 0

☑ Configure EFI System Partition

Disk Partition Style

○ MBR/BIOS

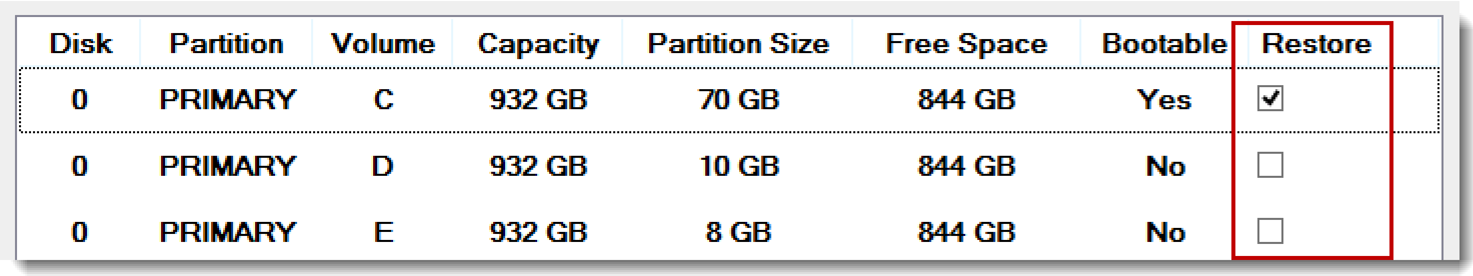
● GPT/EFI

EFI System Configuration

EFI Partition Size: in (MB) 100

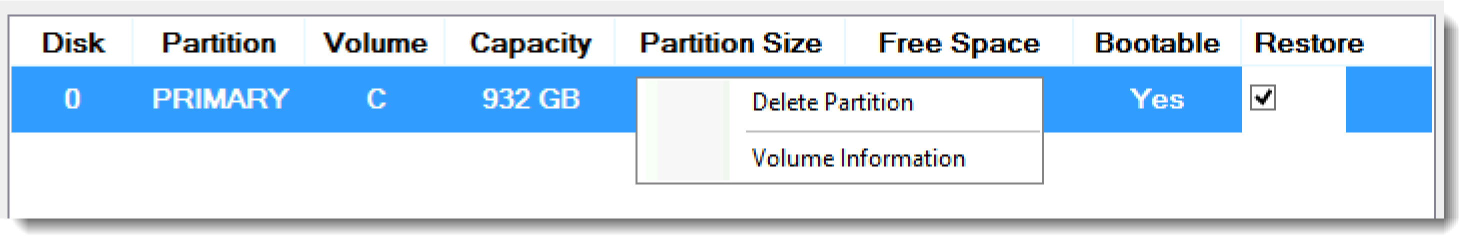
MSR Partition Size: in (MB) 128

c. Select the volumes that you want to restore. Typically you’ll want to select all the volumes; however, you might want to restore only the operating system so as to get the PN up and running quickly as demonstrated in the example below; you can always restore the remaining volumes later using QUARK, FLR, WSR, or a third party tool.



Disk	Partition	Volume	Capacity	Partition Size	Free Space	Bootable	Restore
0	PRIMARY	C	932 GB	70 GB	844 GB	Yes	☑
0	PRIMARY	D	932 GB	10 GB	844 GB	No	□
0	PRIMARY	E	932 GB	8 GB	844 GB	No	□

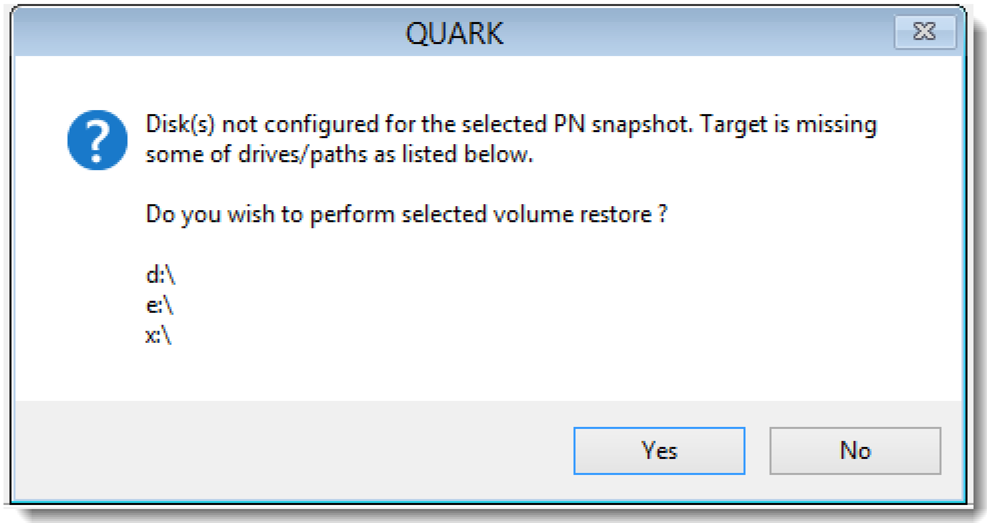
d. If you want to delete a volume or view volume information (for example, file system), right-click on the volume and **Delete Partition** and **Volume Information** respectively.



Disk	Partition	Volume	Capacity	Partition Size	Free Space	Bootable	Restore
0	PRIMARY	C	932 GB			Yes	☑

e. When the **Begin PN Restore** page appears, click **Next**.

If you receive the following error message, the volumes that you added do not match the PN layout. However, as outlined in Step c, you do not need to restore all the volumes.



Disk(s) not configured for the selected PN snapshot. Target is missing some of drives/paths as listed below.

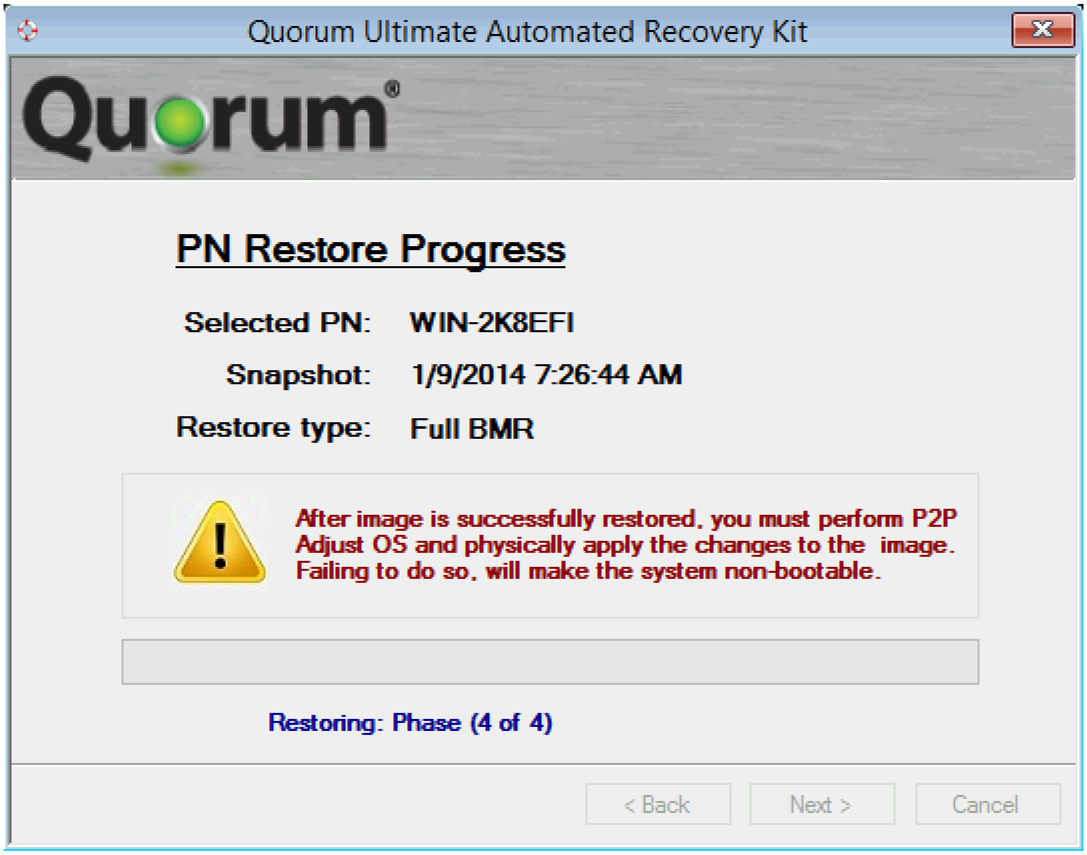
Do you wish to perform selected volume restore ?

d:\
e:\
x:\

f. Wait while the wizard formats the drives. This process can take several minutes.

> **Note:** If you accidently close the QUARK Disk Configuration wizard or you need to reconfigure your disks before you restore, you can launch the wizard from the command prompt:
>
> ```
> # QUARK_Wizard.exe showDiskConfig
> ```

The **PN Restore Progress** page appears.



Quorum Ultimate Automated Recovery Kit

PN Restore Progress

Selected PN: WIN-2K8EFI

Snapshot: 1/9/2014 7:26:44 AM

Restore type: Full BMR

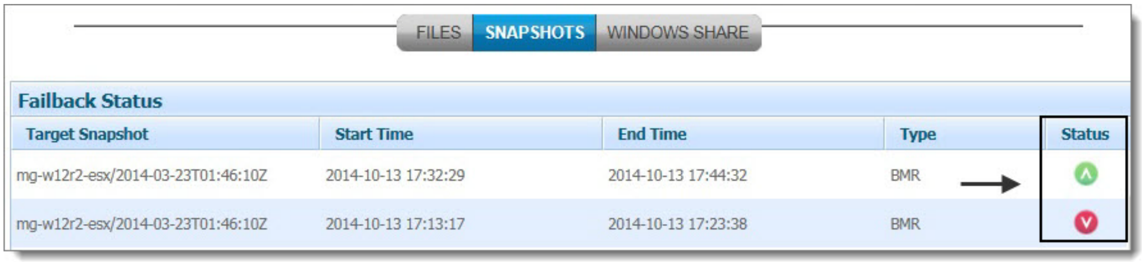
After image is successfully restored, you must perform P2P Adjust OS and physically apply the changes to the image. Failing to do so, will make the system non-bootable.

Restoring: Phase (4 of 4)

12. Wait for the onQ Appliance to restore the Recovery PN to the snapshot you selected.

    a. If the onQ Appliance detects a problem, the QUARK wizard aborts the BMR, then displays a status message. Browse the list of error messages in (Step 4) To interpret QUARK Errors: to correct the problem.

    b. If QUARK does not display any errors, verify that the restore completed successfully. Log on to the onQ Appliance's onQ Portal, then go to **RESTORE** > **SNAPSHOTS**. Locate the target snapshot that you chose. If the **Status** icon is red, hover-over the icon to display the status message.



Failback Status

Target Snapshot	Start Time	End Time	Type	Status
mg-w12r2-esx/2014-03-23T01:46:10Z	2014-10-13 17:32:29	2014-10-13 17:44:32	BMR	▲
mg-w12r2-esx/2014-03-23T01:46:10Z	2014-10-13 17:13:17	2014-10-13 17:23:38	BMR	▼

If the status message indicates `Incomplete: Unexpected Disconnect`, then you will need to launch QUARK and perform the restore again. When you select the PN from **Select PN** page, onQ notifies QUARK of the restore failure, then QUARK provides you the opportunity to resume the restore (see Step 8).

If the status message indicates `Completed Successfully` and if you attached iSCSI devices in Step 6, verify that the Microsoft iSCSI initiator assigned the correct drive letters for each iSCSI device. If not, change the drive letters: **Computer Management** > **Disk Management**.

Sometimes the restored PN can have incorrect drive letters for iSCSI devices if the target has an unexpected Microsoft iSCSI initiator version.

13. Verify that all disks are online. onQ cannot back up offline disks. If there's an offline disk, bring it online by using the OS's Disk Management interface. For more information, see the pertinent troubleshooting tip in BMR Problems.

14. If video reverts to 640x480 or 800x600 resolution, change the related video boot option. For more information, see the pertinent troubleshooting tip in BMR Problems.

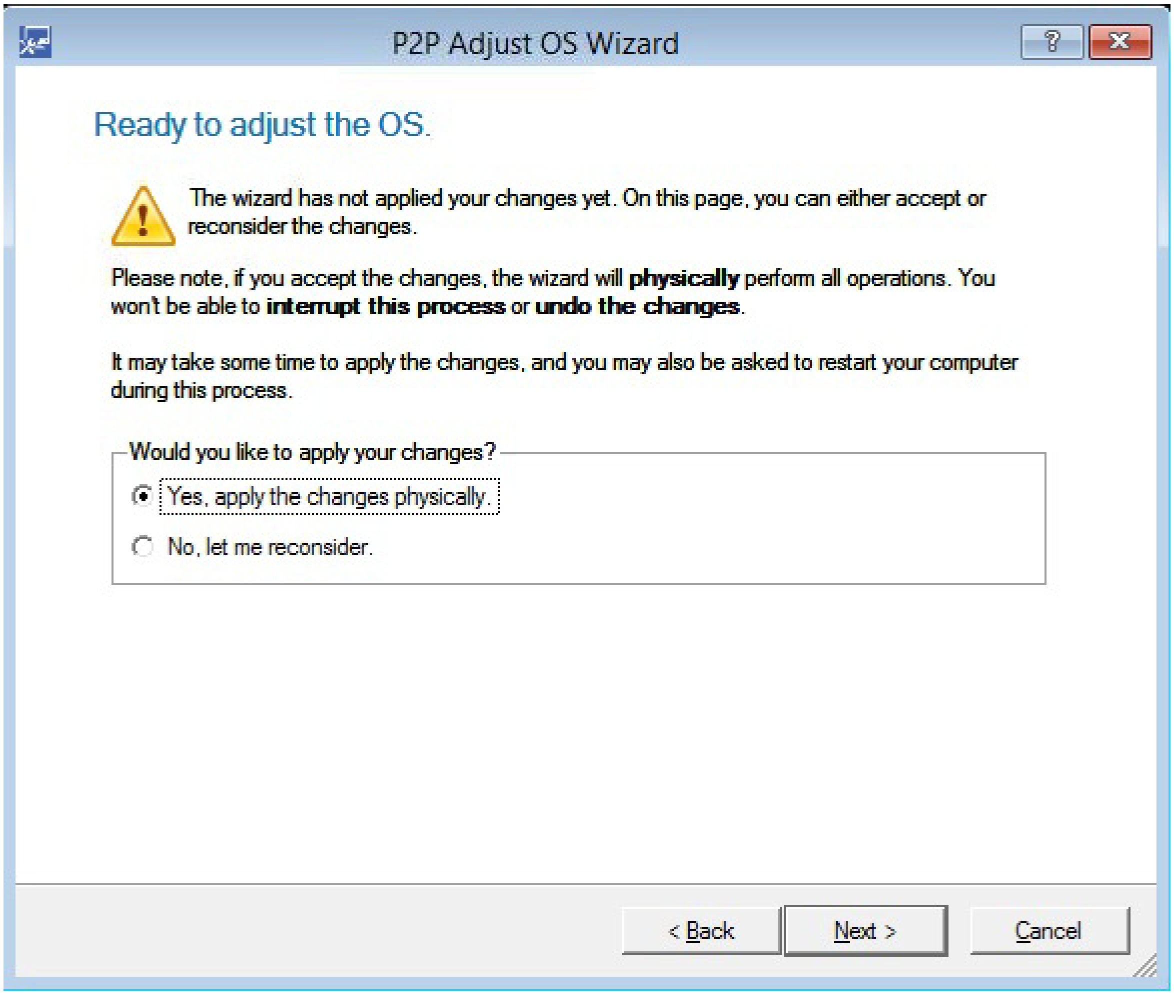
15. Do the following, after you verified that the restore completed successfully:

a. From the **P2P Adjust OS Wizard**, select the Recovery PN's operating system and, when prompted, choose **Adjust the OS to the new hardware automatically**, then **Next**.

If the Recovery PN's hardware is different from the image, the wizard needs to inject the necessary drivers into the image to adjust for this change.

Your snapshot might contain the necessary drivers in its cache; if so, this wizard will inject those drivers; otherwise, you'll need to supply the drivers.

b. When prompted, click **Yes apply the changes physically**, then **Next**:



Ready to adjust the OS.

The wizard has not applied your changes yet. On this page, you can either accept or reconsider the changes.

Please note, if you accept the changes, the wizard will **physically** perform all operations. You won't be able to **interrupt this process** or **undo the changes**.

It may take some time to apply the changes, and you may also be asked to restart your computer during this process.

Would you like to apply your changes?

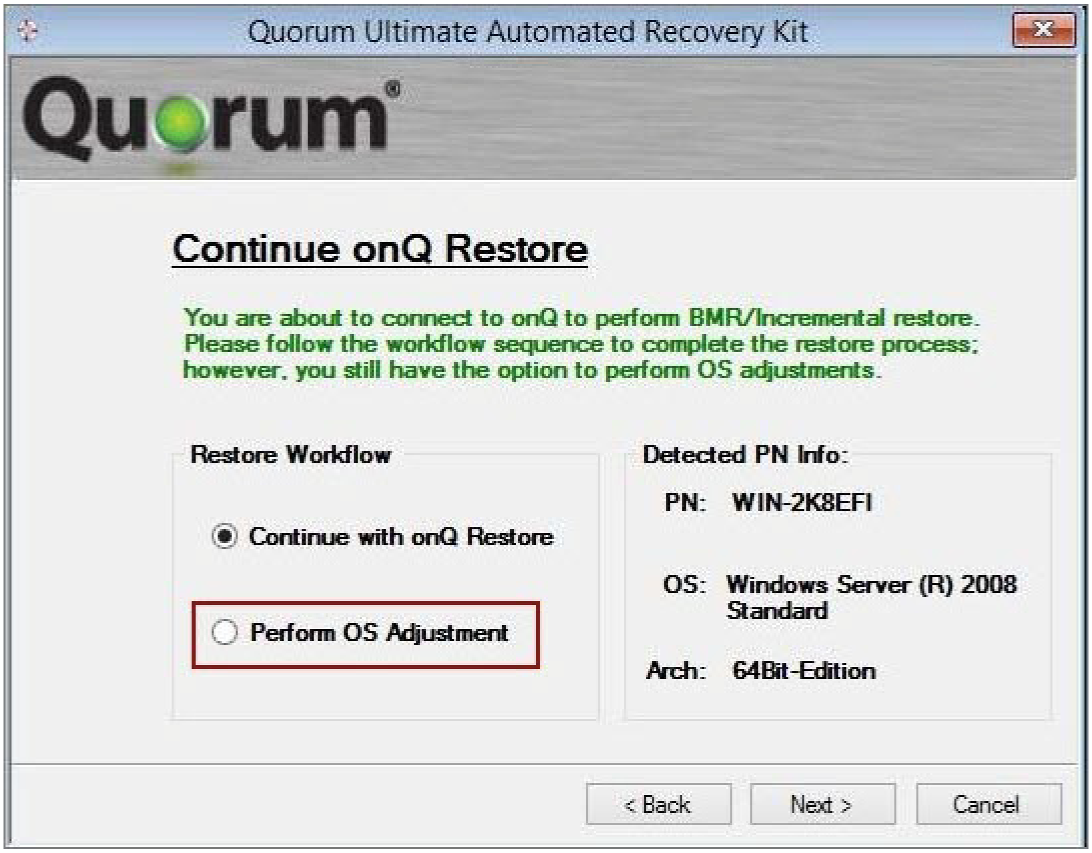
● Yes, apply the changes physically.

○ No, let me reconsider.

c. Select **Reboot the system** or **Shutdown the system** to complete the restore, then **Finish**.

If you reboot the PN without adjusting for new hardware, you can perform the adjustments after the restore completes. Simply launch the wizard again by repeating Step 3 and Step 4, then select the

Perform OS Adjustment workflow from the **Continue onQ Restore** page.



Continue onQ Restore

You are about to connect to onQ to perform BMR/Incremental restore. Please follow the workflow sequence to complete the restore process; however, you still have the option to perform OS adjustments.

Restore Workflow

● Continue with onQ Restore

○ Perform OS Adjustment

Detected PN Info:

PN: WIN-2K8EFI

OS: Windows Server (R) 2008 Standard

Arch: 64Bit-Edition

(Step 3) To manually adjust a PN's operating system for new hardware:

If after performing a BMR your PN does not boot (BSOD), you're missing boot-critical drivers. In the rare case that the P2P tool did not properly adjust your PN's operating system for the new hardware, you need to manually adjust the operating system using the P2P Adjust OS Wizard's **Set parameters for the OS adjustment** option. Before you begin, retrieve the necessary drivers.

1. Launch the QUARK wizard:

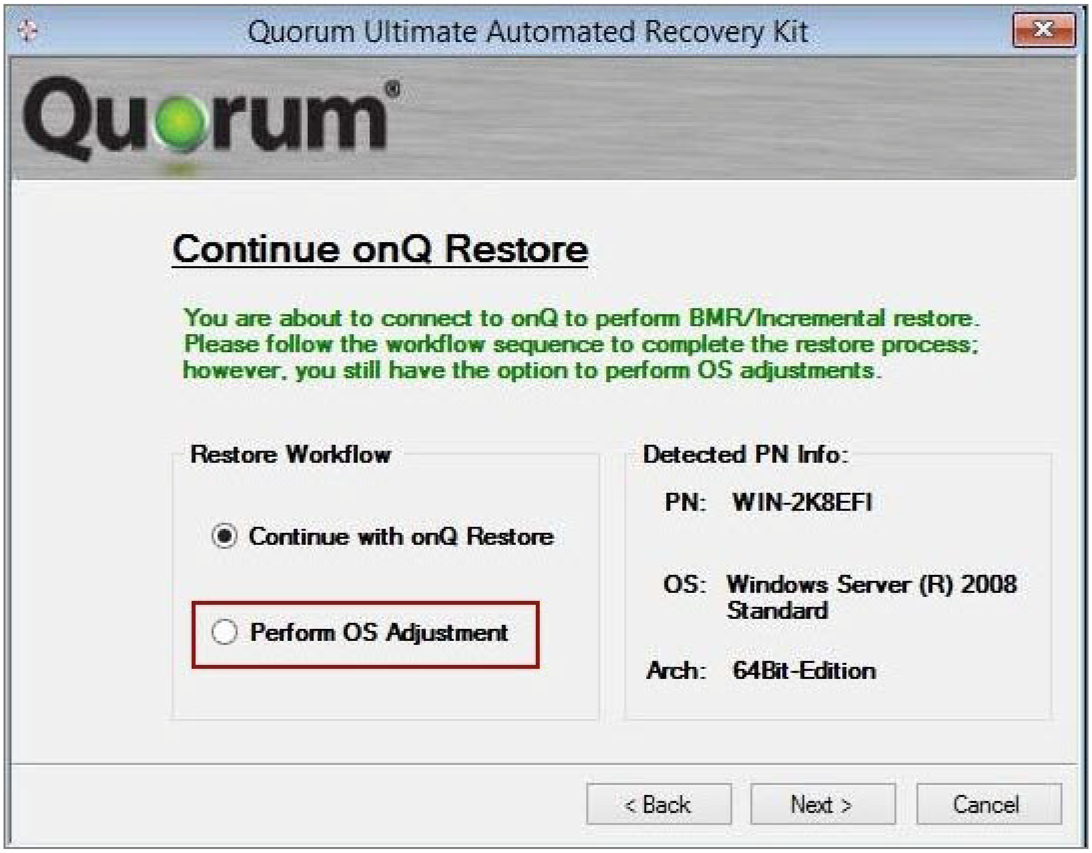
   a. Configure the Recovery PN's BIOS to boot QUARK.

   b. Boot the Recovery PN to load the QUARK image.

   The **Start BMR** page appears.

2. From the **Start BMR** page, allow the QUARK wizard to check for basic network and disk controller drivers on which QUARK depends, then **Next**.

3. From the **Continue onQ Restore** page, select the **Perform OS Adjustment** workflow.



Continue onQ Restore

You are about to connect to onQ to perform BMR/Incremental restore. Please follow the workflow sequence to complete the restore process; however, you still have the option to perform OS adjustments.

Restore Workflow

● Continue with onQ Restore

○ Perform OS Adjustment

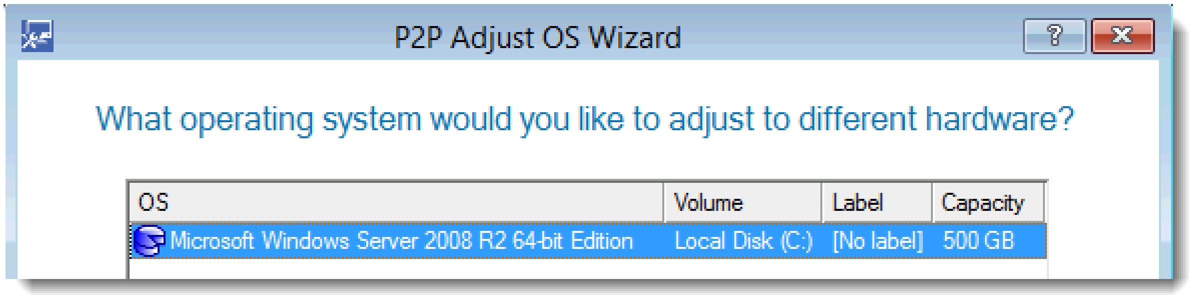
Detected PN Info:

PN: WIN-2K8EFI

OS: Windows Server (R) 2008 Standard

Arch: 64Bit-Edition

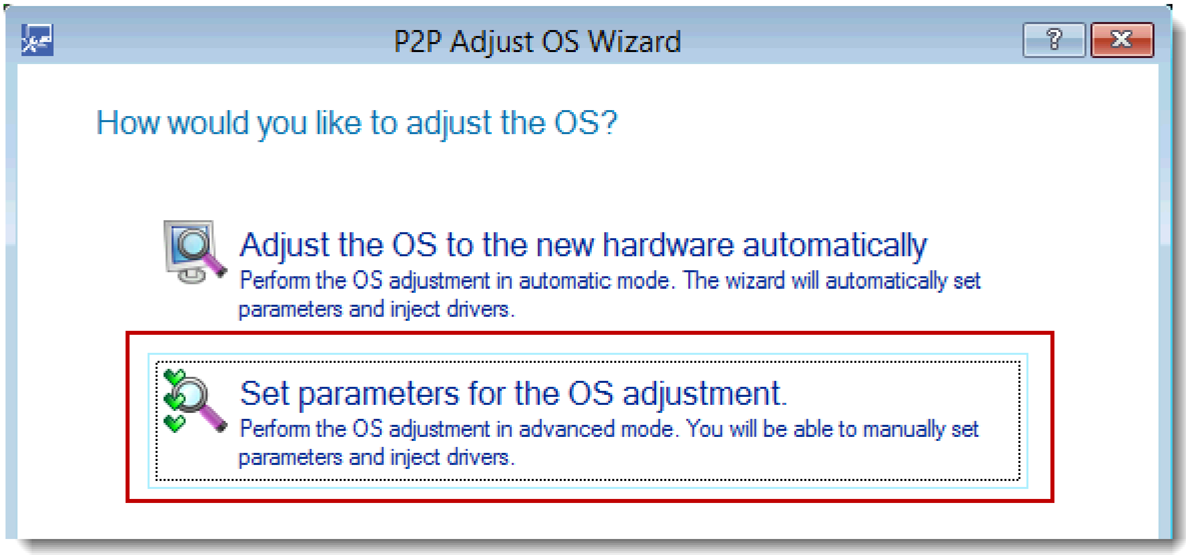
4. From the **P2P Adjust OS Wizard**, select the Recovery PN’s operating system, then **Next**.



What operating system would you like to adjust to different hardware?

OS	Volume	Label	Capacity
Microsoft Windows Server 2008 R2 64-bit Edition	Local Disk (C:)	[No label]	500 GB

5. Choose **Set parameters for the OS adjustment**, then **Next**.

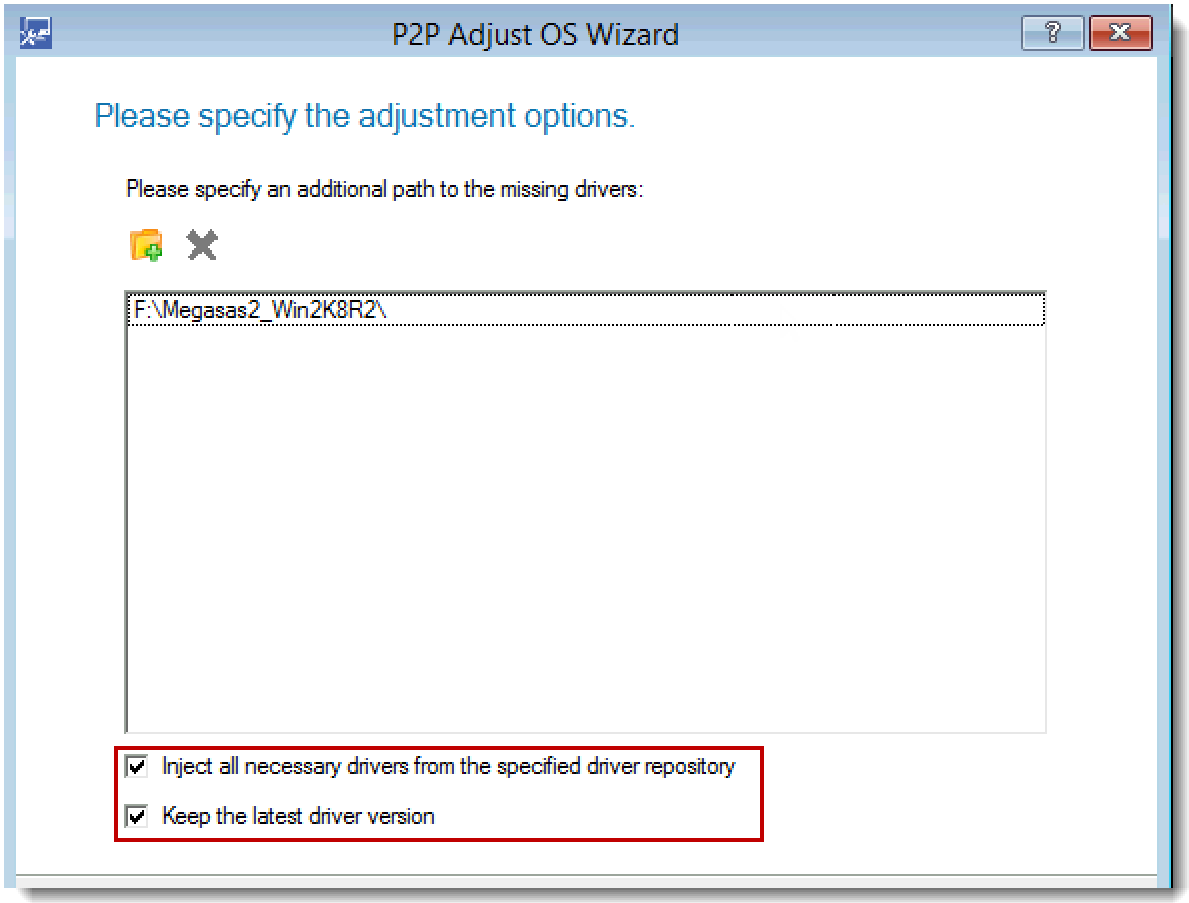


How would you like to adjust the OS?

Adjust the OS to the new hardware automatically
Perform the OS adjustment in automatic mode. The wizard will automatically set parameters and inject drivers.

Set parameters for the OS adjustment.
Perform the OS adjustment in advanced mode. You will be able to manually set parameters and inject drivers.

6. Specify the path to the driver, select the **Inject all necessary drivers from the specified repository** check box and the **Keep the latest driver version** check box, then **Next**.



Please specify the adjustment options.

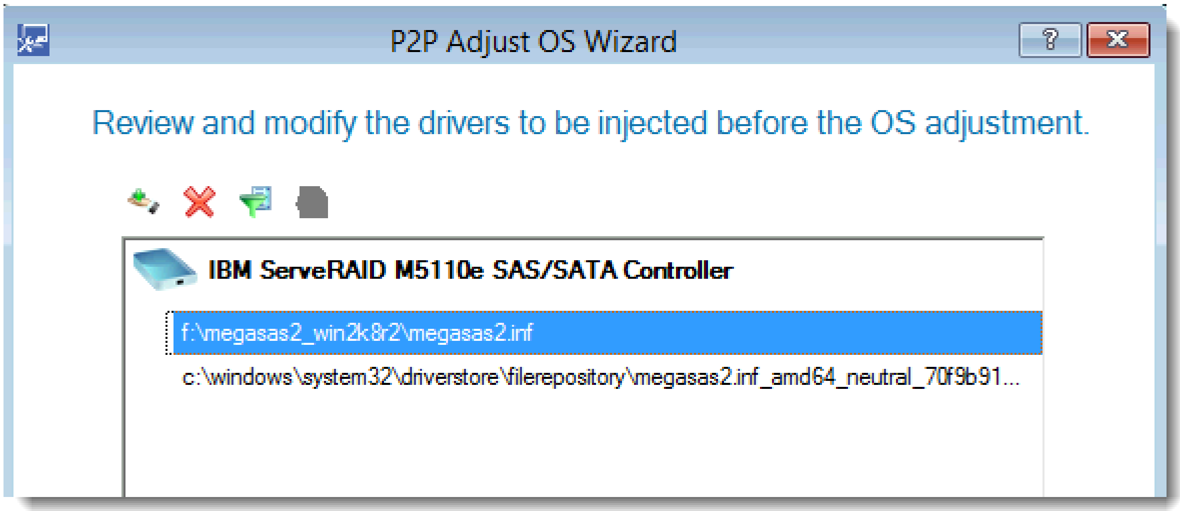
Please specify an additional path to the missing drivers:

F:\Megasas2_Win2K8R2\

☑ Inject all necessary drivers from the specified driver repository

☑ Keep the latest driver version

7. Select the driver, then **Next**.



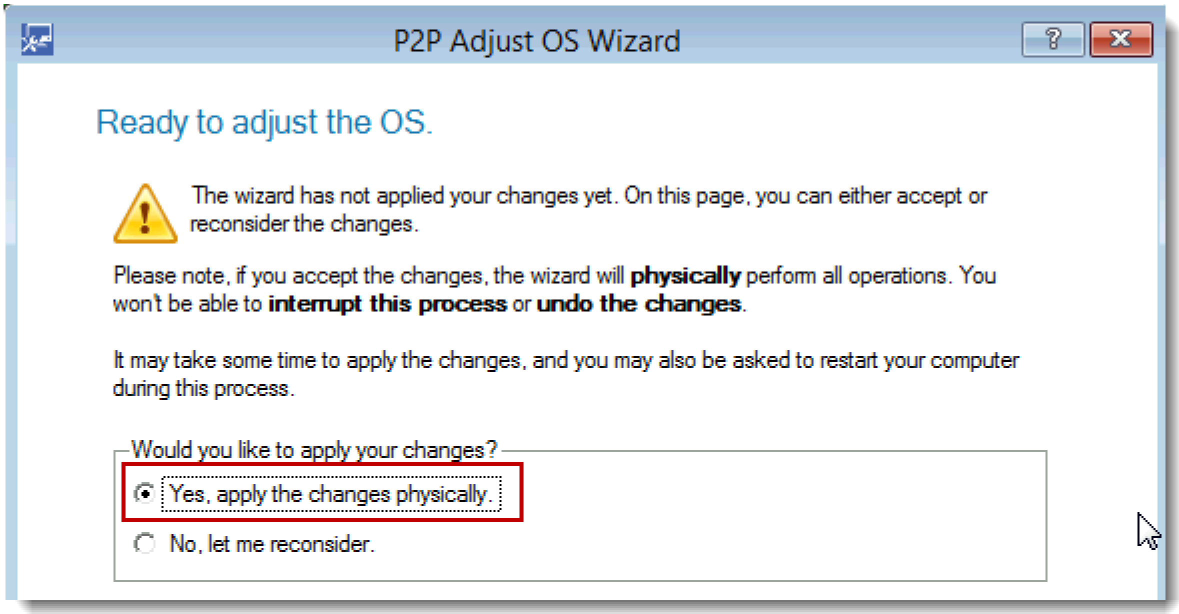
Review and modify the drivers to be injected before the OS adjustment.

IBM ServeRAID M5110e SAS/SATA Controller

f:\megasas2_win2k8r2\megasas2.inf

c:\windows\system32\driverstore\filerepository\megasas2.inf_amd64_neutral_70f9b91...

8. Select the **Yes, apply the changes physically** radio button to make the necessary adjustments, then **Next**.



Ready to adjust the OS.

The wizard has not applied your changes yet. On this page, you can either accept or reconsider the changes.

Please note, if you accept the changes, the wizard will **physically** perform all operations. You won't be able to **interrupt this process** or **undo the changes**.

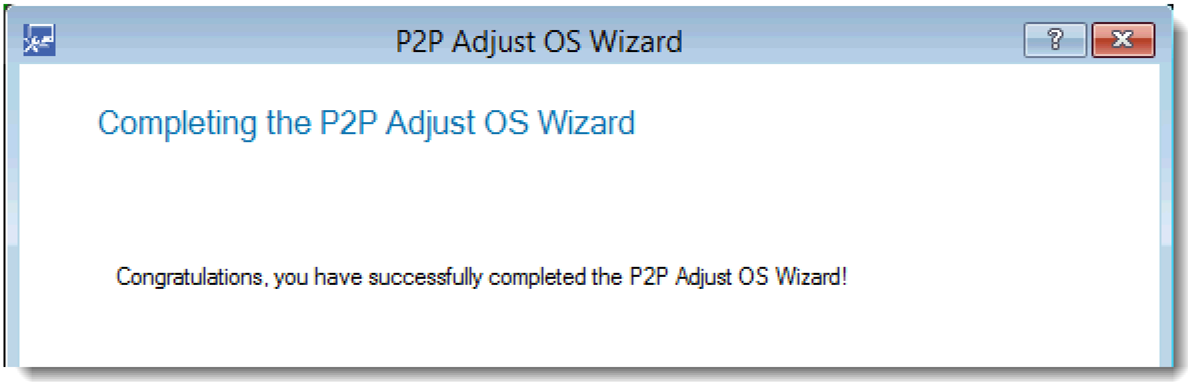
It may take some time to apply the changes, and you may also be asked to restart your computer during this process.

Would you like to apply your changes?

● Yes, apply the changes physically.

○ No, let me reconsider.

9. Click **Finish**. Now that your PN has the correct boot-critical drivers, your PN should now boot.



Completing the P2P Adjust OS Wizard

Congratulations, you have successfully completed the P2P Adjust OS Wizard!

10. Select **Reboot the system** or **Shutdown the system** to complete the adjustments, then **Finish**.

(Step 4) To interpret QUARK Errors:

Error	Cause	What do I do?
`Authentication failed for onQ`	You typed the incorrect credentials.	Try again.
`Command Failed, IP Address is in use by a Protected Node`	When you specified an IP address for the QUARK client, you typed an IP address that's already listed in the onQ's hosts file. The QUARK client needs an IP address to communicate with onQ. A common mistake is to specify the PN's original IP address.	Change the IP address in QUARK's **Network Configuration** page.
`Failback already running for a different target`	The onQ Appliance is busy performing a BMR for a different Recovery PN. An onQ Appliance can only perform one BMR at a time.	Wait for the in-progress BMR to complete, then perform the next BMR.
`onQ Protection turned off. Could not continue with BMR process`	Protection on the onQ Appliance is off.	Turn on protection.

Error	Cause	What do I do?
`onQ connection timeout`	If the wizard doesn't get a response from the onQ Appliance within 60 seconds, the wizard displays this timeout error.	Try again.
`Could not connect to onQ`	The wizard could not connect to the onQ Appliance.	Try again.
`Could not retrieve PN list from onQ`	There was either an unexpected database error; or There are no PNs in the onQ Appliance's list of protected node (the list is empty).	Try again. If the problem persists, verify that you logged on to the correct onQ Appliance.
`No Snapshots available for the selected PN`	There are no snapshots available on this onQ Appliance for the PN you selected.	Verify that you logged on to the correct onQ Appliance.
`onQ already started failback for a different target. onQ terminating current BMR session.`	onQ allows concurrent BMR logins to the same onQ Appliance; however, precedence is given to the last BMR user. If you are not that user and you try to start a BMR/Incremental restore, you will be rejected by onQ: QUARK automatically redirects you to the logon page and displays the aforementioned message.	Perform the BMR at a later time.
`EFI system partition not detected. Please check disk configuration.`	BMR for EFI boot based PNs require EFI system partition to be created prior to restore. If the user's intent is to perform a EFI based restore, then QUARK checks the presence of EFI system partition before the start of the restore. QUARK returns this error if QUARK cannot detect an EFI partition.	Specify the correct partition style in the **QUARK Disk Configuration** wizard.

(Step 5) To troubleshoot PN boot problems:

Go to BMR Problems.

Related Topics

BMR Problems
"Bare Metal Restore Support" in onQ Release Notes
Perform File-level Restore

12

Monitoring

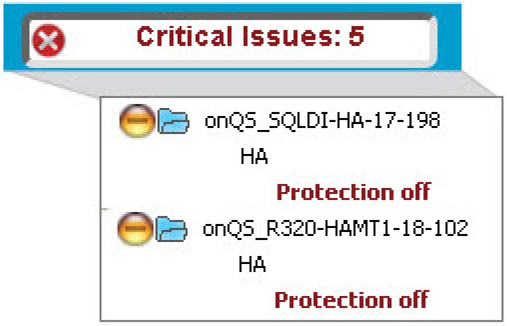
12.1 Monitor multiple onQ Appliances

Use onQ Monitor to monitor all of your onQ Appliances from a "single pane of glass". These onQ Appliances can be located in a local datacenter or in the cloud. Think of your onQ Monitor as a dashboard from which you can retrieve information about your onQ Appliances, Protected Notes, and Recovery Nodes.

onQ Monitor enables you to click one tab or one button to:

- retrieve status information and overhall health for all your onQ Appliances.
- display alerts about all your onQ Appliances.
- display current operations being performed on PNs and jobs.
- display repository use, RN disk in use, RN disk allocated for each onQ as well as RN disk usage/allocation for each PN, providing a quick overview of capacity utilization for each onQ Appliance.
- navigate to your onQ Appliance to retrieve more status information or to browse the log files directly.

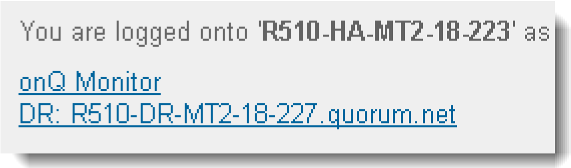
For example, from one location you can view all the onQ Appliances that have protection turned off:



To log on to onQ Monitor.

1. Log on to the HA Appliance's onQ Portal.
2. Scroll to the bottom of the **DASHBOARD** page.

3. Click on the **onQ Monitor** link in the footer.



You are logged onto '**R510-HA-MT2-18-223**' as

onQ Monitor
DR: R510-DR-MT2-18-227.quorum.net

To configure onQ Monitor:

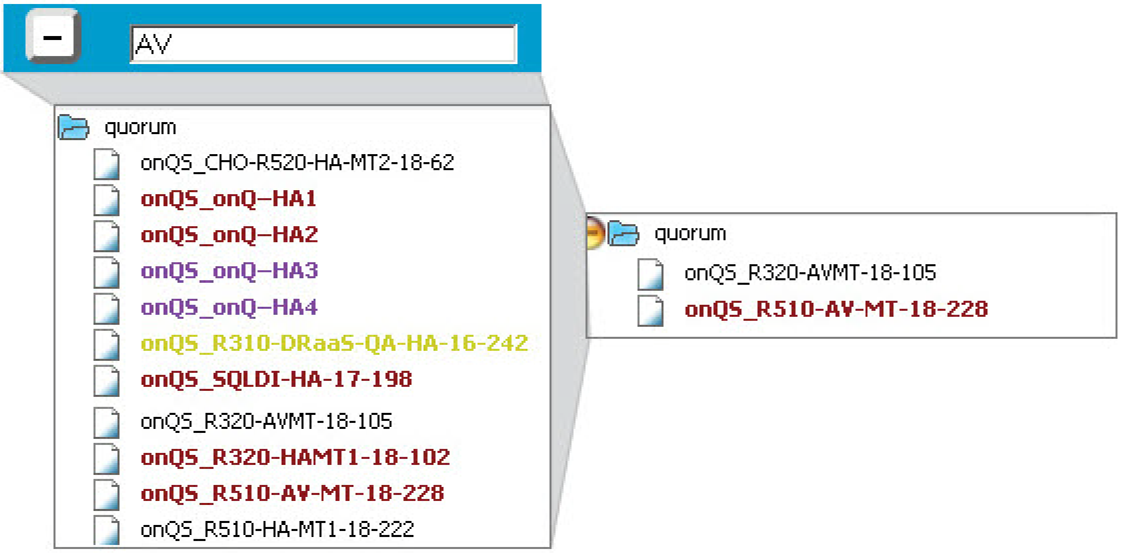
1. Log on to the onQ Monitor.
2. Add all additional HAs and onQ Archive Vaults that exist in your environment:
   a. In the navigation pane, click **Add/Remove** button.
   b. Do one of the following to retrieve the the HA or onQ Archive Vault, then **Get Name**.
      - In the **HA/AV Address** text box, type the address of the HA or onQ Archive Vault
      - In the **Set Name** text box, type the address of the the HA or onQ Archive Vault.
   c. (Optional) Type a **Group** name if you'd like to assign the HA and its DR, DR Mirror(s), and the onQ Archive Vault to a group.

      Groups help you organize your onQ Appliances. For example, you can organize your onQ Appliances by domain, subnet, or department.

      By default, onQ Monitor provides a `quorum` group to include the HA from which you logged on to the onQ Monitor.
   d. Click **ADD**.

To filter on your onQ Appliances:

You can use filters to search for a specific appliance name, or if your onQ Appliances have a naming convention, you can filter on a string to search for multiple onQ Appliances. In the following example, a filter is performed on AV string to search for all AV Appliances.



To delete a group:

When you delete a group, you also delete all the Appliance Sets (aka onQ Appliances) in that group.

1. Log on to onQ Monitor.
2. In the navigation pane, click **Add/Remove** button.
3. In the Group text box, type the name of the group (name is case sensitive), then **Delete Group**.

To browse the issues for a PN:

1. Log on to onQ Monitor.
2. in the navigation pane, click on the name of the onQ Appliance.
3. Click the **Issues** tab.
4. Wait while onQ Monitor requests issue information from the onQ Appliance. This retreival can take up to a minute depending on how busy the machine is and if you have a DR/DR mirror attached.

   onQ Monitor displays information for each PN by onQ Appliance. Each onQ Appliance is a hyperlink.

To browse the status of a PN:

1. Log on to onQ Monitor.

2. in the navigation pane, click on the name of the onQ Appliance.
3. Click the **Status** tab.
4. Wait while onQ Monitor requests status information from the onQ Appliance. This retreival can take up to a minute depending on how busy the machine is and if you have a DR/DR mirror attached.

   onQ Monitor displays information for each PN by onQ Appliance. Each onQ Appliance is a hyperlink.

To browse the status of a job:

1. Log on to onQ Monitor.
2. From the navigation pane, apply a filter to display all AV Appliances. Go to To filter on your onQ Appliances:
3. Click on the **STATUS** tab.
4. Wait a few seconds while onQ Monitor requests status information from the AV Appliance.

   onQ Monitor displays information for each job by onQ Appliance.

Related Topics

Generate on-demand reports

12.2 Generate on-demand reports

onQ Monitor enables you to generate reports that provide you both realtime and historical data. onQ Monitor aggregates this data across one or more onQ Appliances, highlighting the current activities on your onQ Appliances and PNs and the trends over the last 2 years.

These reports (charts and graphs) help you answer questions about your system in an effort to help you:

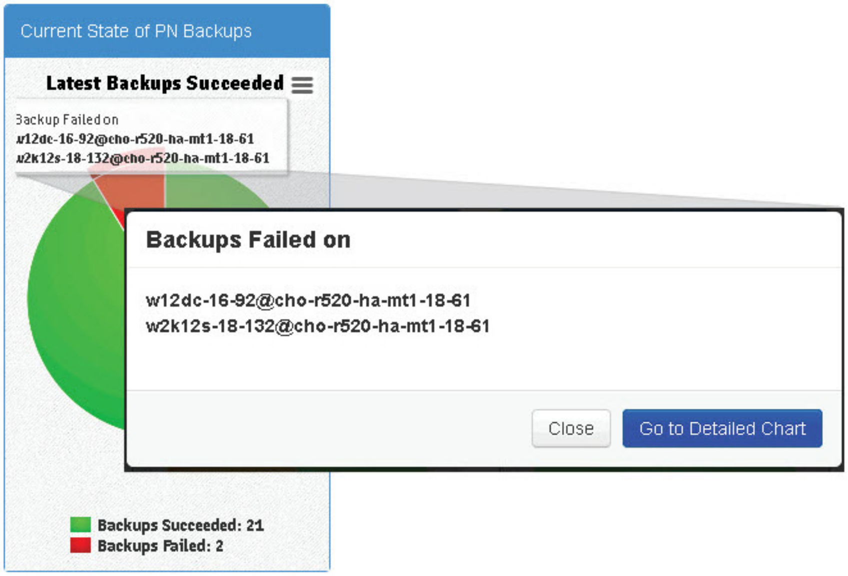
- make changes to your systems.
- forecast the need for system changes.
- prevent system failures.

- debug system issues.

To browse an Overview Report:

Overview Reports represents real-time data. Overview Reports aggregate the most recent backup, repository information, transfer, and self test for all the PNs. Unlike Historical Reports, Overview Reports do not display historical data; however, you can double-click on the pie charts to skip to the related historical report.

- **Backups Succeeded Chart**. This chart displays whether the *most recent* (last) backup for every enrolled PN was successful or not. If, for example, 21 backups out of 23 were successful, the success rate is 91%. Simply hover-over or double-click on the pie chart to retrieve a list of the PNs that correspond to the backup failures.



Current State of PN Backups

Latest Backups Succeeded

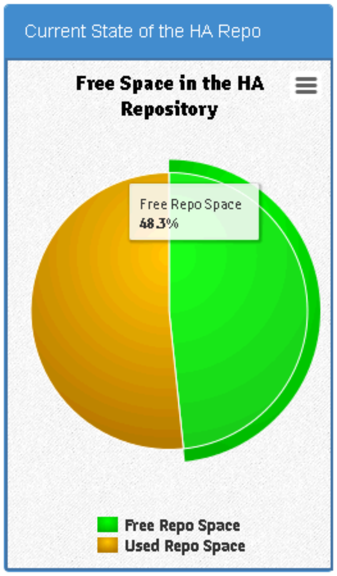
Backup Failed on
w12dc-16-92@cho-r520-ha-mt1-18-61
w2k12s-18-132@cho-r520-ha-mt1-18-61

Backups Failed on

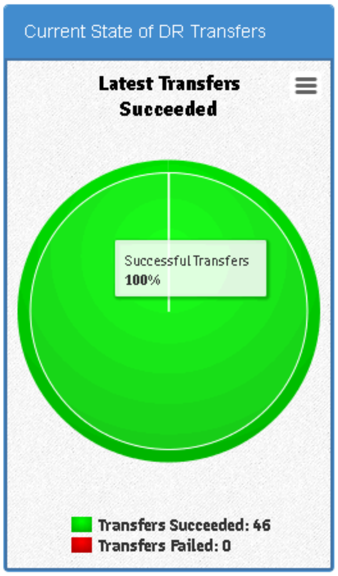
w12dc-16-92@cho-r520-ha-mt1-18-61
w2k12s-18-132@cho-r520-ha-mt1-18-61

🟩 Backups Succeeded: 21
🟥 Backups Failed: 2

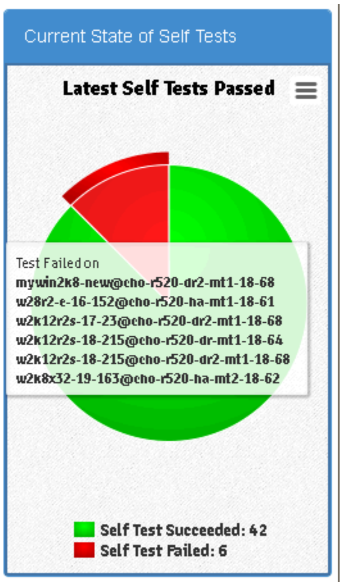
- **Free Space in Repository Chart**. This chart displays the *current* percentage of both free and used disk space in the snapshot repository. In case of a multi-tenant HA, the chart displays the sum of the free space on each snapshot repository and the sum of the used space on each snapshot repository Hover-over text provides you the percentage of free and unused space.



- **DR Transfers Succeeded Chart**. This chart displays whether the *most recent* (latest) DR transfer for every enrolled PN was successful or delayed. If, for example, you have 4 enrolled PNs, the chart displays the aggregation of the latest DR transfer for each of those PNs. If the DR transfer was successful for one of those PNs, but the DR connection was severed for some reason, the DR transfer for the three other PNs will be delayed until the connection is operating.


Current State of DR Transfers
Latest Transfers Succeeded
Successful Transfers
100%
🟩 Transfers Succeeded: 46
🟥 Transfers Failed: 0

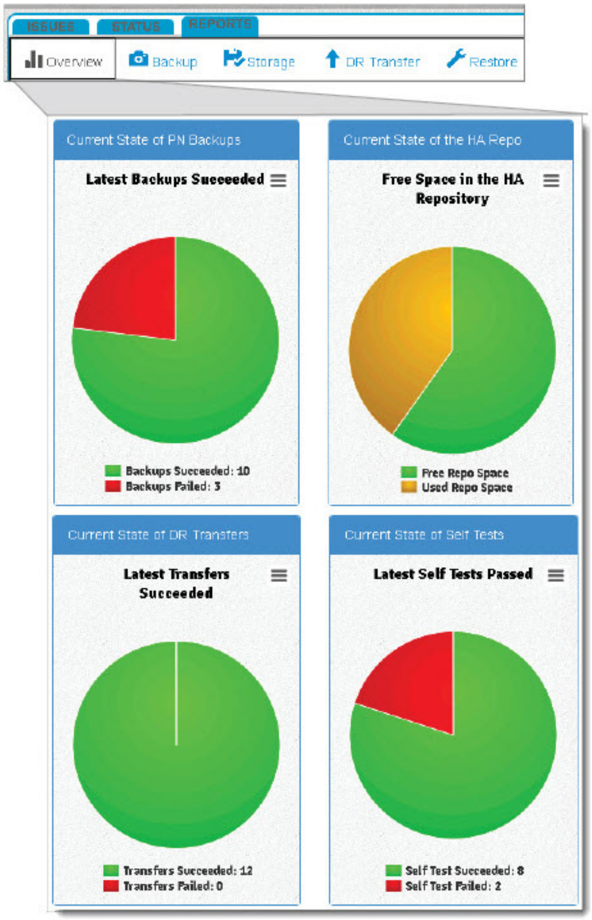
- **PNs Passing Self Test Chart**. This chart displays the *most recent* (latest) self test that passed for every enrolled PN. If, for example, you have 42 enrolled PNs and 6 of them failed the latest self test, the pass rate is 88%. Simply hover-over or double-click on the pie chart to retrieve a list of the PNs that correspond to the self test failures.



Test Failed on
mywin2k8-new@cho-r520-dr2-mt1-18-68
w28r2-e-16-152@cho-r520-ha-mt1-18-61
w2k12r2s-17-23@cho-r520-dr2-mt1-18-68
w2k12r2s-18-215@cho-r520-dr-mt1-18-64
w2k12r2s-18-215@cho-r520-dr2-mt1-18-68
w2k8x32-19-163@cho-r520-ha-mt2-18-62

1. Log on to onQ Monitor.

2. Click on the **REPORTS** tab > **Overview** subtab.



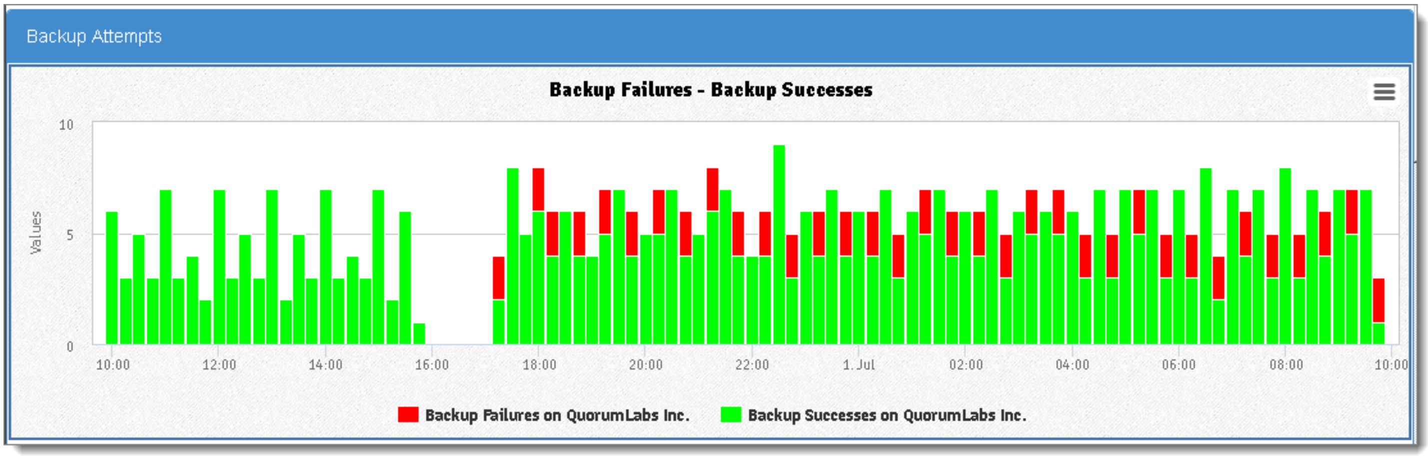
3. Wait for the charts to display.

To generate a Historical Report:

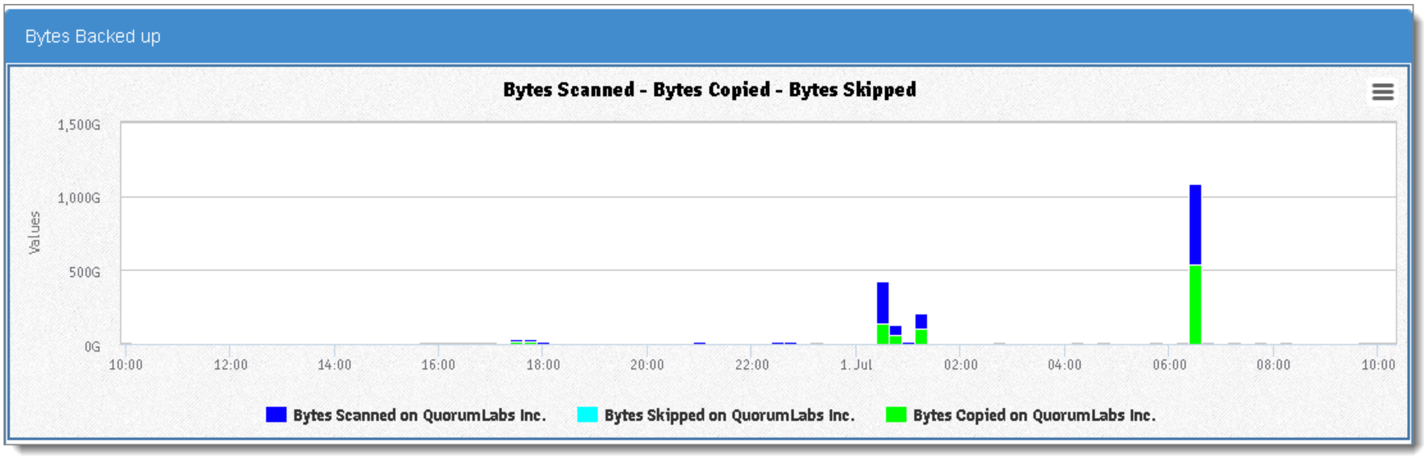
Historical Reports can report on activity going back 24 months. Historical Reports communicate reporting information using graphs. You can choose from the following Historical Reports:

- **Backup Historical Report**. Use this report in conjunction with the knowledge that queued snapshots can occur if the onQ is overly busy backing up other PNs or if the PNs have short backup intervals.
  - **Backup Attempts Graph**. This graph shows the total number of backup failures and successes in the time interval that you

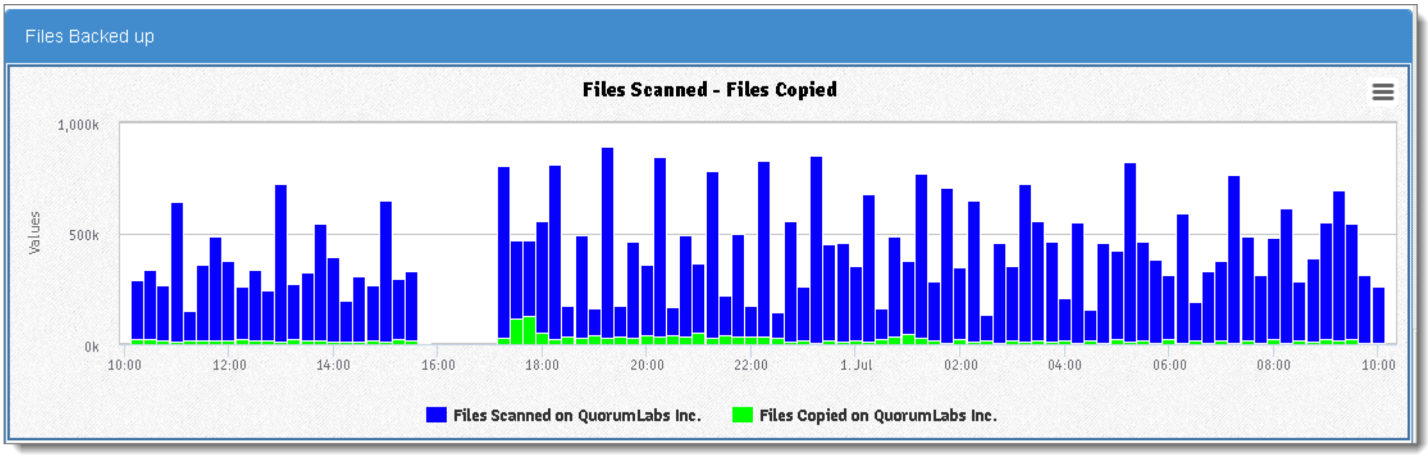
specified across different instances.



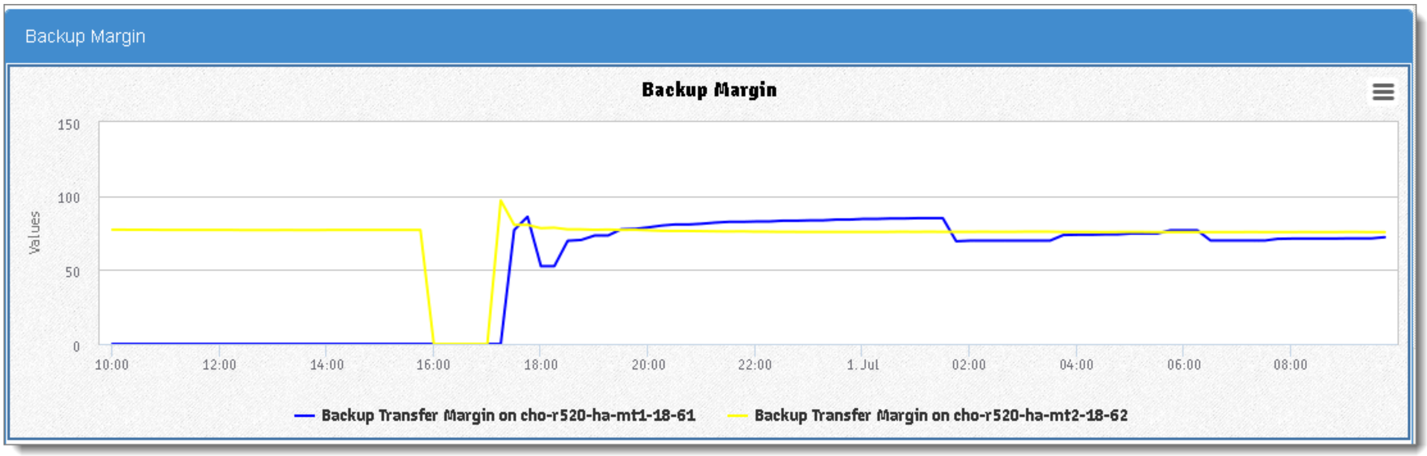
- **Bytes Backed up Graph**. The total number of bytes squirtcopy scanned, copied, and skipped in the time interval that you specified across the different instances. onQ skips bytes/files if instructed to do so as outlined in Edit backup exclude list.



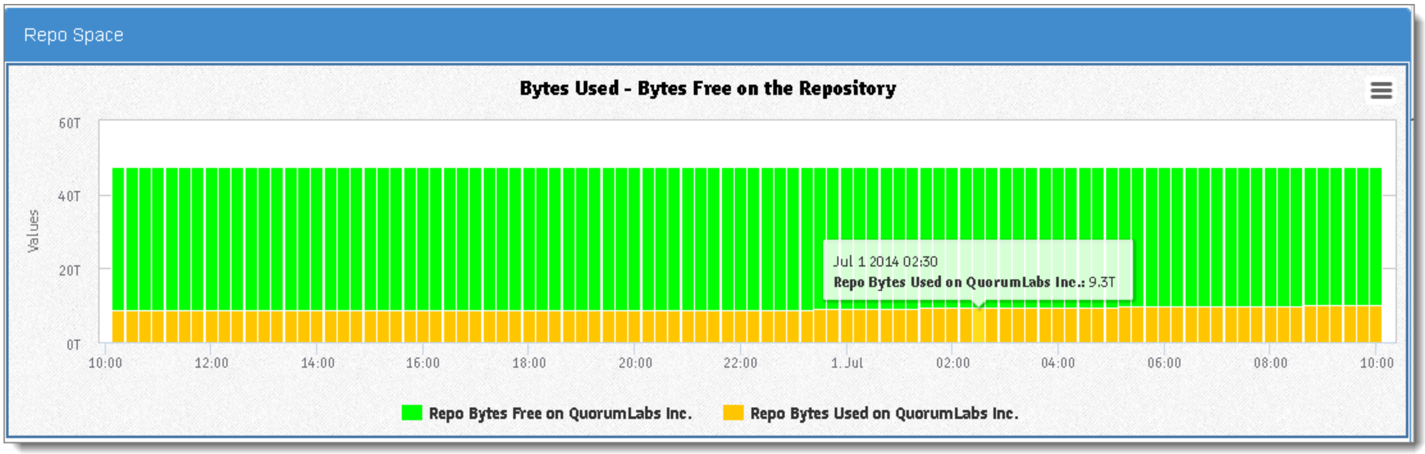
- **Files Backed up Graph**. The total number of scanned files on the PN by squirtcopy and the total number files that squirtcopy copied to the instances and within the time interval that you specified.



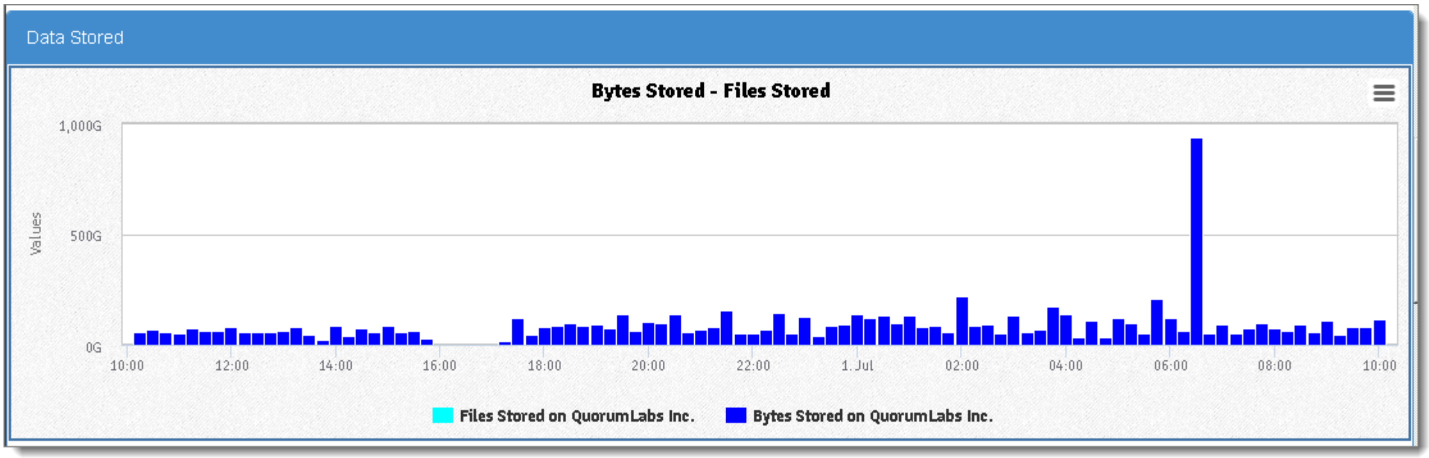
- **Backup Margin Graph**. If the margin value is low, backups are taking longer than expected to complete. This is the same value shown in the HA portal's **Backup Transfer Margin** column. You might need to change your backup interval as outlined in Monitor protected nodes and Monitor backups.



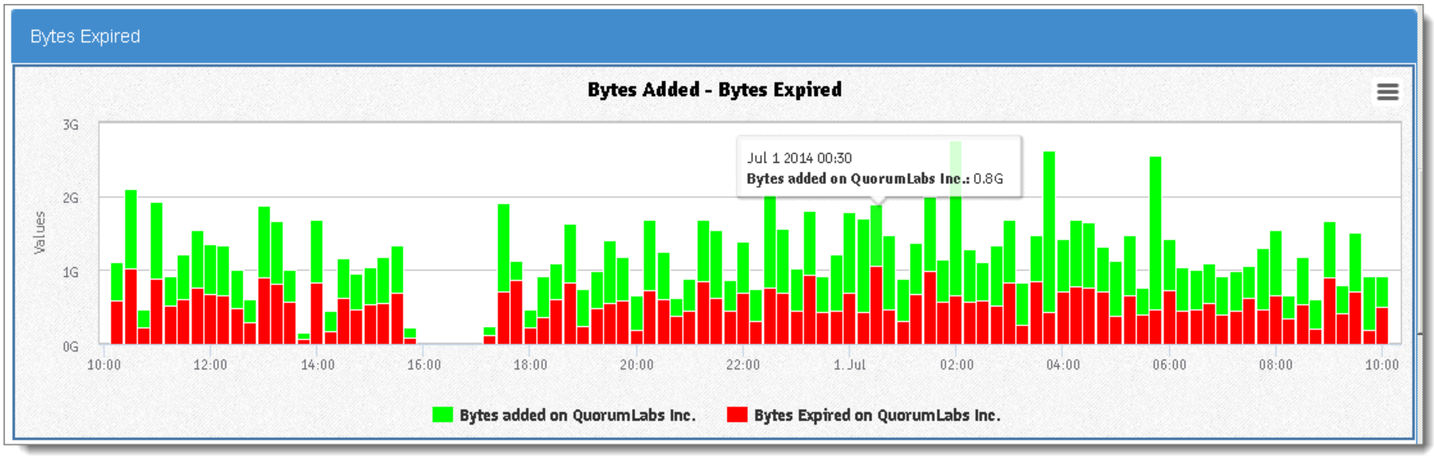
- **Storage Historical Report**. Use this historical report to determine if you need to add more snapshot disk space or delete orphan backups manually to free up space.
  - **Repo Space Graph**. This graph displays the total number of bytes used on the Repository.


Repo Space
Bytes Used - Bytes Free on the Repository
60T
40T
20T
0T
Values
Jul 1 2014 02:30
Repo Bytes Used on QuorumLabs Inc.: 9.3T
10:00
12:00
14:00
16:00
18:00
20:00
22:00
1. Jul
02:00
04:00
06:00
08:00
10:00
🟩 Repo Bytes Free on QuorumLabs Inc.
🟨 Repo Bytes Used on QuorumLabs Inc.

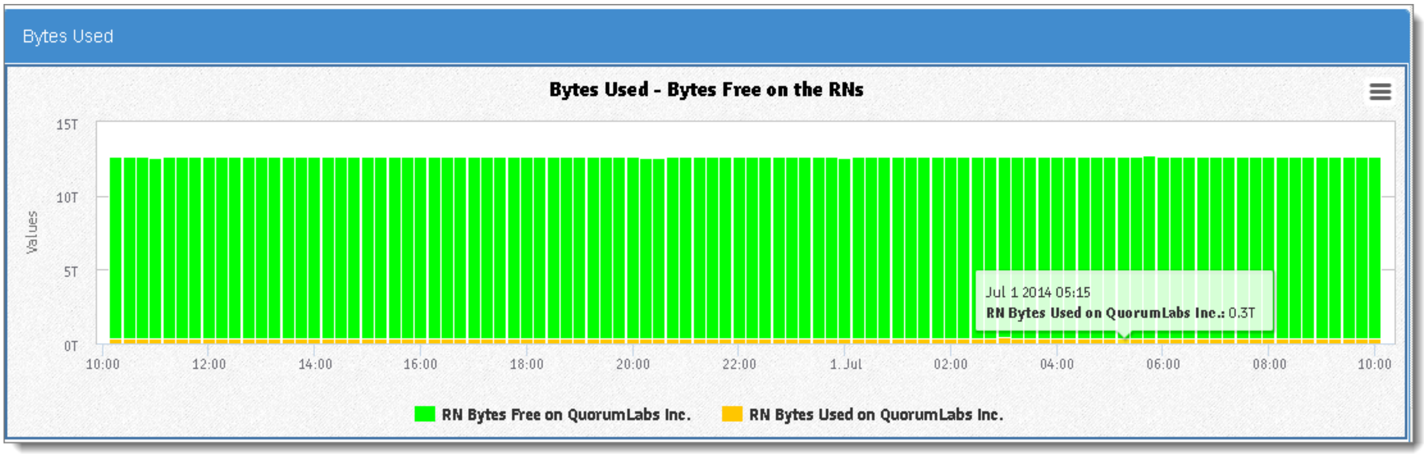
  - **Data Stored Graph**. This graph displays the total bytes or files stored in the snapshot repository. The repository is the deduplicated archive of all snapshots of all of your Protected Nodes. From the repository, onQ can reproduce a complete system image from any snapshot.



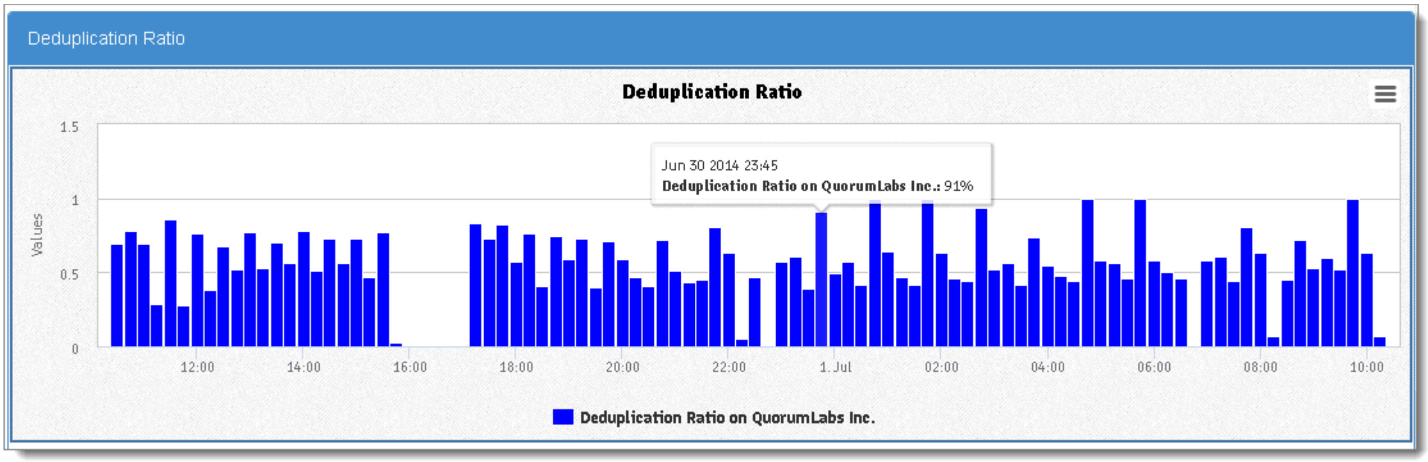
  - **Bytes Expired**. When the onQ Appliance was pre-configured, a specific amount of disk space was allocated to the repository. Moreover, onQ has a built-in purge policy whereby if its disk space exceeds 85% onQ begins to "free up" space by deleting PN backups, starting with the oldest backups. Files expired and bytes expired values refer to the data (in files and bytes) that onQ expired plus the bytes expired due to the retention period being met.



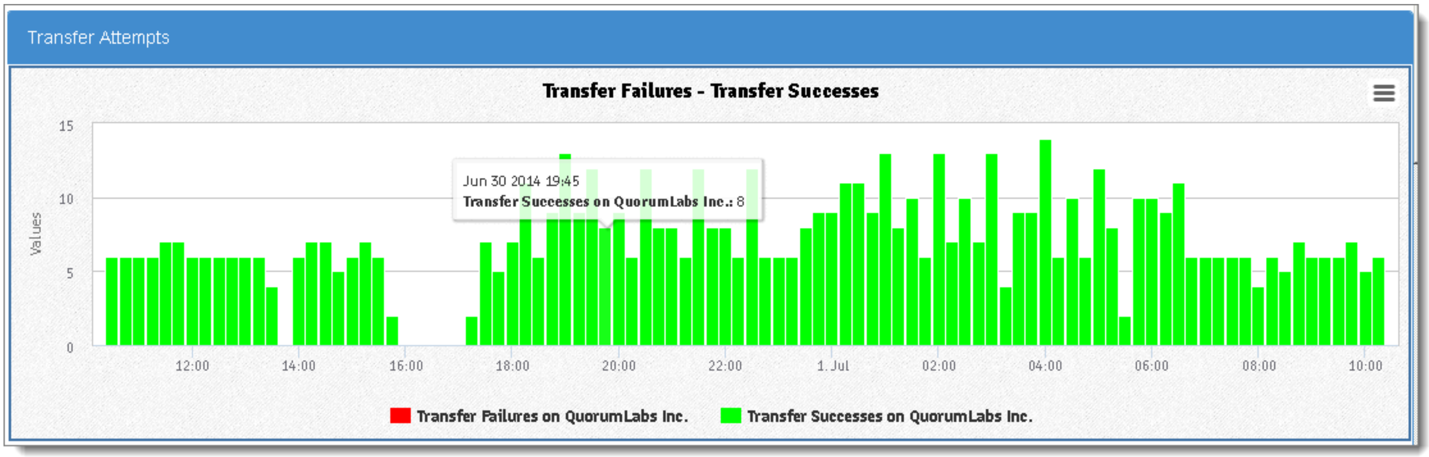
- **Bytes Used Graph**. This graph displays the total number of bytes used on the Recovery Nodes.



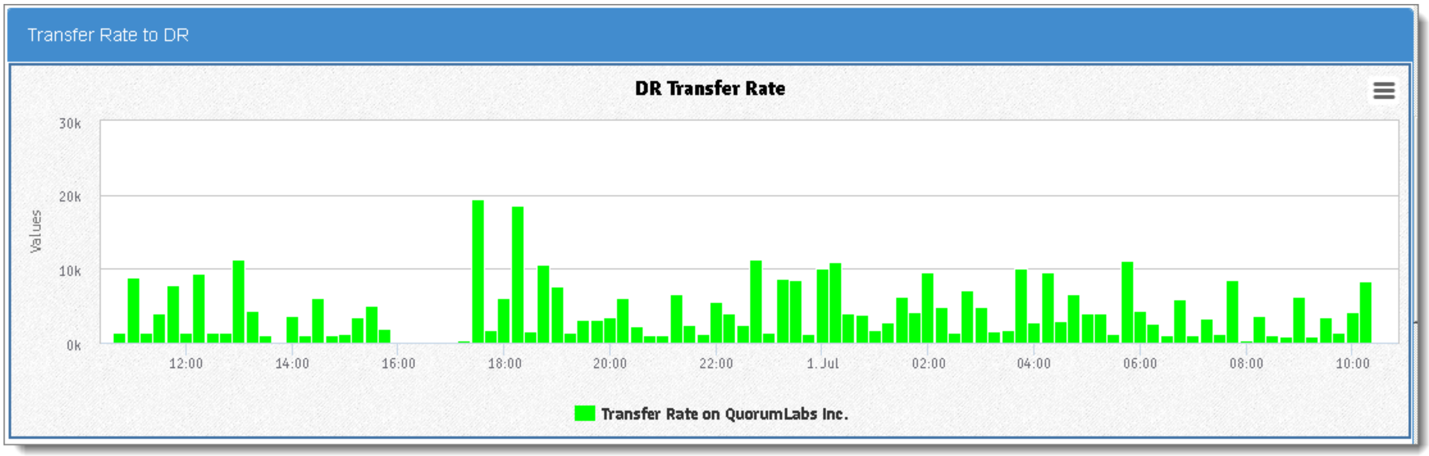
- **Deduplication Ratio Graph**. This graph shows the data compression ratio, which is equal to the total number of bytes copied divided by the total number of bytes added. If your PNs all have the same data, you'll see a better compression ratio then if your PNs have unique data; the latter scenario is indicative of duplicate data on your PNs.


Deduplication Ratio
Deduplication Ratio
1.5
1
0.5
0
Values
Jun 30 2014 23:45
Deduplication Ratio on QuorumLabs Inc.: 91%
12:00
14:00
16:00
18:00
20:00
22:00
1. Jul
02:00
04:00
06:00
08:00
10:00
Deduplication Ratio on QuorumLabs Inc.

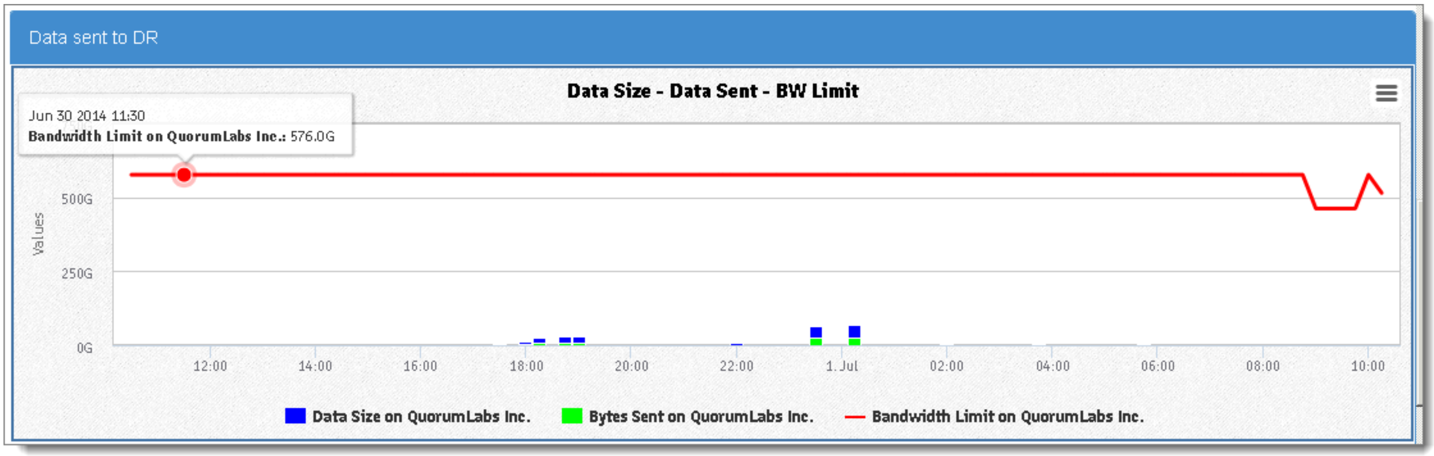
- **DR Transfer Historical Report**. After performing a backup, the HA transfers this data from the HA to the DR Appliance. Use this report to help determine whether or not to adjust bandwidth throttling to speed up data transfers.
  - **Transfer Attempts Graph**. This graph shows the number of HA-to-DR or DR-to-DRMirror or both transfer attempts and successes in the time interval that you specified and depending on the instances that you choose. For example, if you want to show all HA-to-DR transfers, then select the HA Appliances; do not select any DR Appliances.


Transfer Attempts
Transfer Failures - Transfer Successes
Values
15
10
5
0
Jun 30 2014 19:45
Transfer Successes on QuorumLabs Inc.: 8
12:00
14:00
16:00
18:00
20:00
22:00
1. Jul
02:00
04:00
06:00
08:00
10:00
🟥 Transfer Failures on QuorumLabs Inc.
🟩 Transfer Successes on QuorumLabs Inc.

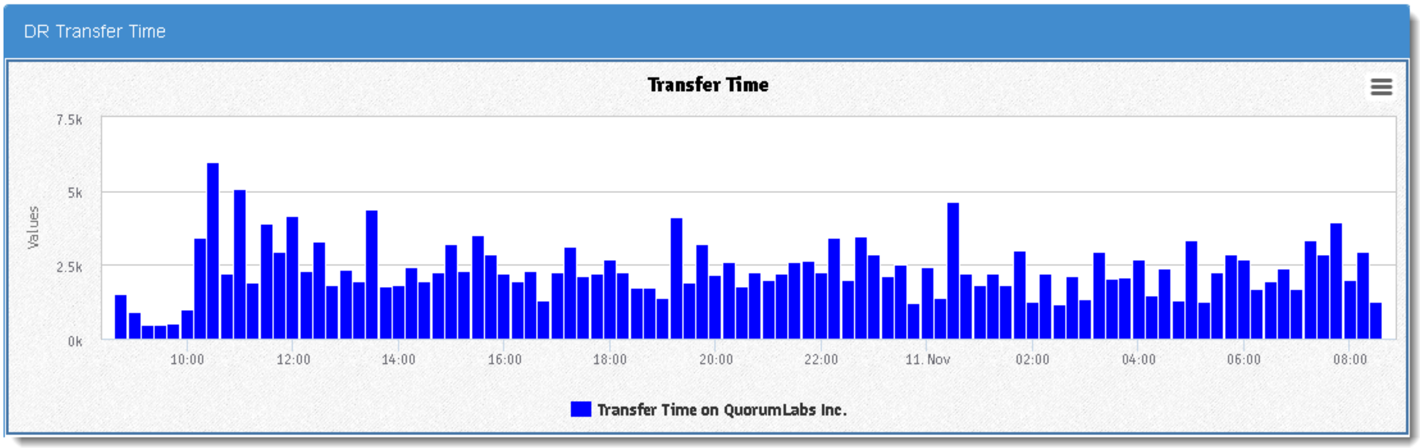
  - **Transfer Rate to DR Graph**. This graph shows the transfer rate, in bytes/seconds, for all successful transfers within a time interval that you specified.



  - **Data Sent to DR Graph**. This graph shows the total bytes sent from the HA appliance and the total bytes sent to the DR appliance. The bandwidth limit is the transfer limit at the time of transfer that you defined in the onQ portal.

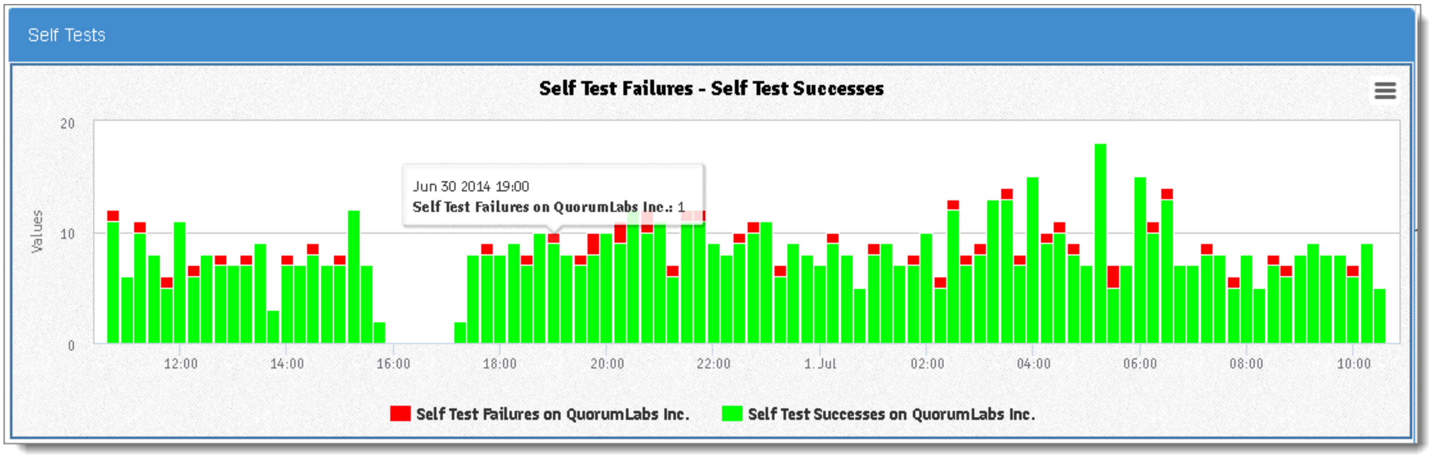


- **Transfer Time**. If the transfers are taking longer than expected to complete, you might need to modify the backup interval, modify the Window Start time, and adjust bandwidth throttling.

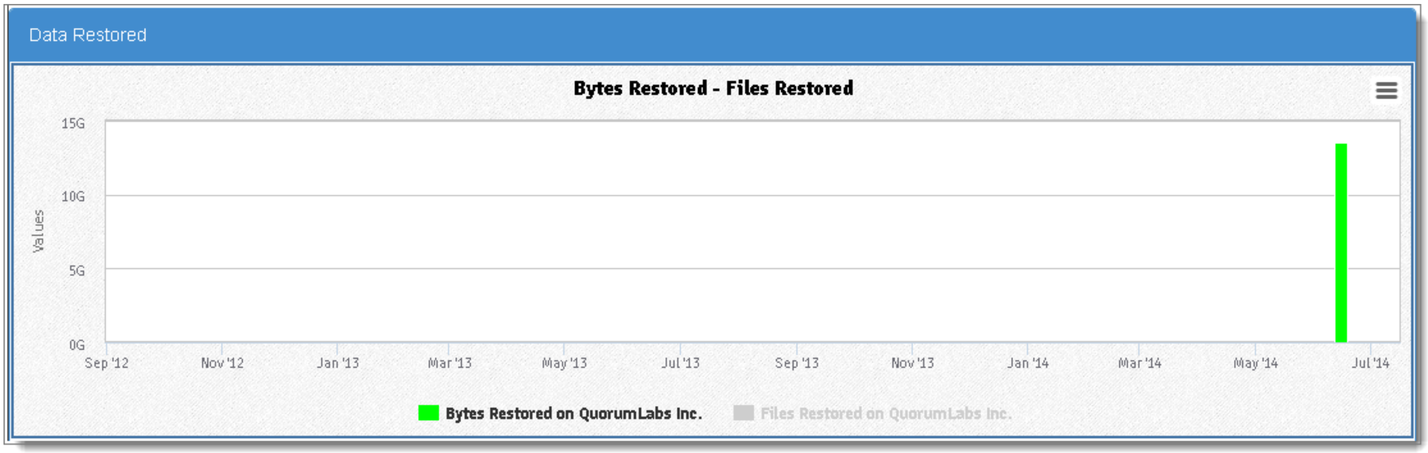


- **Restore Historical Report**.
  - **Self Tests Graph**. onQ can automatically test (also called Self Test), on a predefined schedule, recovery nodes’ ability to boot properly and can communicate with the onQ Service. This historical report shows the number of self test failures and successes in the time interval that you specified. Use this data to

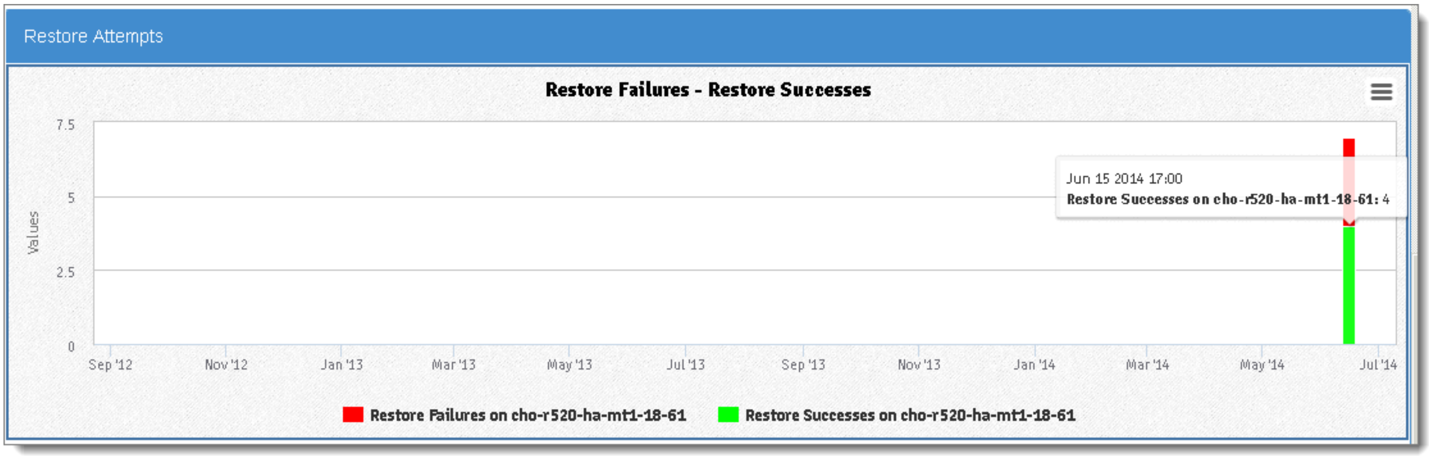
help assess your PN’s vulnerability to disasters.


Self Tests
Self Test Failures - Self Test Successes
Values
20
10
0
Jun 30 2014 19:00
Self Test Failures on QuorumLabs Inc.: 1
12:00
14:00
16:00
18:00
20:00
22:00
1. Jul
02:00
04:00
06:00
08:00
10:00
🟥 Self Test Failures on QuorumLabs Inc.
🟩 Self Test Successes on QuorumLabs Inc.

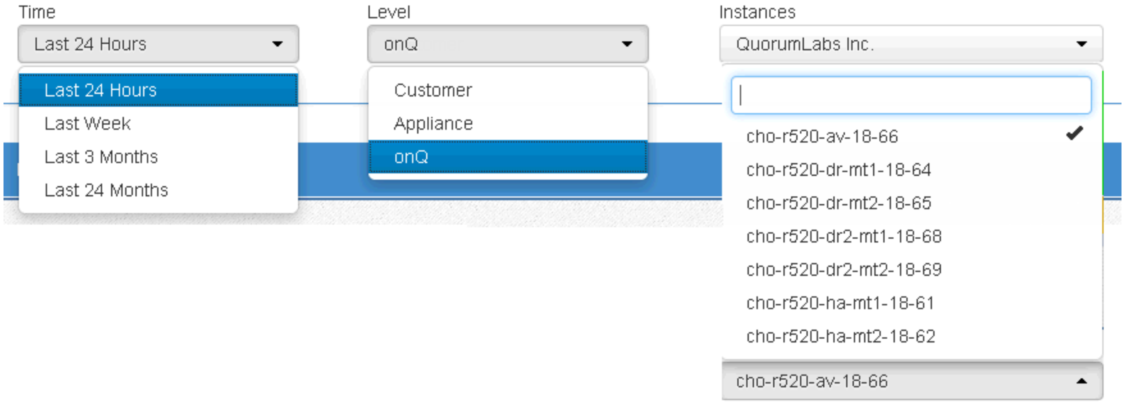
- **Data Restored Graph**. This historical report shows the number of bytes and files restored using FLR. You can use this chart to provide restore statistics for SLA reporting. You can also use this report to verify that the number of files and bytes that you expected to restore matches the files and bytes that were actually restored.



- **Restore Attempts Graph**. This historical report shows the number of FLR restore attempts that failed and succeeded.



1. Log on to onQ Monitor.
2. Click on the **REPORTS** tab.
3. Click on the **Backup**, **Storage**, **DR Transfer**, or **Restore** subtab. Each of these pages maps to a different Historical Report.
4. Specify the reporting parameters.



a. In the **Time** drop-down list, specify the time interval that you want to capture. Each time interval displays information in specific reporting increments.

Time Interval	Reporting Increment
Last 24 Hours	15 minutes
Last Week	2 hours
Last 3 Months	Daily
Last 24 Months	Weekly

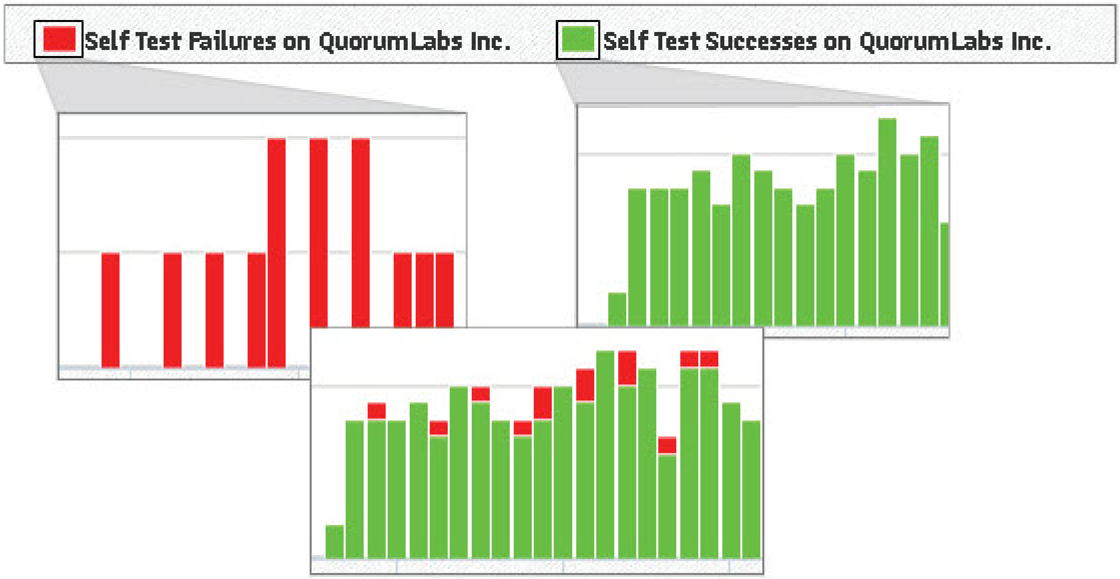
b. In the **Level** drop-down list, specify the entity on which you want to report:

Level	Displays data for...
Customer	All of a customer's onQ Appliances combined. For example, HA and DR. Customer is defined by **APPLIANCE CONFIG** > **ADVANCED** > **License** > **Customer** field.
Appliance	One specific onQ Appliance. The onQ Appliance is identified by **APPLIANCE CONFIG** > **HYPERVISOR** > **Hypervisor Name** field.
onQ	One specific onQ. In the case of a multi-tenant environment (**DASHBOARD** tab > **onQ STATUS** page > **Configuration** field), one onQ Appliance can have many onQs. The onQ is identified by the onQ Manager hostname (aka Manager hostname or onQ hostname) as shown in **DASHBOARD** tab > **onQ STATUS** page > **Manager hostname** field.
PN	One specific protected node.

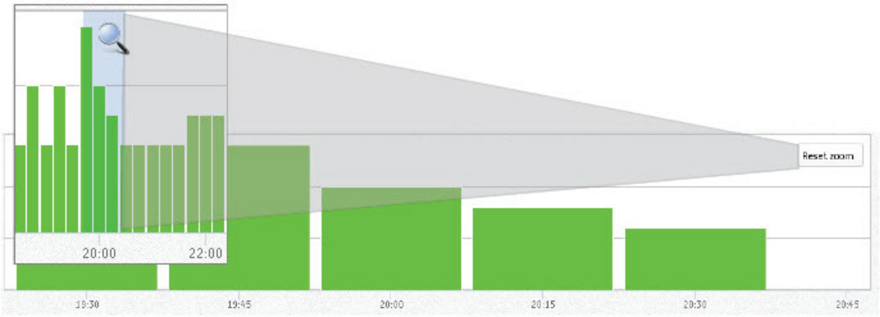
c. In the **Instances** drop-down list, select the specific Customer(s), Appliance(s), onQ(s), or PN(s) that you want included in your report.

5. Click **Update Chart**.
6. (Optional) Click on the Legend links within the report to include or exclude specific data (quantities). You can use this feature to compare data.

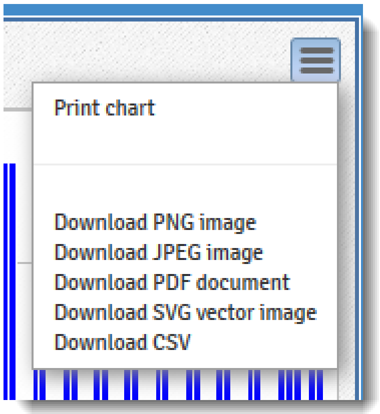
In some cases, you’ll need to exclude data (toggle between legend links) when there is a huge disparity in the quantities. For example, you cannot view the files restored and bytes restored simultaneously in the Restored Data Chart because the scale for number of restored bytes has a long range relative to the number of files restored thereby hiding the bar color for the files restored.


🟥 Self Test Failures on QuorumLabs Inc.
🟩 Self Test Successes on QuorumLabs Inc.

7. (Optional) Zoom in on a subset of data by highlighting a section of the timeline. Click the **Reset Zoom** button when you’re done to return to the entire report.



8. (Optional) Export the report. An export does not include zoom-in data.



12.3 Monitor protected nodes

From the onQ Portal you can quickly identify the connection status, protection status, and backup status of protected nodes (PNs).

Monitoring is particularly useful if you've started a PN or you recently upgraded a host.

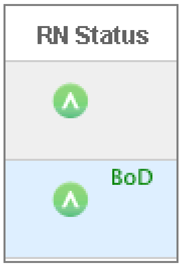
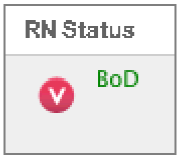
To monitor the status of a PN:

1. Log on to the HA's onQ Portal.
2. Go to **DASHBOARD** tab > **PROTECTED NODES** page.

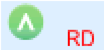
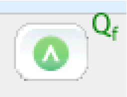
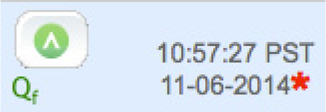
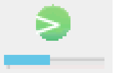
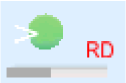
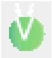
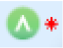
   A list of all your protected nodes and their current status appears:

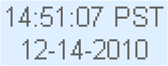
Connection Status	🔼 carat is green and white arrow points upward	PN is running and protection is turned on. Tooltip indicates `PN online` (agent-based) or `Proxy online` (agent-less). • (agent-based) the online state of the PN reflects the Power State of the PN. • (agent-less) the online state of the Proxy reflects the communication state of the PN proxy on the ESX Server.
	➖ carat is green with a yellow dash	For agent-less PNs, the PN proxy is currently being upgraded: 1. Before upgrade 🔼 : solid green carat; white arrow points upward. 2. During upgrade ➖ : solid green carat; yellow dash. 3. After upgrade 🔼 : solid green carat; white arrow points upward.
	🔽 carat is red and white arrow points downward	PN is not online. Tooltip indicates `PN offline` or `Proxy offline`. See (Agent-based PNs) Connection Problems or (Agent-less PNs) Connection and Backup Problems.
	🔼🔒	onQ Appliance's connection to PN is secure.
	🔽🔒	onQ Appliance's connection to PN is not secure. See "(Agent-based PNs) Connection Problems" on page 483.
Protected Node		Hostname of the protected node. Hostname is the same as the Windows hostname.
Type	**PN**	PN itself is running as opposed to the recovery node.
	RN ⚠	RN, not the protected node is running, implying that the primary node has failed or has been stopped and its recovery node equivalent has been started.

Protection Disabled	no check mark	Protection is enabled on this node.
	✓ check mark appears	Protection is disabled on this node. onQ has a built-in protection policy whereby it automatically disables backups if an HA’s repository disk space utilization exceeds 85% (see Schedule backups).

RN Status	⋀ carat is green and white arrow points upward	Recovery Node image of the Protected Node is available and ready to run. The acronym `BoD` appears next to the icon if `Auto RN Creation` (see (On-Site/Prime/Plus) Modify RN build policy) is set to disabled.  Mouse-over help displays a record of recent events for the RN.
	V carat is green and white arrow moves top to bottom	onQ is preparing the Recovery Node. Hover-over help indicates. `RN is not updated – RN is NOT Ready to Run`. 
	V carat is red and white arrow points downward	No Recovery Node is available. See Recovery Node Problems. The acronym `BoD` appears next to the icon if `Auto RN Creation` (see (On-Site/Prime/Plus) Modify RN build policy) is set to disabled.
	⌛ hourglass on a yellow background	Internal processing is occurring. Typically this icon persists for one to two minutes before changing to red or green.
	⋀ * carat is green, white arrow points upward, and is accompanied by a red asterisk	The Recovery Node is runnable, but not running, and has not been updated with the latest snapshot The RN is more than one snapshot behind the most recent snapshot in the Repository. Mouse-over text displays the snapshot that the RN is running. The red asterisk might appear in a normal backup cycle for a short period of time, after the new snapshot is created and before the update of the RN begins.

	▶* carat is green with right arrow and is accompanied by a red asterisk	The RN is running, but has not been updated with the latest snapshot. The RN is more than one snapshot behind the most recent snapshot in the Repository. Mouse-over text displays the snapshot that the RN is running.

Backup Status	 carat is green and white arrow points upward	Complete restorable backup exists in the repository. Hover-over help indicates `Idle, backup complete`. The date and time of the most recent completed backup appear to the right. The acronym `RD` appears next to the icon if replication (see Disable replication for individual nodes) is set to disabled. 
	 	The Qf icon indicates that the filter driver is enabled.
	 10:57:27 PST 11-06-2014*	The Qf icon indicates that the filter driver is enabled, but the red asterisk at the end of the Last Backup time indicates that onQ did not use the filter driver when performing the last successful backup. Due to problems with the logs, onQ resorts to using the Non-Filter backup method to correct the problem. The PN's Event Logs also confirm this proactive action. onQ uses Qfilter for the next backup and the red asterisk disappears. The Event Log shows the correct Qfilter state in the backup statistics.
	 carat is green and white arrow moves left to right	Backup is in progress. Hover-over help indicates `Running` or Backup. The acronym `RD` appears next to the icon if replication (see Disable replication for individual nodes) is set to disabled. 
	 carat is green and white arrow moves top to bottom	Transfer of the backup to the repository is in progress. Hover-over help indicates `Adding backup to repository`.
	 carat is green, white arrow points upward, and accompanied by a red asterisk	A valid snapshot exists, but the last backup attempt resulted in an error or the snapshot wasn't added to the repository.
	 carat is red and white arrow points downward	Not a single copy of a backup snapshot exists.

Next Scheduled Backup	 14:51:07 PST 12-14-2010 timestamp	Date and time of the next scheduled backup. Matches the output in the corresponding log entry: Backup next schedule =”nxt_<pnName>:<timeStamp>:<timeStamp>”.

Backup Transfer Margin

● solid green icon

Backup margin is within an acceptable range. Backup margin indicates how well PN backups are keeping up with the backup interval as calculated by averaging the minimum, average, and maximum intervals from the previous 24 hours. This 24-hr time period automatically resets each time you restart protection.

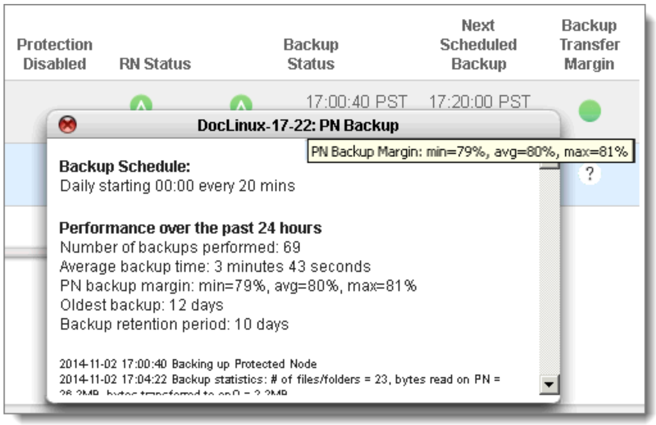
Backup margin is the amount of free time between the completion of one backup and the start of the next. Backup margin uses three inputs from the Event Log to calculate the minimum (min), average (avg), and maximum (max) margins that display when you mouse-over the Backup Margin icon.

- `Backing up Protected Node` = Backup start time
- `Backup complete` = Backup end time
- `Next Backup scheduled for` *`timeStamp`* = Next Scheduled Backup

In other words:

```
Backup margin = (100 - (100 *
((endTime-
startTime)/nextScheduledBackup-
startTime)))
```

So, as the backup takes longer, the backup margin decreases. Incremental backups take longer when the PN performs continuous database updates. Hover-over help displays more information:



Protection Disabled	RN Status	Backup Status	Next Scheduled Backup	Backup Transfer Margin
			17:00:40 PST	17:20:00 PST

DocLinux-17-22: PN Backup

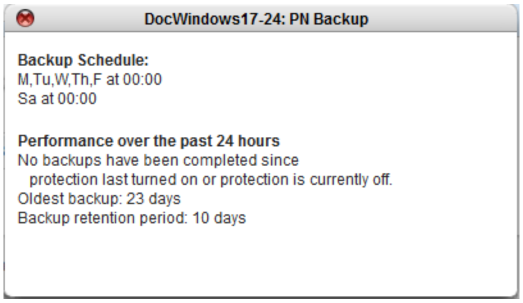
PN Backup Margin: min=79%, avg=80%, max=81%

Backup Schedule:
Daily starting 00:00 every 20 mins

Performance over the past 24 hours
Number of backups performed: 69
Average backup time: 3 minutes 43 seconds
PN backup margin: min=79%, avg=80%, max=81%
Oldest backup: 12 days
Backup retention period: 10 days

```
2014-11-02 17:00:40 Backing up Protected Node
2014-11-02 17:04:22 Backup statistics: # of files/folders = 23, bytes read on PN =
```

For aggregate data on backup transfers, see the DR Transfer page header.

Backup Transfer Margin (Contd)	● solid yellow icon	Backups transfers are not within an ideal range—the backup margin *average* is below 35%. Modify the backup interval.
	● solid red icon	Backups transfers are not within an acceptable range—the backup margin *average* is below 10%. Modify the backup interval.
	● solid grey icon	The PN was configured with replication disabled. Mouse-over help indicates `DR Transfer Margin: N/A` and `DR Replication Disabled`. Tooltip dialog’s title read `Replication Disabled`.
	? white icon with question mark	Backup margin is not applicable because no backups have been performed in the last 24 hours. Also displays if protection is off or if backup or DR transfer has not been completed since you turned on protection.  DocWindows17-24: PN Backup **Backup Schedule:** M,Tu,W,Th,F at 00:00 Sa at 00:00 **Performance over the past 24 hours** No backups have been completed since protection last turned on or protection is currently off. Oldest backup: 23 days Backup retention period: 10 days
Disk Usage	3 %	Percentage disk usage of entire onQ Appliance, and includes any recovery nodes that are running.

Related Topics

Monitor recovery nodes
Monitor backups
Generate on-demand reports

12.4 Monitor recovery nodes

Each of your primary protected nodes has a corresponding recovery node. The HA constructs a recovery node after each periodic backup.

The recovery node is then ready to be started as a replacement for the primary if the protected node fails. Even after you have started a recovery node, backups continue on the HA.

If the RN has been started and is running in production mode, it effectively becomes a PN; the RN, not the PN, is being backed up by the HA Appliance.

In the event that a protected node fails, you need to start the corresponding HA recovery node. Similarly, if there's an HA recovery node failure or HA failure, you need to start the recovery node on the DR Appliance. In both cases, you'll want to monitor the progress of these recovery nodes. Of course, in the event of a disaster, you'll receive alerts.

To view the status of a recovery node:

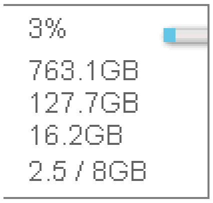
1. Log on to either the HA's onQ Portal or the DR Appliance's onQ Portal.
2. Go to **DASHBOARD** tab > **RECOVERY NODES** page.

   You see a list of all the recovery nodes and their current status.
3. Locate the recovery node(s).

   Each row in the list represents the recovery node corresponding to a protected node:

Recovery Node		Hostname of the protected node to which this recovery node belongs.
Auto RN Creation	no check mark	Recovery node creation policy is set to On Demand.
	✓ check mark appears	Recovery node creation policy is set to Ready-to-Run.
Space Required	2%	Disk space required to run the recovery node.

Power State	⌃ carat is green and points upward	Recovery node is running and protection is on. Tooltip indicates `RN VM Running`. An agent-less PN is backed up using a PN proxy and the Power State of that PN proxy is detected using the power state of the VM on the ESX Server.
	⌄ carat is red and points downward	Recovery node is not running. Tooltip indicates one of the following: • `RN VM exists but Not Running` – the RN was stopped but not removed and thus the virtual machine exists but is not running. • `RN VM Not Running` – the RN virtual machine was removed or never created.
	⌃ carat is yellow and points upward	Recovery node is starting.
	⌄ carat is yellow and points downward	Running recovery node is shutting down
	⏳ hourglass on a yellow background	Startup dependencies are being evaluated.
Test Mode	no check mark appears	Backup is running in production mode.
	✓ check mark appears	Backup is running in test mode.

Startup Time		When (date and time) the running recovery node was started.
CPU Utilization	field is blank	Recovery node is not running.
	 2% field is not blank	Recovery node is running. Percentage of the onQ Appliance’s allotted CPU used by this recovery node.
Console	🖥	Recovery node is running. The icon launches the recovery node’s operating system’s console.
Appliance CPU Load	 3 %	Percentage of onQ’s CPU usage.
RN Disk Space Available	 3% 763.1GB 127.7GB 16.2GB 2.5 / 8GB	Total amount of disk space available for RNs. See also Monitor disk space and memory usage.
RN Disk Space Allocated		Total amount of disk space allocated for RNs. See also Monitor disk space and memory usage.
RN Disk Space Used		Total amount of disk space used by RNs. See also Monitor disk space and memory usage.
RN Memory Available		Total amount of memory available to RNs. See also Monitor disk space and memory usage.

Related Topics

Monitor protected nodes

Generate on-demand reports

12.5 Monitor backups

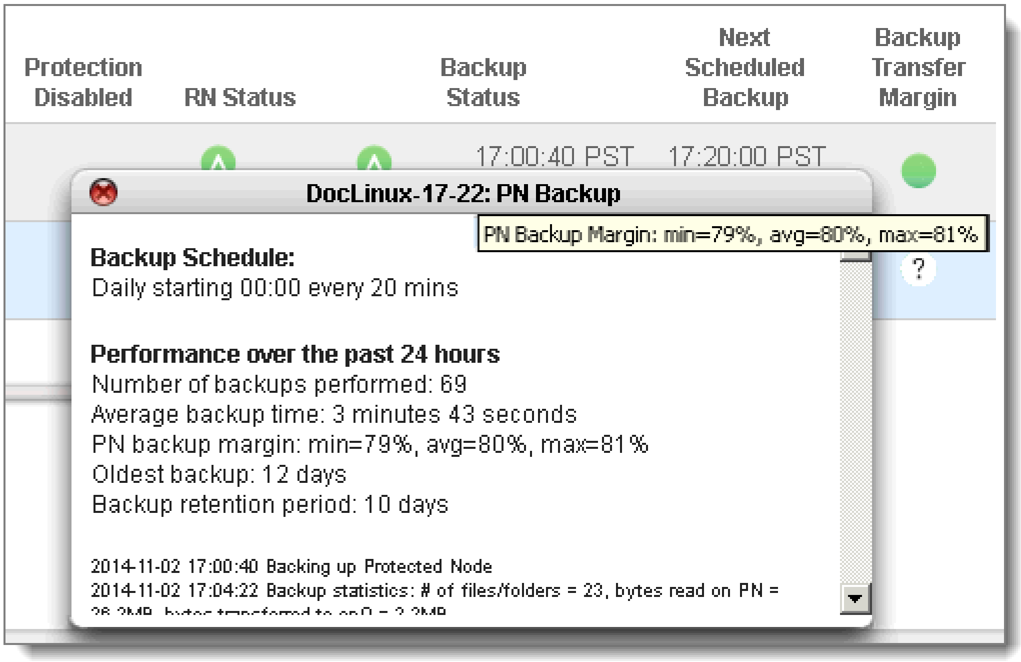
onQ Manager provides two main tools to help you monitor your backups:

- Backup Transfer Margin
- Event Log
- Backup Activity Report
- Alerts

From a protected node's dashboard, you can get insight into backup margin and transfer margin for that protected node's backups. The backup transfer margin icons indicate how well backups and DR transfers are keeping up with the backup interval.

In the event that the interval isn't met, the Event Log indicates `scheduled backup request for <pn_name> occurred before previous backup completed`....In this case, increase your interval time so as to avoid this scenario.

If you want to see recent backup events for individual recovery nodes, simply mouse-over the recovery node on either the HA or the DR Appliance:



Backup Schedule:
Daily starting 00:00 every 20 mins

Performance over the past 24 hours
Number of backups performed: 69
Average backup time: 3 minutes 43 seconds
PN backup margin: min=79%, avg=80%, max=81%
Oldest backup: 12 days
Backup retention period: 10 days

```
2014-11-02 17:00:40 Backing up Protected Node
2014-11-02 17:04:22 Backup statistics: # of files/folders = 23, bytes read on PN =
26.2MB, bytes transferred to onQ = 2.2MB
```

Lastly, be sure to browse the Backup Activity Report on a regular basis and all critical alerts.

Related Topics

Initial Backup
Backup Activity Report
Generate on-demand reports

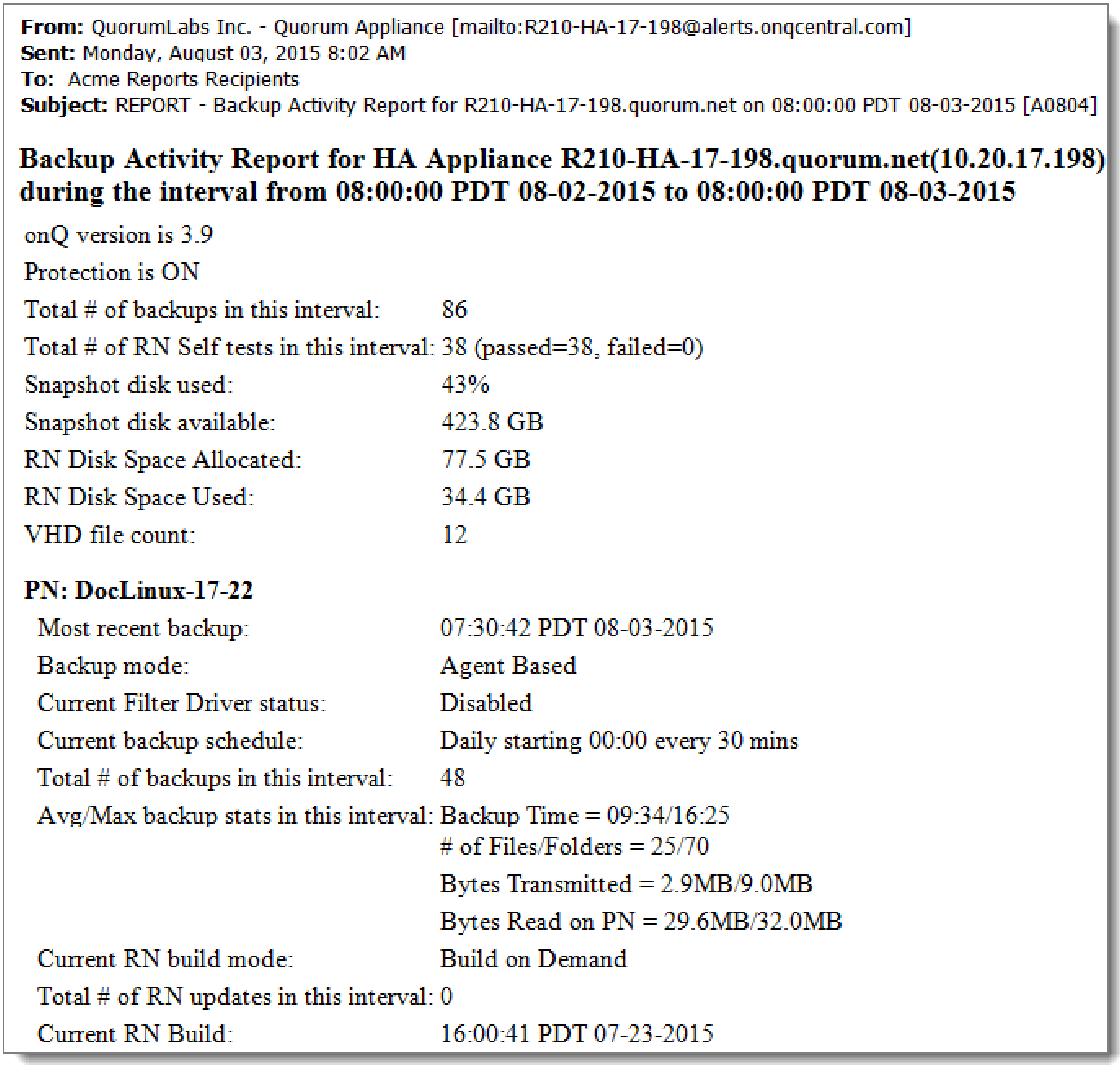
12.6 Backup Activity Report

onQ emails you a Backup Activity Report on a daily basis. If you are not receiving this report, ensure that you have alerts enabled and that your email program is not sending the emails to your SPAM folder.

The Backup Activity Report lists:

- The total number of backups that completed for the day for each protected node and a timestamp for the most recent backup.
- Statistics on the amount of disk space that remains on the Vdisk.

- Status of each PN’s Self Test.



From: QuorumLabs Inc. - Quorum Appliance [mailto:R210-HA-17-198@alerts.onqcentral.com]
Sent: Monday, August 03, 2015 8:02 AM
To: Acme Reports Recipients
Subject: REPORT - Backup Activity Report for R210-HA-17-198.quorum.net on 08:00:00 PDT 08-03-2015 [A0804]

Backup Activity Report for HA Appliance R210-HA-17-198.quorum.net(10.20.17.198) during the interval from 08:00:00 PDT 08-02-2015 to 08:00:00 PDT 08-03-2015

onQ version is 3.9	
Protection is ON	
Total # of backups in this interval:	86
Total # of RN Self tests in this interval:	38 (passed=38, failed=0)
Snapshot disk used:	43%
Snapshot disk available:	423.8 GB
RN Disk Space Allocated:	77.5 GB
RN Disk Space Used:	34.4 GB
VHD file count:	12

PN: DocLinux-17-22

Most recent backup:	07:30:42 PDT 08-03-2015
Backup mode:	Agent Based
Current Filter Driver status:	Disabled
Current backup schedule:	Daily starting 00:00 every 30 mins
Total # of backups in this interval:	48
Avg/Max backup stats in this interval:	Backup Time = 09:34/16:25 # of Files/Folders = 25/70 Bytes Transmitted = 2.9MB/9.0MB Bytes Read on PN = 29.6MB/32.0MB
Current RN build mode:	Build on Demand
Total # of RN updates in this interval:	0
Current RN Build:	16:00:41 PDT 07-23-2015

If the Backup Activity Report shows failures, generate the applicable logs to get more information. For example, if a Self Test failed, generate the Self Test Log for the specified time period.

Moreover, the Backup Activity Report has attachments that provide you additional information.

- Backup Statistics Report (`BackupStats.csv`) – byte information for all transfers.
- Alert Activity Report (`Alerts.csv`) – summary of all alerts sent by onQ Central.
- PN Health Report (`Health.txt`) – data to help debug the PN and predict when a given PN will exceed disk space and VSS limits. This report will not appear as an attachment if the report is empty. Also, if your onQ is not configured to send this report to onQ Central, Quorum Support might request it in an effort to debug PN issues. This report is not currently available for agent-less PNs.

Related Topics

Resize protected node's vdisk
About Alerts
Modify e-mail alert settings

12.7 Monitor DR Appliance

Managing disaster recovery with the DR Appliance is slightly different from managing high availability, but just as simple.

The main function of the DR Appliance is to accept PN snapshots from the HA, vet them, save them to the DR Appliance, and load the most recent snapshot when the DR recovery node is needed.

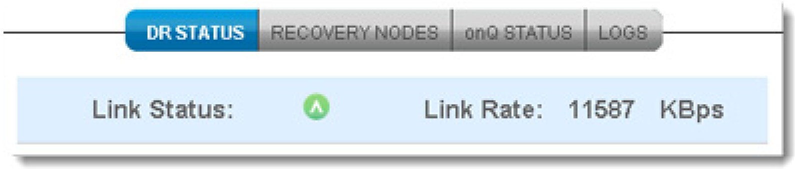
To monitor from the DR Appliance:

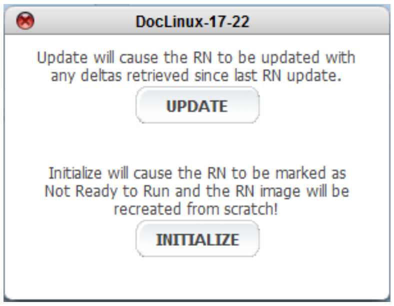
In a nutshell, ensure that:

- the connection between the two onQ Appliance is active.
- each RN's Last Update Time equals the corresponding PN's Backup Status. If not, the RNs and corresponding PNs may be out of sync because (1) The transfer of snapshots from HA to DR paused for some reason, or (2) RNs are not being updated on the DR Appliance.
- there's enough disk space to store the snapshots.

1. Log on to the DR Appliance's onQ Portal.
2. Go to **DASHBOARD** tab > **DR STATUS** page.

3. Observe the following:

Link Status	▲ green carat points upward	WAN/VPN connection to the companion HA is up.
	▼ red carat points downward	WAN/VPN connection to the companion HA is down.
	● solid yellow icon	Usually indicates that Protection is turned off.
	 Link Status: ▲ Link Rate: 11587 KBps	
Link Rate		Available bandwidth (in kbps) of WAN/VPN connection to the companion HA.
RN Name		Hostname of the recovery node. In most cases this hostname is the same as the protected node's hostname. onQ assembles this list of recovery nodes from backup data received from the HA.
Protection Disabled on HA	no check mark	Protection is enabled on this node.
	✓ check mark appears	Protection is disabled on this node.

RN Ready Status	^ green carat points upward	Recovery node is ready.
	^ * green carat points upward and accompanies red asterisk	Recovery node is ready, but it has an `OUT OF DATE RN Template`. You have two choices:  DocLinux-17-22 Update will cause the RN to be updated with any deltas retrieved since last RN update. UPDATE Initialize will cause the RN to be marked as Not Ready to Run and the RN image will be recreated from scratch! INITIALIZE
	v red carat points downward	Recovery node is not ready.

RN Running Status	⌃ green carat points upward	Recovery node is running and protection is turned on. Tooltip indicates `RN VM Running`.
	⌄ red carat points downward	Recovery node is not running and protection is turned off. Tooltip indicates one of the following: • `RN VM exists but Not Running` – the RN was stopped but not removed and thus the virtual machine exists but is not running. • `RN VM Not Running` – the RN virtual machine was removed or never created.
	⌛ hourglass with yellow background	In production mode, this icon occurs when startup dependencies have been defined for an RN and the RN is being started as part of a group or using the **Start all RNs** button.

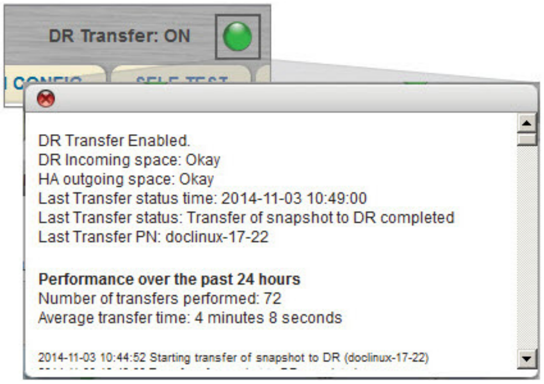
Test Mode	no check mark appears	Backup is running in production mode.
	✓ check mark appears	Backup is running in test mode.
Last Update Time		Last protected node snapshot taken from the DR Repository. RN’s Last Update Time must equal the corresponding PN’s Backup Status; otherwise the Appliances are not synchronized.
Disk Usage		Percentage disk usage of entire onQ Appliance, and includes any recovery nodes that are running. To see the files that are consuming this space, go to the DR Repository (click on the **RETRIEVAL** tab).

To monitor from the HA:

The HA’s onQ Portal has header information that provides information about DR transfers, the HA-DR communication link, and DR disk space.

1. Log on to the HA’s onQ Portal.
2. Go to the **DASHBOARD** tab.
3. Observe the **DR Transfer** status in the page header.

Mouse-over the status icon to view transfer statistics:.

🟢 solid green icon	ON	DR transfers are enabled and the link between the HA and the DR is good. Also, the last transfer, if any, completed successfully.  DR Transfer Enabled. DR Incoming space: Okay HA outgoing space: Okay Last Transfer status time: 2014-11-03 10:49:00 Last Transfer status: Transfer of snapshot to DR completed Last Transfer PN: doclinux-17-22 **Performance over the past 24 hours** Number of transfers performed: 72 Average transfer time: 4 minutes 8 seconds 2014-11-03 10:44:52 Starting transfer of snapshot to DR (doclinux-17-22)
🔴 solid red	OFF	DR transfers are disabled.
🔴 solid red	ERR	Either of the following: • the DR returned a link error. • the last transfer to the DR resulted in an error. • protection is off, but starting up. • the disk space on HA for storing outgoing transfers to DR is critically low.

🟡 solid yellow icon	ERR	The disk space on the DR for storing incoming transfers from HA is critically low.
? solid yellow icon with question mark	?	onQ is unable to retrieve status information. This status can appear when: • Screen first loads. • Protection is off. • Software mismatch. In this case, hover-over help indicates `Version Mismatch`. See also A0014 and A0015.
! solid yellow with exclamation	WARN	The disk space on the DR for storing incoming transfers from HA is low, or the disk space on HA for storing outgoing transfers to DR is low. This status can also occur if onQ is unable to communicate with the DR.
	XFER, followed by an hour glass (⌛)	A transfer to the DR is underway. This status might not be displayed for all transfers if the transfer is under 30 seconds and the refresh of the status display occurs between transfers.

Related Topics

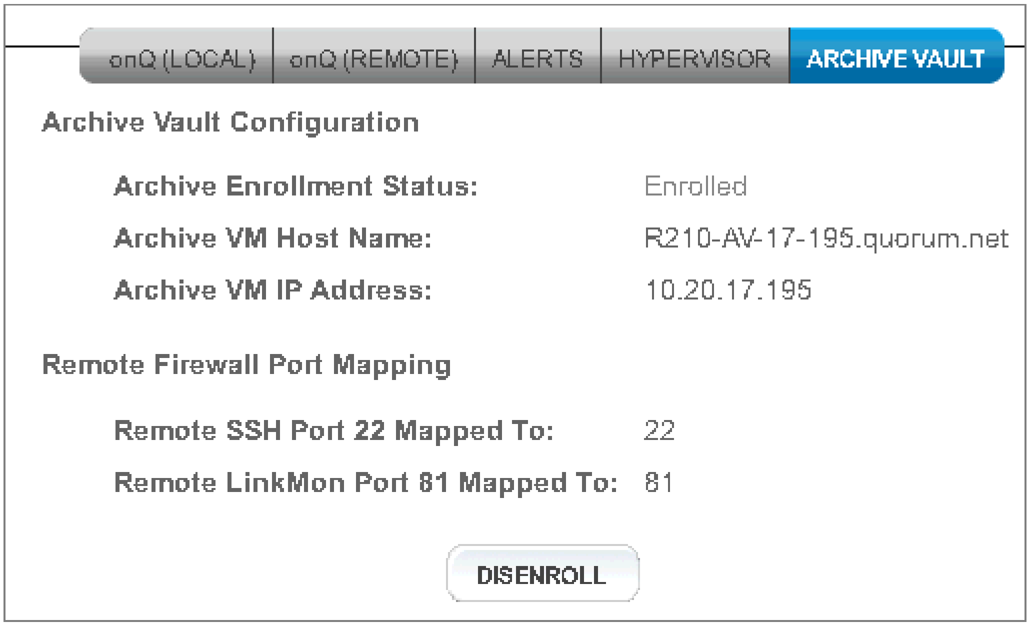
Monitor backups

Disable replication globally

12.8 Monitor onQ Archive Vault enrollment

After you set up the trust relationship between the onQ Appliance and the onQ Archive Vault (see AV online help for instructions), your onQ Appliance's onQ Portal displays an enrollment status for the AV: the **Enroll** button reads

`Disenroll`, and the **Archive Enrollment Status** is `Enrolled`:



Archive Vault Configuration

Archive Enrollment Status: Enrolled

Archive VM Host Name: R210-AV-17-195.quorum.net

Archive VM IP Address: 10.20.17.195

Remote Firewall Port Mapping

Remote SSH Port 22 Mapped To: 22

Remote LinkMon Port 81 Mapped To: 81

To verify enrollment status:

1. Log on to the onQ Appliance’s onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ARCHIVE VAULT** page.

   If the onQ is enrolled on the onQ Archive Vault for archiving, then the **Archive Enrollment Status** indicates `Enrolled`.

Related Topics

Enroll and Disenroll onQ Archive Vault

12.9 Monitor disk space and memory usage

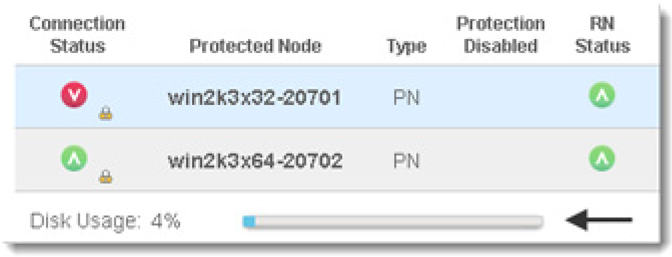
onQ can report on the disk usage of the onQ Appliance’s Repository and disk and memory usage of recovery nodes through the onQ Portal as outlined below, or through the onQ Monitor as outlined in Monitor multiple onQ Appliances.

When the onQ Appliance was pre-configured, a specific amount of disk space was allocated to the Repository for snapshots. You cannot change this allocation.

To determine disk space usage of *protected nodes*:

1. Log on to the HA's onQ Portal.
2. Go to **DASHBOARD** tab > **PROTECTED NODES** page.

   A **Disk Usage** bar appears toward the bottom of the page. This bar shows the percentage disk usage on onQ, in two ways: a percentage figure and a corresponding bar graph.



Connection Status	Protected Node	Type	Protection Disabled	RN Status
V 🔒	win2k3x32-20701	PN		Λ
Λ 🔒	win2k3x64-20702	PN		Λ

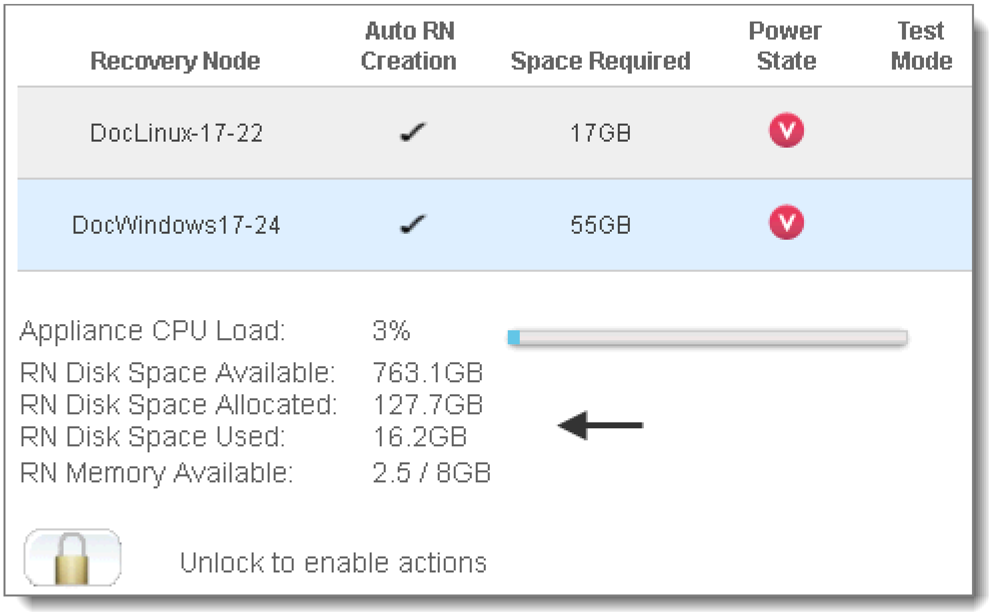
Disk Usage: 4%

   Disk usage is calculated based on the disk usage of all the protected nodes that are running.

To determine disk space usage of *recovery nodes*:

1. Log on to the HA's onQ Portal.
2. Go to **DASHBOARD** tab > **RECOVERY NODES** page.

Statistics appears toward the bottom of the page..



Recovery Node	Auto RN Creation	Space Required	Power State	Test Mode
DocLinux-17-22	✓	17GB	V	
DocWindows17-24	✓	55GB	V	

Appliance CPU Load: 3%

RN Disk Space Available: 763.1GB

RN Disk Space Allocated: 127.7GB

RN Disk Space Used: 16.2GB

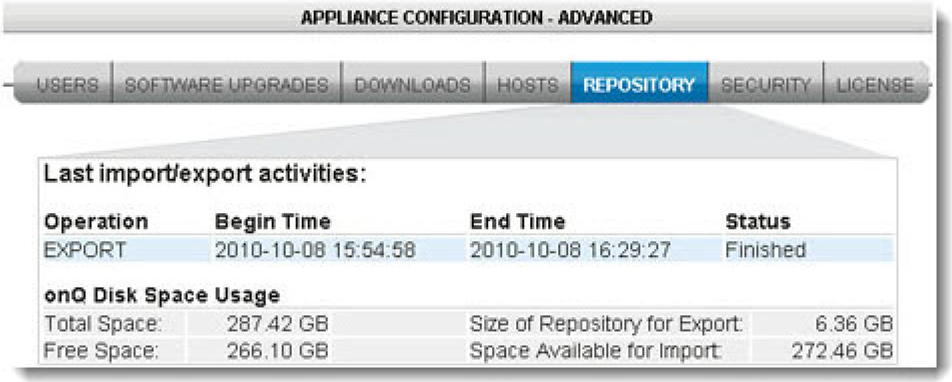
RN Memory Available: 2.5 / 8GB

Unlock to enable actions

To determine disk space available to the *Repository*:

1. Log on to either the HA Appliance's onQ Portal or the DR Appliance's onQ Portal.
2. Go to **APPLIANCE CONFIG** > **ADVANCED** button > **REPOSITORY** page.

   Free Space indicates the amount of space that the Repository can grow.



Last import/export activities:

Operation	Begin Time	End Time	Status
EXPORT	2010-10-08 15:54:58	2010-10-08 16:29:27	Finished

onQ Disk Space Usage

Total Space:	287.42 GB	Size of Repository for Export:	6.36 GB
Free Space:	266.10 GB	Space Available for Import:	272.46 GB

Related Topics

Initial Backup
Seed the DR Repository

12.10 About Alerts

The onQ Manager sends alerts if it detects possible system issues (for example, if a protected node or an incremental snapshot fails). This topic includes the most common alerts that require your attention.

These alerts can be critical or informational only, and Quorum has assigned each alert a preconfigured delivery policy. A summary of alert activity is available in the Backup Activity Report as an attachment.

> **Note:** If recovery is required, you can start any or all of the recovery nodes. The backup and replication process continues after recovery, based on the recovery nodes and not the original protected nodes.

12.11 Modify e-mail alert settings

onQ sends alerts if it detects possible system failures. To receive such alerts, you must configure the onQ Appliance to send those alerts.

As your alert delivery mechanism, you can specify either onQ Central, which only requires port 443 access to the internet, or e-mail, which requires a SMTP server and, optional credentials.

To modify alert settings:

1. Log on to either the HA Appliance's onQ Portal or the DR Appliance's onQ PortalArchive Vault Portal.
2. Go to **APPLIANCE CONFIG** tab > **ALERTS** page.
3. Click **MODIFY**.
4. In the **Alert Delivery Configuration** pane, do the following:
   a. Select one of the following mechanisms to deliver your alerts.
      - **(Recommended) onQ Central** — Use this option if you want the Appliance to send alerts to onQ Central, Quorum's support management system, in addition to the recipients that you specify. This option provides Quorum Support information about your Appliance as it relates to those alerts, enabling Quorum Support to better respond to potential issues with your Appliance. This option requires that you open outbound port 443 on your firewall.
      - **email** — Use this option if you want the onQ virtual machine to send alerts to use your company's mail server to the recipients that you specify. Specify your company's email server and, optionally, the credentials for authenticating with that server. Ensure that port 25 is open on that mail server.

   b. In the **Daily Report Time** field, specify when you want the report to begin capturing data for the Backup Activity Report. This time is a 24-hr period, and defaults to 8pm.
5. In the **Alert distribution lists** pane, type a comma-separated or space-separated list of email addresses for the recipients:
   - **Reports**. Recipients for the Backup Activity Report.
   - **Notify Alerts**. Recipients for all the notification alerts.
   - **Critical Alerts**. Recipients for all the critical alerts.

6. Click each **Test** button to test your email settings. This test sends a sample email to the recipients that you specified in Step 5.
   - If onQ Central is your delivery mechanism and you don’t receive the test email, ensure that port 443 is open on your firewall. In this case, onQ is saving the alerts to its alert queue. onQ will send these alerts after you configure your firewall correctly.
   - If the onQ virtual machine’s delivery mechanism is to an email server (SMTP relay host) such as your company’s email server, and you don’t receive the test email, ensure that port 25 of that mail server is open to the onQ virtual machine.

12.12 Retrieve logs

Logs provide a convenient record of internal activity (events) on the Appliance. Logs can serve as a useful means of monitoring, compliance reporting, and, if necessary, troubleshooting the onQ Appliance. The log you want to retrieve depends on the activity or component you’re trying to monitor or audit.

To retrieve a log:

You can either view or download a given log. You can also use the log filters to view specific data, then export that data to a text file.

1. Log on to either the HA Appliance’s onQ Portal or the DR Appliance’s onQ Portal.
2. Go to **DASHBOARD** tab > **LOGS** page.

   You see a page similar to the following:
3. From the **Log Type** drop-down list choose one of the following:
   - Event Log — a log of current and past events, listed in alphabetical order by hostname, for all recovery nodes. Use the **Display only errors** check box to generate a log that only includes events that result in failures or errors. This log has no expiration.
   - Event DB Log — a log of database events internal to the Appliance. These events have severity levels. This log is for

Quorum Support use only.

- Expired Snapshot Log — a log that lists the snapshots and corresponding Protected Nodes that onQ expired and the reason for the expiration. onQ expires snapshots because of a predefined retention policy or critically low disk space.
- FLR Activity Log — a log of file-level restores initiated from the onQ Appliance. The report lists the user that initiated the restore, the time the restore started and completed, the status of the restore, the files and folders that were restored, the source (snapshot), and the machine (PN name or IP address) to which the objects were restored.
- HA --> DR Transfer Log — a log of HA to DR data transfer statistics. The transfer log report includes Protected Node name, start and end times, size of data transferred, and the rate of transfer for each snapshot. The transfer rate is an average, and is calculated based on start/stop times and the size in the log entry.
- Manager Debug Log — a log of debug reports initiated by Quorum. This log is for Quorum Support use only.
- PN Configuration — a report of all the configuration data that is listed in the Protection Config menus, including advanced settings, backup include/exclude lists, startup dependencies, and RN services. This report is often used for compliance reporting. The data is listed by PN, setting, and setting value.
- Self Test Log — a log that shows the results of your RN testing.
- Upgrade Log — a log of all onQ software upgrades for a selected period of time. The report lists the date, time, and the software packages installed on to onQ.
- WSR Activity Log — a log of all Windows Share Restore activity initiated from the Appliance. The report lists the browsing history, file objects accessed, time of access, and the client machine address from which the WSR was initiated.

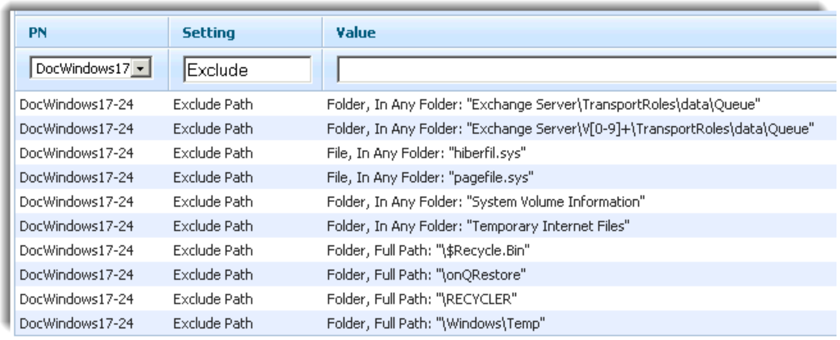
4. Specify a single PN or all PNs, if applicable.

5. Specify a time range for the data you want to display by specifying the start and end dates, if applicable.

6. Do one of the following:
   - Click **VIEW LOG** to see the information displayed.
   - Click **DOWNLOAD LOG** to download the log to a file on your local computer.

7. (Optional) Use the log filters to include or exclude specific information, then **Save** the filtered data to a text file.

   If you have a browser older than IE 10, this **Save** button doesn't appear. Use the **DOWNLOAD LOG** button instead.



PN	Setting	Value
DocWindows17 ▾	Exclude	
DocWindows17-24	Exclude Path	Folder, In Any Folder: "Exchange Server\TransportRoles\data\Queue"
DocWindows17-24	Exclude Path	Folder, In Any Folder: "Exchange Server\V[0-9]+\TransportRoles\data\Queue"
DocWindows17-24	Exclude Path	File, In Any Folder: "hiberfil.sys"
DocWindows17-24	Exclude Path	File, In Any Folder: "pagefile.sys"
DocWindows17-24	Exclude Path	Folder, In Any Folder: "System Volume Information"
DocWindows17-24	Exclude Path	Folder, In Any Folder: "Temporary Internet Files"
DocWindows17-24	Exclude Path	Folder, Full Path: "\$Recycle.Bin"
DocWindows17-24	Exclude Path	Folder, Full Path: "\onQRestore"
DocWindows17-24	Exclude Path	Folder, Full Path: "\RECYCLER"
DocWindows17-24	Exclude Path	Folder, Full Path: "\Windows\Temp"

13

Troubleshooting

13.1 Deployment Problems

Use the following table to help you troubleshoot installation problems as reported by the onQ Portal.

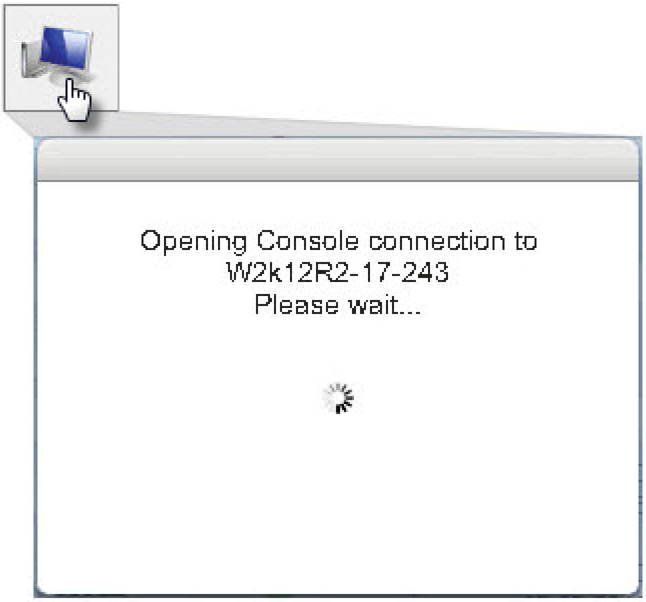
Symptom	Possible Cause	Solution
I see a `Browser and onQ are not on the same network` message	This message means that the PN and HA are on different subnets. This configuration is okay.	If you intend for them to be on different subnets, ignore this message. This message is just a reminder.
(applies to agent-based PNs only) I don't see the **Protect Me** button.	The following conditions must be met before the **Protect Me** button is visible: • The onQ Appliance must have been initially configured. • The PN's operating system must be supported by onQ. • Protection must be turned **OFF**.	Verify that the conditions are met. For os support, go to "Platform Support" in onQ Release Notes.

13.2 RN Console Mouse Problems

On Windows Server 2012 R2, it is possible that the mouse may not work when an agent-based or agent-less RN is running in test mode or production mode when launched via the RN's VNC console.

To work around this issue:

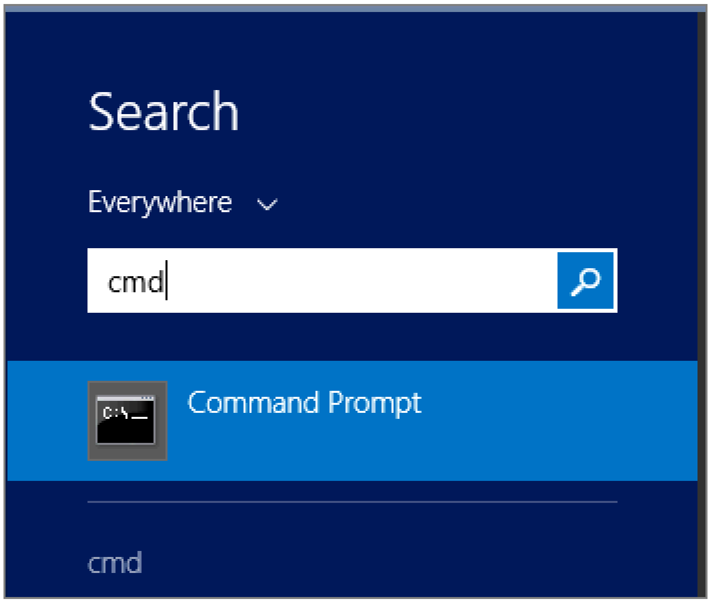
1. Power on the RN in test or production mode: **DASHBOARD** > **RECOVERY NODES** tab > **Power State** button. Wait for the RN to come up.
2. From the **RECOVERY NODES** tab launch the VNC console in a separate tab in your browser:



Opening Console connection to
W2k12R2-17-243
Please wait...

3. Use a Quorum-provided script to disable and re-enable Intel(R2) 82371SB PCI to USB Host Controller.
   a. In the VNC console that you launched in Step 2, click the **Send Ctrl-Alt-Del** button and log on at the prompt.

b. Press the **Send Ctrl-Esc** button in the upper right corner and type **cmd**, which will type **cmd** in the **Search Everywhere** drop-down box. Press **Enter** to launch a command prompt.



c. Run the batch file by typing the following commands:

```
> cd C:\Program Files\Quorum\QuorumDCRM-NODE
> restartIntelUSBController.bat
```

After the Intel(R2) 82371SB PCI to USB Host Controller drivers are working, the mouse should work.

4. If mouse does not work or the RN hangs, shut down and restart the RN. If the mouse still does not work, repeat Step 1 thru Step 3.

If this workaround procedure does not work, Quorum recommends that you protect a Windows (any supported version other than Windows 2012 R2) client machine and power on the RN for that client. Later run the console via the Recovery Nodes tab for that RN client and RDP to the problematic Windows 2012 R2 server RN that did not display the mouse. "RDPing" from the Windows RN client to the Windows 2012 R2 server RN guarantees a mouse presence in the Windows 2012R2 server RN.

Related Topics

Launch recovery node's console

13.3 (Agent-based Enrollment) Protected Node Enrollment Problems

If you receive errors *during* the enrollment process, browse the troubleshooting in (Agent-based Windows Enrollment) Problems Before Enrollment.

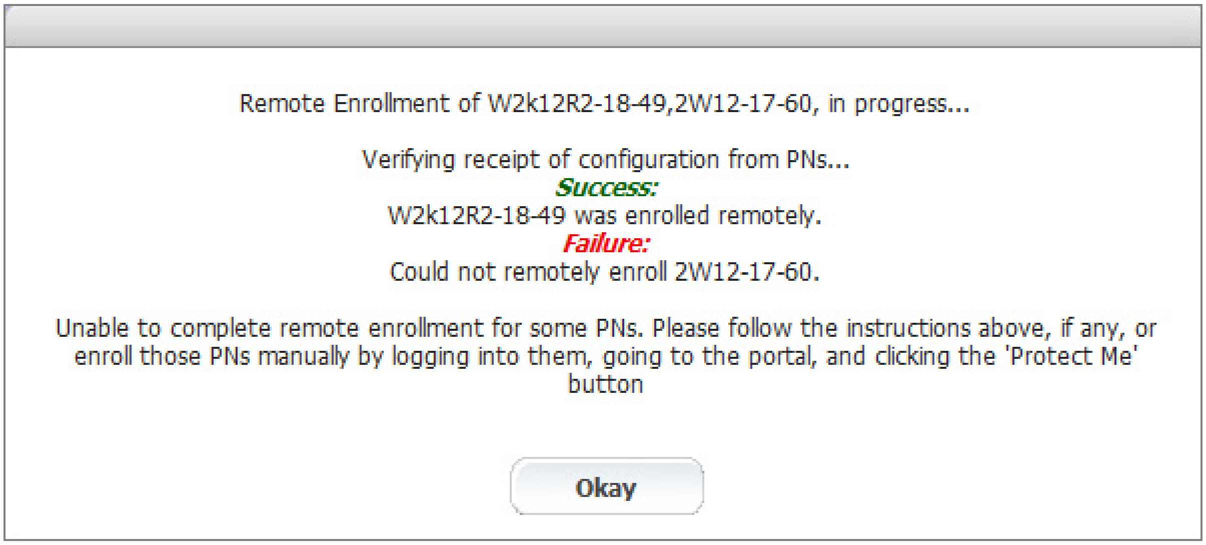
If onQ fails to enroll the PN and if instructed to do so by Quorum Support, ssh to the onQ and observe the messages in the most recent `/tmp/enrollstatus.log`.

Related Topics

(Agent-based PNs) Connection Problems

13.4 (Centralized Enrollment) Protected Node Enrollment Problems

If onQ fails to enroll a given PN as shown below, simply follow the instructions in the dialog. .



Remote Enrollment of W2k12R2-18-49,2W12-17-60, in progress...

Verifying receipt of configuration from PNs...
Success:
W2k12R2-18-49 was enrolled remotely.
Failure:
Could not remotely enroll 2W12-17-60.

Unable to complete remote enrollment for some PNs. Please follow the instructions above, if any, or enroll those PNs manually by logging into them, going to the portal, and clicking the 'Protect Me' button

If onQ fails to enroll the PN and if instructed to do so by Quorum Support, ssh to the onQ and observe the messages in the most recent `/tmp/centralized_enrollment.log`.

Related Topics

(Agent-based PNs) Connection Problems

13.5 Upgrade Problems

Use the following table to troubleshoot problems with your onQ Appliances or Protected Nodes (PNs) during or following an upgrade.

Symptom	Possible Cause	Solution
When you try to upgrade an onQ Appliance, the upgrade process pauses or hangs. The Updates icon 🔄 at the bottom of the onQ Portal page does not disappear.	Upgrade process fails to exit one of the system/platform upgrade modules such as PHP, Apache, or mysql.	Reboot the onQ, then click the **Install Updates** button to resume the upgrade.

Symptom	Possible Cause	Solution
(Agent-based PNs only) You see the following error during a PN upgrade and following an onQ upgrade and protection restart: `Error updating service on many 2003 PNs (msi: code 800b0101)`	The global root certificate on your Windows PN is invalid or expired. The upgrade is not the cause; moreover, any industry software upgrade requires a valid global root certificate.	Do the following: 1. Install a new global root certificate on the PN from https://support.globalsign.com/customer/portal/articles/1426602-globalsign-root-certificates. 2. Perform a Windows update.
You receive one of the mismatch errors outlined in License Expiration and Upgrade Alerts and onQ Portal's DR Transfer status indicates mismatch.	Each of the onQ Appliances listed is running different software versions. They must be in sync.	Compare the versions between the onQ Appliances, then resolve the incompatibility by upgrading each onQ Appliance to the same version level.
(Agent-based PNs only) PN did not upgrade, as defined in (Agent-based PNs) Verify PN software compatibility, although the PN is `online`.	Firewall or Anti-virus software could be blocking upgrades.	Add the exceptions outlined in Network and Firewall Requirements.
(Agent-based PNs only) PN did not upgrade, as defined in (Agent-based PNs) Verify PN software compatibility, and the PN is `offline`.	Various reasons.	See (Agent-based PNs) Connection Problems

Related Topics

PN Status Alerts

License Expiration and Upgrade Alerts

(Agent-based PNs) Connection Problems

(Agent-less PNs) Connection and Backup Problems

13.6 BMR Problems

Use the following table to help you troubleshoot PN problems after performing a BMR. If you are receiving errors from the BMR wizard itself, go to (Step 4) To interpret QUARK errors:.

Symptom	Possible Cause	Solution
PN will not boot and results in a BSOD (Blue Screen Of Death).	You might be trying to restore a XenTools 6.0.2-based RN image onto a virtual machine with XenServer 6.1 or later.	Modify the restored PN's vm `device_id` parameter to `0001` so that XenServer 6.1 or later host presents the disk properly to the operating system: • Shut down the virtual machine. • Retrieve the virtual machine UUID for the PN. • SSH to the XenServer and execute the following xe command: **`xe vm-param-set uuid=VM-UUID platform:device_id=0001`** • Boot the virtual machine.
	You're missing boot-critical drivers and the P2P tool did not or was not able to properly adjust your PN's operating system for the new hardware (rare).	(Step 3) To manually adjust a PN's operating system for new hardware:
PN boots, but the onQ Portal indicates a **Connection Status** of `PN offline`.	Your PN might have acquired a DHCP IP address, not the original static IP address.	Modify the PN's configuration to reflect its original, static IP address. Afterward, onQ can resume backups of the PN.

Symptom	Possible Cause	Solution
After a full cross-hypervisor BMR, the BMR'd image comes up with a DHCP address. Original network adapter is hidden and the image has a second, additional NIC with a DHCP address.	This is a known issue in a cross-hypervisor scenario.	See VMware's Knowledge Base article. It's not possible for QUARK's BMR process to manipulate the image registry and preset a static IP for a given PN.
When a restored, VMware-based PN initially boots, it might bring online only the OS disk—all other disks remain offline.	In this case, the PN loses some of its protected volumes if they reside on any of those offline disks. When onQ backs up this PN in this state, the backup fails, reporting that some of those protected volumes are missing in the PN. Because this issue reveals itself during a restore, QUARK might appear to be the cause, but that's not the case: QUARK always comes up with all attached disks and shows an online status for all target disks.	Using the OS's Disk Management interface, bring online all offline disks before onQ attempts a backup of the PN. This best practice is also outlined in Step 13 of (Step 2) To restore data to your PN:. After an offline disk is brought online, it stays online indefinitely, regardless of the number of PN reboots.

Symptom	Possible Cause	Solution
When you attempt to manually inject drivers into the target using QUARK's third-party P2P tool, the tool reports that it loaded the drivers, but doesn't actually load them.	Most of the time P2P works beautifully, and does so better than other, third-party tools; however, in some configurations, the tool isn't able to inject drivers.	Use another third-party tool (for example, DISM, if the target OS is 64-bit and Windows Server 2008 or above), to inject the drivers: `> Dism.exe /Image:C:\ /add-driver /driver:`***`fullPathToDriverINF file`***
After a restored PN reboots, video reverts to 640x480 or 800x600 resolution.	BMR process sets PN boot parameters to `Base video`. When set to `Base video`, Windows loads standard VGA drivers instead of display drivers specific to the video hardware on the computer.	After the restore and on the BMR target, launch the System Configuration utility (`msconfig.exe`), then go to **Boot** tab > **Boot Options** pane. Clear the **Base video** check box.

13.7 (Agent-based PNs) Connection Problems

Use the following table to troubleshoot connection problems with agent-based PNs as reported by the onQ Portal. This table lists the most likely causes first; therefore, verify the possible causes in the order that they are listed.

Symptoms: PN's **Connection Status** icon is red Tooltip indicates `PN offline`	
Possible Cause	**Solution**
System time on the PN is not synchronized with the onQ Appliance. If you're currently installing, this red icon appears 3 minutes (180 seconds) into the installation process or 5 minutes (300 seconds) after installation. If you've successfully deployed and the PN and the onQ Appliance subsequently become unsynchronized, a missing padlock appears next to the PN, in addition to this red icon.	You have a few choices. Go to Synchronize system time.
PN is down.	Bring up the server.
onQ Service is not running	Restart the service. Go to (Agent-based PNs) Restart the onQ Service.
PN's IP address or hostname changed.	Update IP address and hostname. See Manage hosts.
UDP port 5990 and TCP ports 5000 and 5990 are not open on the PN.	Verify that you performed this step during enrollment: Step 6: Enroll protected nodes and onQ Appliance-to-PN Communications.

Symptoms: PN's **Connection Status** icon is red Tooltip indicates `PN offline`	
Possible Cause	**Solution**
Certificate is corrupt.	Regenerate and reinstall the certificate. See Create secure connection to PNs.
DNS Server is down	Bring up DNS Server. Add host. See Manage hosts.
Incorrect IP address for DNS Server. If you migrated the DNS Server, onQ might have the incorrect IP address.	Go to the hosts file and update the IP address. See Manage hosts.
If you just performed a restore using QUARK, but the onQ Portal indicates a PN `offline` Connection Status, your PN may have acquired a DHCP IP address, not the original static IP address.	Modify the PN's configuration to reflect its original, static IP address. Afterward, onQ can resume backups of the PN.

Related Topics

Connection Alerts

13.8 (Agent-less PNs) Connection and Backup Problems

Use the following table to troubleshoot connection and backup problems with agent-less PNs as reported by the onQ Portal. This table lists the most likely causes first; therefore, verify the possible causes in the order that they are listed.

Symptom	Possible Cause	Solution
PN's Connection Status icon is red and tooltip indicates `PN offline`.	Firewall might be preventing ping.	Check firewall. Configure it to allow PN to respond to ping.
	PN proxy might be powered off.	On the ESXi host, verify that PN proxy (VM) is powered on. If not, power on the vm.
	If you just performed a restore using QUARK, your PN may have acquired a DHCP IP address, not the original static IP address.	Modify the PN's configuration to reflect its original, static IP address. Afterward, onQ can resume backups of the PN.
PN's Connection Status icon is green with a yellow dash (–) sign and tooltip indicates `Proxy offline`.	PN proxy might be in the process of restarting (every backup request from onQ does so).	Wait for the PN proxy to restart.
	PN proxy might be in a bad state.	Try re-installing via portal enrollment.
	Unknown.	Log on to the ESXi host and manually reset the PN proxy's power.

Symptom	Possible Cause	Solution
Backup process fails to create snapshots and the PN's Event Log indicates an event for this issue.		Disable backups for the PNs from the same host, then initiate a manual snapshot. If the snapshot completes successfully, delete that snapshot.
		From the ESXi host, reset power on the PN proxy.
		Restart protection on the onQ.
Backup of PN's pauses and the PN's Event Log indicates that there is a backlog for backup requests.		From the ESXi host, power off the PN proxy (VM). onQ restarts the proxy and starts backups again.
PN proxy returns the following exception: `system: 2014-06-02 06:31:29: Snapshot of PN and mount to proxy failed: PN wasn't moved to the new snapshot, or Snapshot creation failed.`	Base-disk must be mounted within 30 minutes. VMware supports creation of snapshots via the vSphere SDK. The PN proxy uses this API to create a snapshot and mount the snapshot disks. In some cases, (for example, a faulty VSS in the PN or a quiesce script in the PN), the snapshot API can fail. After the vSphere SDK returns a success for snapshot creation, the proxy waits 30 minutes for the base-disk to be mounted. If the snapshot disk isn't mounted during that time and the PN hasn't moved to the new snapshot disks, the PN proxy fails the operation and errors out with aforementioned exception.	

13.9 Recovery Node Problems

Use the following table to troubleshoot problems with your recovery nodes as reported by the onQ Portal.

Symptom	Possible Cause	Solution
RN's RN Status icon is red	You just added the PN and onQ is backing up the PN for the first time.	Wait for the backup to complete. See also Monitor backups.
	Protection is off.	Turn on protection. Go to Start node protection.
	Creation policy is set to Build-on-Demand.	Change the build policy. Go to (On-Site/Prime/Plus) Modify RN build policy.
Red exclamation point appears next to the protected node	The protected PN is down and the corresponding RN is running.	This is expected behavior. Fix your PN. Before you bring the PN online, stop the RN.

Related Topics

Recovery Node and PN Disk Space Alerts

13.10 Self-Test and RN Boot Problems

Use the following table to troubleshoot self-test failures with agent-based and agent-less PNs as reported by the onQ Portal and one or more of the alerts outlined in Self-Test Alerts. For each symptom, this table lists the most likely cause first; therefore, verify the possible causes in the order that they are listed.

Before You Begin: Verify that the RN is in a usable state by booting it in test mode. If the RN fails to boot, reinitialize it to eliminate the possibility that the problem is with the RN build process itself. Afterward, proceed with the table below.

Symptom	Possible Cause	Solution
RN may or may not boot	Occurs immediately following a Linux PN enrollment. Typo in boot menu loader or mismatch between the kernel versions and the initramfs version.	If you're in the process of enrolling the Linux PN for the first time and the RN won't boot, see the troubleshooting tips in (Agent-based Linux PNs) Enroll protected nodes or (Agent-less Linux/Windows PNs) Enroll protected nodes.
	Operating system is not supported.	Verify that the operating system is supported. Go to "Platform Support" in onQ Release Notes.
	RN has insufficient resources.	If RN boots, verify that there is adequate memory and disk space for the RN: go to Monitor disk space and memory usage. If there isn't, provide the RN more resources.
	Unresolved dependencies led to the onQ Service not starting on time on the RN.	Determine if the RN is dependent on another service, then make that service available. Some services might take time to start; eventually those services might succeed or fail or time out thereby delaying the onQ Service from starting on time. Such services might rely on other resources (internal or external). For example, the service might be waiting for a mount manager (internal resource) to process huge mount points leftover in the registry, or for a time server/Domain Controller (external resource) to become available.

Symptom	Possible Cause	Solution
RHEL 7 RN cannot boot and self-test fails	`/boot/grub/grub.conf.xvf5` boot menu doesn’t exist or has incorrect contents	Make the grub boot menu changes outlined in (RHEL 7.0) To enroll an agent-based Linux PN: or (RHEL 7.0/ESXi) To enroll an agent-less Linux PN:
RHEL 7 RN boots with desired IP address, but self-test fails	Misconfigured firewall rules.	The RHEL 7 default firewall service is firewalld. However, you can use iptables service instead. For specific instructions, go to (RHEL 7.0) To enroll an agent-based Linux PN: or (RHEL 7.0/ESXi) To enroll an agent-less Linux PN:
RN booted with correct IPs but no network activity	PN has a dynamic IP address.	Make sure that the PN has a static IP.
	PN is running on an OEM version	Make sure that the PN is not running an OEM version. Networking might be disabled. For more information, go to Go to “Platform Support” in onQ Release Notes.
BSOD and RN cannot boot	RN has a faulty service	If there is a blue screen, read the blue screen code as it might indicate the service that caused the blue screen. Disable that faulty service; if that doesn’t work, capture the BSOD screen and contact Quorum Support.

Symptom	Possible Cause	Solution
RN/PN takes too long to boot	RN has slow-to-start service	Does the RN take more than 15 minutes to come up? If yes, check the Windows event log and figure out which service(s) is taking a long time to start or which service(s) is timing out. Disable or reconfigure this service to speed up the boot time.
	PN has large registry	Check the PN's boot time. If the PN has a long boot time, the problem needs to be addressed at your PN site. For example, the PN might have a large registry that causes the PN to boot slowly. Resolve the root cause of the growing registry and clean up the registry.
RN reboots continuously	Windows Server 2012 R2 Bug	(Windows Server 2012 R2) If RN continues to reboot, boot it in self-mode, then search the Windows event logs for the suspicious service and disable it. For example, the `ShellHWDetection` service is notorious for continuously rebooting an RN running Windows Server 2012 R2. Disabling the `ShellHWDetection` service resolves the problem.
RN boots, but has no XenServer NIC hardware	3rd party software	In specific cases, some 3rd party software applications prevent the XenServer NIC from functioning. For example, Symantec endpoint protection 12.1.4100.426 blocks the XenServer NIC from functioning. In this case, disabling the Symantec endpoint protection services resolves this problem.

Symptom	Possible Cause	Solution
RN boots with XenServer NIC, but has an incorrect IP address	Misconfigured RN network	Check the RN NIC configuration and IP configuration via the onQ Portal. Verify that `xvf.dat` exists on the PN and that the PN does not have a custom network configured. Make sure the network configuration is correct.
RN boots with XenServer NIC, but has no IP address	Misconfigured cluster network	RN does not own the cluster resources as set forth in the cluster policy, so the IP address is inactive. If you want the RN to own the cluster resources, use the Enable Cluster Support parameter or change the cluster policy.
	3rd party software	In specific cases, some 3rd party software applications prevent the IPs from attaching to XenServer NIC. For example, Network load balancing software (NLB) might block an IP from being used. Also, the WLBS Windows NLB service blocks NIC IPs on Windows Server 2012R2; therefore, delete the WLBS service on the RN build via the onQ Portal, if required. Disable the WLBS service on other Windows Server platforms as needed.
RN booted with correct IPs but no network activity or limited network connectivity	3rd party software	Check if any 3rd party network management software is installed: `Antivirus/firewall/network manager/....` If yes, disable this software on the RN build.

If the self-test still fails or the RN cannot boot, contact Quorum Support, providing the information outlined in Helpful System Information. In addition, provide us the answers to the following questions to speed up resolution:

- Is there a PN with the same operating system on the same onQ Appliance where self-tests are passing?
- Is this a newly protected PN?
- Is this PN experiencing *sudden* self-test failures with prior success?

(Important!) In addition:

- Did you provide a screen shot of RN’s Programs and Features (Control Panel > Programs and Features)? If not, please do so. This output tells Quorum what 3rd party software is installed.
- Did you include a screen shot of the RN’s BSOD, if applicable? If not, please do. This output might indicate the offending service.
- Did you include RN’s output from `systeminfo` command? If not, please do.

13.11 Helpful System Information

To speed up technical support for your issue, please provide the following information when contacting Quorum Support.

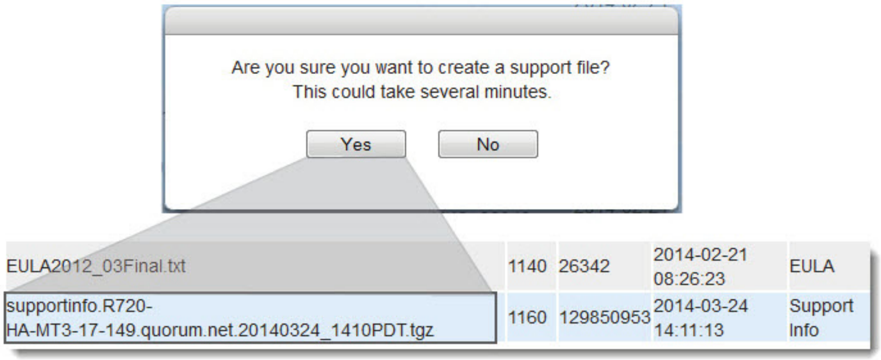
- Account information.
- PN’s operating system, host name, hardware vendor/model, physical or virtual: # `systeminfo`.
- onQ STATUS page—screen shot or copy/paste.
- Screen shot of special networking configuration and software installation: Control Panel > Programs & Features.
- BSOD screen shot, if applicable.
- List of any recent upgrades or software changes.
- If your PN is VMware-hosted, specify whether it’s agent-based or agent-less.
- Support Log (see Generate Support Log).
- The Health Report, if your onQ is not configured to send these reports to onQ Central.
- List of your troubleshooting steps and results.

13.12 Generate Support Log

If requested by Quorum Support, email your support engineer the Support Log. This log provides additional information to help Quorum Support troubleshoot issues with your onQ Appliance.

To generate a Support Log:

1. Log on to the onQ Appliance's onQ Portal.
2. Go to **APPLIANCE CONFIG** > **ADVANCED** > **DOWNLOADS**.
3. Click on the **SUPPORT** button, then **Yes** to generate the log (`.tgz` file).
4. From the **DOWNLOADS** tab, scroll down to the end of the download list and select the file that you just generated, then click the **DOWNLOAD** button to save the Support Log.



Are you sure you want to create a support file?
This could take several minutes.

EULA2012_03Final.txt	1140	26342	2014-02-21 08:26:23	EULA
supportinfo.R720-HA-MT3-17-149.quorum.net.20140324_1410PDT.tgz	1160	129850953	2014-03-24 14:11:13	Support Info

5. Email this Support Log to Quorum Support.

   This Support Log is quite large, and many email systems will reject it. If you have problems emailing this file, contact Quorum Support.

13.13 Backup Alerts

It's important that you resolve backup failures. Fortunately, most failures can be attributed to are few common causes, including conflicting VSS-based (Volume Shadow Copy Service) backup solutions, insufficient disk space, and high CPU usage.

For specific alerts:

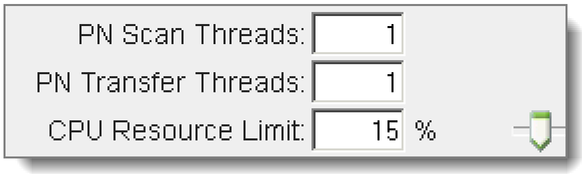
- A0801
- A0802
- A0803

13.13.1 A0801

Message: The onQ backup of Protected Node *PNName* has repeatedly failed. The last backup attempt returned code: *ReturnCodeListedBelow*. Please verify that there is sufficient free disk space on the Protected Node. Backups will continue on the configured schedule or when triggered from the onQ web portal.

Cause: The specific cause depends on the return code that appears in the alert message.

Solution: Regardless of your return code, perform the following solutions in the following table and in the order listed:

Possible Cause	Solution
High CPU Usage	Go to the Task Manager and determine if you have high CPU usage (> 30%). If yes, reduce the load on the system. In addition, go to **PROTECTION CONFIG** tab, select the PN, **MODIFY** > **ADVANCED**, then do the following: **1.** Reduce scan threads to 1. **2.** Reduce transfer threads to 1. **3.** Reduce CPU resource limit by 50% of current limit. The system default is 30%. Set it to 15%.  PN Scan Threads: 1 PN Transfer Threads: 1 CPU Resource Limit: 15 %
Conflicting VSS-based Backup Solutions	There are conflicting VSS-based backup solutions running. Disable all conflicting VSS-based backup solutions.
Insufficient Disk Space	Backups can fail if the PN is running out of disk space. Free up some space on the PN by deleting temp files or, if the PN is a virtual machine, expand the disk.
Other Solutions	Restart the onQ Service and Restart protection.

If these solutions don’t work, perform the solution(s) outlined in the applicable return status listed under the drop-down hotspots below and in alphabetical order.

\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy3\ (The system cannot find the path specified.

There are conflicting VSS-based backup solutions running: see Conflicting VSS-based Backup Solutions.

Block sums file c:\Program Files\Quorum\usr/blocksums/99restart-blocksums.bin corrupted: expected file object

Delete all files under blocksums folder.

DoSnapshotSet

Do the following:

1. From the PN, run the following command: .

   ```
   # vssadmin list writers
   ```

2. If writers are at a failed state, reboot the PN.

If that solution doesn’t work, contact Quorum Support.

Error writing raw data to c:\Program Files\Quorum\usr/blocksums/sorted-blocksums.bin (Broken pipe)

PN is running out of disk space: see Insufficient Disk Space. Also, delete all files under blocksums folder.

Error writing c:\Program Files\Quorum\usr/scan/0.txt (No space left on device)

The PN ran out of space during a backup. Free up some space: see Insufficient Disk Space.

Error: E_INVALIDARG

Reboot the PN. If that solution doesn’t work, reinstall the node software as outlined in (Alternative) To manually install or reinstall agent-based Windows PN software:

Error: VSS_E_VOLUME_NOT_SUPPORTED (..\volumes_win32.cpp @

297)

We do not support non-NTFS volumes as outlined in Limitations.

Fail to rotate log, QFilter

Do the following:

1. From a cmd prompt, run the following commands:

```
> sc stop quorum
> sc stop qfilter
```

2. From `C:\Program Files\Quorum\usr`, delete all files with filenames that begin with `qfilter.log`.
3. Run the following command:

```
> net start qfilter
> net start quorum
```

Invalid Drive

The drive needed to perform the backup is no longer available. Log on to the PN and verify (Windows Explorer > My Computer) that all the drives are available. If the drives are present, reboot the PN. If the drives are missing, add the drives.

NotStarted

There are conflicting VSS-based backup solutions running: see Conflicting VSS-based Backup Solutions. If that solution doesn't work, reboot the PN.

Oracle VSS Writer failed during snapshot, aborting

Restore the Oracle database using one of the following procedures:

- Back up and restore Oracle 11g database on Linux
- Back up and restore Oracle 10g+ database on Windows

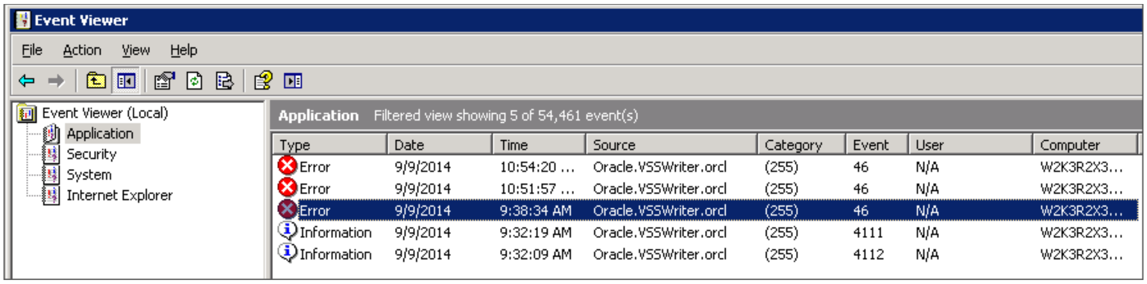
A Windows PN backup fails if onQ detects a VSS_WS_FAILED_AT_*ErrorState* for any of the following VSS Writer error states, and records the error state in the PN's Event Log.

```
VSS_WS_FAILED_AT_IDENTIFY
```

```
VSS_WS_FAILED_AT_PREPARE_BACKUP
```

```
VSS_WS_FAILED_AT_PREPARE_SNAPSHOT

VSS_WS_FAILED_AT_FREEZE

VSS_WS_FAILED_AT_THAW

VSS_WS_FAILED_AT_POST_SNAPSHOT

VSS_WS_FAILED_AT_BACKUP_COMPLETE

VSS_WS_FAILED_AT_PRE_RESTORE

VSS_WS_FAILED_AT_POST_RESTORE

VSS_WS_FAILED_AT_BACKUPSHUTDOWN
```

To troubleshoot these error states, look at the PN's Windows log via Event Viewer: **Start** button > **Control Panel** > **System and Security** > **Administrative Tools** > **Event Viewer**.



Application Filtered view showing 5 of 54,461 event(s)

Type	Date	Time	Source	Category	Event	User	Computer
Error	9/9/2014	10:54:20 ...	Oracle.VSSWriter.orcl	(255)	46	N/A	W2K3R2X3...
Error	9/9/2014	10:51:57 ...	Oracle.VSSWriter.orcl	(255)	46	N/A	W2K3R2X3...
Error	9/9/2014	9:38:34 AM	Oracle.VSSWriter.orcl	(255)	46	N/A	W2K3R2X3...
Information	9/9/2014	9:32:19 AM	Oracle.VSSWriter.orcl	(255)	4111	N/A	W2K3R2X3...
Information	9/9/2014	9:32:09 AM	Oracle.VSSWriter.orcl	(255)	4112	N/A	W2K3R2X3...

For an explanation of the error states, go to Microsoft's Volume Shadow Copy API Reference documentation. For overview information, go to Microsoft's Event and Error Handling Under VSS. Contact your Oracle database administrator to resolve the error.

scan failed, aborting

The PN might not have enough disk space: see Insufficient Disk Space.

If that solution doesn't work, do the following:

1. From the PN, run the following command: .

```
# vssadmin list writers
```

2. If writers are at a failed state, reboot the PN.

If that solution doesn't work, there might be conflicting VSS-based backup solutions running: see Conflicting VSS-based Backup Solutions.

If that solution doesn't work, reboot the PN.

SS_E_PROVIDER_VETO

There might be too much CPU load: see High CPU Usage. If that solution doesn't work, there might be conflicting VSS-based backup solutions running, resulting in VSS writer failures: see Conflicting VSS-based Backup Solutions. If that solution doesn't work, reboot the PN.

Transfer incomplete

If your PN is a Windows Server 2003, you might need to change the values for the `PoolUsageMaximum` and `PagedPoolSize` registry settings as outlined in Microsoft KB 304101.

Unable to resolve target hostname

Do the following:

- Verify that the hostname hasn't changed. If it has, update the IP address in the onQ's hosts file as outlined in Manage hosts.
- Verify that the DNS entry is correct. If it isn't, update the entry in the onQ's hosts file as outlined in Manage hosts.
- If this PN is in a cluster, ensure that you configured things correctly. Go to Enrollment in Windows Cluster Services Environment.

vss unexpected provider

Oracle VSS Writer failed during a snapshot. There are conflicting vss backup solutions running. *Uninstall* any conflicting VSS-based backup solutions. If this doesn't work, reboot the PN.

VSS_E_SNAPSHOT_SET_IN_PROGRESS

There might be conflicting VSS-based backup solutions running: see Conflicting VSS-based Backup Solutions. If that solution doesn't work, then reboot the PN.

13.13.2 A0802

Message: The onQ backup of Protected Node *PNName* has failed due to a failure of the PN. Backups will continue when the PN comes online.

Cause: A few issues can cause this problem: (1) PN and onQ do not have the same system time; (2) High CPU load; and (3) Other connectivity problems between the PN and onQ.

Solution: Verify system time on both the PN and onQ. If necessary, update the system time. Go to Synchronize system time.

If that solution doesn't work, verify connectivity by attempting to ping the onQ from the PN (see also (Agent-based PNs) Connection Problems).

If that solution doesn't work, you might have high CPU load: see High CPU Usage.

13.13.3 A0803

Message: The onQ service on *PNName* is unable to stop the backup process, `squirtcopy.exe`. This may be due to a transient problem with `taskkill.exe`. Backups on *PNName* have been suspended until protection is stopped and restarted.

Cause: The cause depends on a number of factors.

Solution: Restart protection. If the problem persists, restart the PN.

13.14 Snapshot Alerts

Snapshot issues are rare. However, when they occur, a rescan or protection restart typically resolves the problem.

For specific alerts:

- A0401
- A0402
- A0403
- A0404

13.14.1 A0401

Message: *ApplianceName* has detected an unexpected error during the BCVPreAdd process for *PNName*. The return status was: *ReturnStatus*. Protection will be disabled for this PN.

Cause: The cause depends on a number of factors.

Solution: Restart protection. If that solution doesn't work, contact Quorum Support.

13.14.2 A0402

Message: *ApplianceName* has detected that an inconsistent object count has been stored in the repository. The HA onQ should have sent an alert for 'Object count inconsistency'. Please refer to that alert for information on resolving this issue.

Cause: The cause depends on a number of factors.

Solution: From the HA Appliance (always start with the HA, even when resolving DR error messages):

1. Force a full rescan. Go to Perform full rescan on PN.
2. Trigger an immediate backup. Go to Initiate immediate backups.

The database will resync. After the full snapshot is processed on the HA, the error on the HA will go away. After the same snapshot is transferred and fully processed/consumed by the DR, the error message on the DR will also go away. Because of the time needed to transfer and process the snapshot, there will be a delay between when the HA Appliance resolves the issue and when the DR Appliance resolves the same issue.

13.14.3 A0403

Message: *ApplianceName* has detected that the object count for *PNName* is inconsistent with the value stored in the repository. A full rescan of the PN is required to resolve this issue.

Cause: The cause depends on a number of factors.

Solution: From the HA Appliance (always start with the HA, even when resolving DR error messages):

1. Force a full rescan. Go to Perform full rescan on PN.
2. Trigger an immediate backup. Go to Initiate immediate backups.

The database will resync. After the full snapshot is processed on the HA, the error on the HA will go away. After the same snapshot is transferred and fully processed/consumed by the DR, the error message on the DR will also go away. Because of the time needed to transfer and process the snapshot, there will be a delay between when the HA Appliance resolves the issue and when the DR Appliance resolves the same issue.

13.14.4 A0404

Message: *ApplianceName* has detected an unexpected error during the BCVAdd process for *PNName*. The error status was: *ReturnStatus*. Protection will be disabled for this PN until protection is restarted for this onQ appliance.

Cause: The cause depends on a number of factors.

Solution: Restart protection. If that solution doesn't work, contact Quorum Support.

13.15 PN Status Alerts

If the PN (or HA) is actually down, perform the appropriate DR workflow in conjunction with your business continuity plan:

- (Workflow) Fail over HA to DR Appliance
- (Workflow) Fail back DR to HA
- (Workflow) Fail over a PN to an RN
- (Workflow) Fail back an RN to a PN

If the PN is up, the problem can usually be resolved by updating the system time or the onQ hosts file.

For specific alerts:

- A0704
- A0710

13.15.1 A0704

Message: *ApplianceName* has detected a FAILURE of the Protected Node *PNHostName*. If this is an actual failure, use the onQ web portal to start the backup Recovery Node for this machine.

Cause: Either a host IP changed or, more commonly, the system time being off by roughly 5 minutes. Typically when a PN shows red for offline it is one of these 2 cases. However, this error can also occur if the PN shut down or rebooted or the onQ Service isn't running.

Solution: Do one of the following, and in the following order:

- *Time off Scenario*: Verify system time on both the PN and onQ. If necessary, update the system time. Go to Synchronize system time. Finally, restart protection. The PN should reconnect to the onQ.
- *IP Address Scenario*: This problem most commonly occurs when the onQ Service is installed during a PN enrollment when the PN has a DHCP address, prior to a static being assigned. If the IP address of the PN changed, update the IP address in the onQ's hosts file as outlined in Manage hosts, then restart protection.
- *onQ Service not running on agent-based PN*. PN is up and running, but the onQ Service isn't. This situation is possible following a successful automatic upgrade of the PN or after a reboot of the PN. If true, restart the onQ Service.
- *PN shutdown or reboot*. The PN shut down or rebooted for maintenance or some other reason. If true, power on the PN or wait for the PN to reboot, then verify that the PN is online.
- *Actual PN failure*: If true, go to (Workflow) Fail over a PN to an RN.

13.15.2 A0710

Message: *ApplianceName* was unable to upgrade the onQ Service on *PNName* to version *VersionNumber*. The current version on the PN is *VersionNumber*. The return status from the upgrade attempt was: *ReturnStatus.*

Cause: The most likely cause for this agent-based PN upgrade is that the PN has too many other programs running thereby causing high CPU utilization, or the installer is currently installing a different program.

Solution: Fix the utilization problem. If that solution doesn't work, reinstall the node software as outlined in (Alternative) To manually install or reinstall agent-based Windows PN software: or (Agent-based Linux PNs) Enroll protected nodes.

13.16 License Expiration and Upgrade Alerts

Each Appliance requires a license. Without a valid license, your nodes are not protected. onQ sends license alerts before and after expiration.

For specific alerts:

- A0008
- A0009
- A0014
- A0015
- A0017

13.16.1 A0008

Message: The installed license has expired. Protection on this onQ appliance has been disabled and will not run until a new license is installed.

Cause: The license expired.

Solution: Upload a replacement license. Go to Install onQ Appliance license.

13.16.2 A0009

Message: The installed license has expired. Protection on this Archive Vault appliance has been disabled and will not run until a new license is installed. Please send an email to license@quorum.net with your appliance serial number if you have already purchased your new license.

Cause: The license expired.

Solution: Upload a replacement license. Go to Install onQ Appliance license.

13.16.3 A0014

Message: A software version mismatch has been detected between this appliance and *ApplianceName*. The current running version for this appliance is *VersionNumber*, while the version reported by *ApplianceName* is *VersionNumber*. Due to compatibility reasons no further configuration changes, such as newly enrolled protected nodes, will be available on this appliance until this issue has been resolved. When possible please ensure each appliance is updated to the same version level.

Cause: Each of the onQ Appliances listed is running different software versions. They must be in sync.

Solution: Compare the versions between the onQ Appliances, then resolve the incompatibility by upgrading each onQ Appliance to the same version level. If the documented upgrade process does not support your upgrade path, contact Quorum Support.

13.16.4 A0015

Message: A software version mismatch has been detected between this appliance and *ApplianceName*. The current running version for this appliance is *VersionNumber*, while the version reported by *ApplianceName* is *VersionNumber*. Due to compatibility reasons no further configuration changes, such as newly enrolled protected nodes, will be available on the remote appliance until this issue has been resolved. When possible please ensure each appliance is updated to the same version level.

Cause: Each of the onQ Appliances listed is running different software versions. They must be in sync.

Solution: Compare the versions between the onQ Appliances, then resolve the incompatibility by upgrading each onQ Appliance to the same version level. If the documented upgrade process does not support your upgrade path, contact Quorum Support.

13.16.5 A0017

Message: The installed license will expire on *Date*. You must install a new license before that date in order to maintain protection.

Cause: The license is about to expire.

Solution: Upload a replacement license. Go to Install onQ Appliance license.

13.17 Reboot Alerts

If onQ identifies a problem, determines that a reboot will fix the problem, onQ initiates that reboot and restarts protection. If onQ has enough time prior to the reboot to log the cause for the reboot, it will do so, providing a detail Cause in the alert. Otherwise, a generic message appears in the alert.

For specific alerts:

- A0010
- A0011
- A0012
- A0013
- A0018

13.17.1 A0010

Message: Protection is enabled but the manager process cannot be found. Rebooting the onQ VM and restarting protection.

Cause: This is expected behavior.

Solution: Nothing. onQ rebooted the onQ VM and restarted protection. However, If protection does not start correctly, contact Quorum Support.

13.17.2 A0011

Message: Protection is enabled but the manager process cannot be found. Rebooting the Archive Vault VM and restarting protection.

Cause: This is expected behavior.

Solution: Nothing. onQ rebooted the onQ VM and restarted protection. However, If protection does not start correctly, contact Quorum Support.

13.17.3 A0012

Message: Rebooting the onQ VM and restarting protection to clear 3761.

Cause: This is expected behavior.

Solution: Nothing. onQ rebooted the onQ VM and restarted protection. However, If protection does not start correctly, contact Quorum Support.

13.17.4 A0013

Message: Rebooting the Archive Vault VM and restarting protection to clear 3761.

Cause: The cause depends on a number of factors.

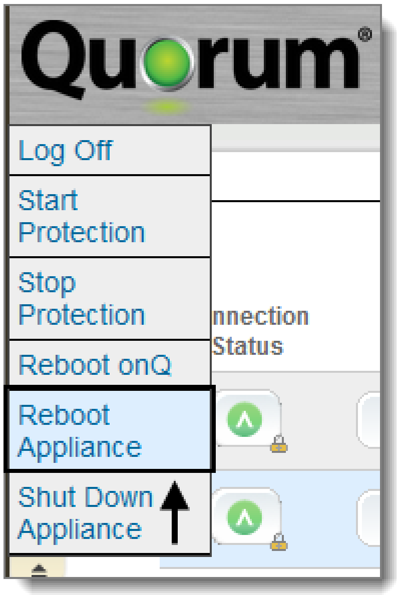
Solution: Nothing. onQ rebooted the onQ VM and restarted protection. However, If protection does not start correctly, contact Quorum Support.

13.17.5 A0018

Message: Unable to shut down *VMName* VM while starting onQ protection.

Cause: The cause depends on a number of factors.

Solution: If an RN is in production due to a disaster, do not reboot the onQ Appliance; contact Quorum Support instead. If no RN is in production, go ahead and reboot the onQ Appliance.



13.18 Protection Alerts

The following alerts are sent out when protection is turned on or off on the onQ by a user that has VARAdmin user role.

- A0001
- A0003

13.18.1 A0001

Message: onQ protection has been stopped at user request

Cause: A user that has VARAdmin user or Admin user role stopped protection on the protected node.

Solution: Nothing as there are cases in which you might want to stop protection. However, don't forget to start protection afterward; otherwise, your nodes will not be protected. Also, if you did not perform this action, identify other administrators who have credentials to access the onQ.

13.18.2 A0003

Message: onQ protection has been started at user request

Cause: A user that has VARAdmin user or Admin user role started protection on the protected node.

Solution: Nothing as you must start protection in order to protect your nodes. However, if you did not perform this action, determine who is managing the onQ.

13.19 Recovery Node and PN Disk Space Alerts

A protected node's virtual disk (vdisk) requires a specific amount of disk space. onQ alerts you when your protected node's vdisk capacity usage exceeds 90%.

For specific alerts:

- A0901
- A0902
- A0903
- A0904
- A0906

13.19.1 A0901

Message: An unexpected error was encountered when attempting to update the contents of a Recovery Node. The error status returned was: *ReturnStatusListedBelow*. No further updates to the Recovery Node will be attempted until you select the Initialize button.

Solution: Depends on the return status listed under the drop-down hotspots below.

InvalidData

Do not reinitialize the RN. This issue might indicate a problem with the Repository. Contact Quorum Support.

SelectTimeout

Reinitialize the RN.

SystemErrDiskFull

Data in one or more protected volumes has exceeded its virtual disk size allocated on the onQ. Resize the vdisk for the volume(s) indicated in the alert.

13.19.2 A0902

Message: Volume *DriveLetter* of Recovery Node *RNName* is configured with disk space insufficient to create a new RN from the current snapshot. The previously built RN left unchanged. The snapshot data for the PN is intact and a new RN will be created after the configured disk space is increased. You should increase the amount of disk space allocated to this RN.

Cause: Initial vdisk size allocated for a volume on the PN is inadequate because of the growing data on the PN in the corresponding volume. In this case, the onQ Manager does not update the RN.

Solution: Resize the vdisk 15–20% over what is currently being used.

13.19.3 A0903

Message: The Recovery Node disk space allocated for volume(s) *DriveLetter* of *RNName* is over 90% used. The RN will be created, however you may wish to increase the amount of disk space allocated to each named above volume of that RN.

Cause: Initial vdisk size allocated for a volume on the PN is inadequate because of the growing data on PN in the corresponding volume. In this case, the onQ Manager does not update the RN.

Solution: Resize the vdisk 15–20% over what is currently being used.

13.19.4 A0904

Message: The R2V Export process on *ApplianceName* has returned an unexpected error code. This is preventing the update of the RN for *RNName*. The error code return was: `ExportFailed`.

Cause: This is a transient error.

Solution: Wait for one more update to occur. Contact Quorum Support if next update is not successful.

13.19.5 A0906

Message: The onQ restriction [no more than 15 virtual disks per Recovery Node] was hit while making a copy of volume $arg1: Reinitializing the RN image may reduce the number of virtual disks involved.

Cause: You exceeded a virtualization limitation (see Resize protected node's vdisk for explanation).

Solution: Rebuild the RN. If a rebuild doesn't work, contact Quorum Support.

13.20 Repository Space Alerts

The Repository needs a certain amount of disk space. If you're low on disk space, there are things that you can do to free up space before the issue becomes critical.

For specific alerts:

- A0101
- A0102
- A0103
- A0104
- A0303
- A0304
- A0502
- A0503

13.20.1 A0101

Message: The free Repository space on *ApplianceName* has fallen below normal limits. If the free Repository space continues to decrease, onQ will expire the oldest backups for each Protected Node in order to recover space.

Cause: This alert is for informational purposes: repository disk utilization is at 75%. onQ has a built-in purge policy whereby if its repository disk space utilization exceeds 85% onQ begins to "free up" space by deleting PN backups, starting with the oldest backups.

Solution: Delete orphan backups manually, reduce retention period, or remove a node for which you don't need protection. Contact Sales to discuss options for expanding disk space.

13.20.2 A0102

Message: The free Repository space on *ApplianceName* has fallen below normal limits. If the free Repository space continues to decrease, the Archive Vault will disable the addition of any new archive jobs until additional space becomes available.

Cause: This alert is for informational purposes: repository disk utilization is at 75%. AV has a built-in job policy whereby if its repository utilization exceeds 85%, AV suspends all jobs. In this case, this threshold has not yet been reached.

Solution: Contact Quorum Support to remove archive jobs as there is no user facility in the onQ Archive Vault to remove jobs, or contact Quorum Sales to discuss purchasing additional storage.

13.20.3 A0103

Message: The free Repository space on *ApplianceName* has fallen to critical limits. onQ is starting to expire the oldest backups for each Protected Node in order to recover space.

Cause: onQ has a built-in purge policy whereby if its repository disk space utilization exceeds 85% onQ begins to "free up" space by deleting PN backups, starting with the oldest backups. In this case, this threshold was reached, so onQ began deleting PN backups, starting with the oldest backups.

Solution: Nothing. The system is working as expected.

13.20.4 A0104

Message: The free Repository space on *ApplianceName* has fallen to critical limits. The Archive Vault is suspending all archive jobs until additional space becomes available.

Cause: AV has a built-in job policy whereby if its repository disk space utilization exceeds 85%, AV suspends all jobs. In this case, this threshold was reached. Protection remains ON, but no further archiving will take place.

Solution: Contact Quorum Support to remove archive jobs as there is no user facility in the onQ Archive Vault to remove jobs, or contact Quorum Sales to discuss purchasing additional storage.

13.20.5 A0303

Message: The free Repository space on *ApplianceName* has fallen below allowable limits. Expiration of oldest backups failed for some PNs. onQ successfully expired *PercentageExpired* oldest backups: *NumberOfExpiredByPN*

Cause: onQ has a built-in purge policy whereby if its repository disk space utilization exceeds 85% onQ begins to “free up” space by deleting PN backups, starting with the oldest backups. In this case, this threshold was reached, so onQ tried deleting PN backups, starting with the oldest backups. Some expirations failed.

Solution: Contact Quorum Support to help with expirations, then contact Quorum Sales to add more disk space.

13.20.6 A0304

Message: The free Repository space on *ApplianceName* has fallen below allowable limits. onQ expired oldest *PercentageExpired* of backups (total of *NumberOfExpiredBackups*) for each Protected Node in order to recover space: *NumberOfExpiredByPN*.

Cause: onQ has a built-in purge policy whereby if its repository disk space utilization exceeds 85% onQ begins to “free up” space by deleting PN backups, starting with the oldest backups. In this case, this threshold was reached, so onQ began deleting PN backups, starting with the oldest backups.

Solution: Delete orphan backups manually, reduce retention period, or remove a node for which you don’t need protection. Contact Sales to discuss options for expanding disk space.

13.20.7 A0502

Message: The file system holding incoming snapshots on *DRApplianceName* is at *PercentageUsed* capacity. Transfers will be suspended until use drops below 85%.

Cause: onQ has a built-in policy whereby if its repository disk space utilization exceeds 85% onQ begins to “free up” space by suspending transfers of backups from the HA to the DR. In this case, this threshold was reached, so onQ suspended all snapshot transfers. onQ resumes snapshot transfers when use drops below 85%. This suspension policy attempts to prevent your DR Appliance from using 100% of its repository’s disk space.

Solution: Contact Sales to discuss options for expanding disk space.

13.20.8 A0503

Message: The file system holding incoming snapshots on *DRApplianceName* is at *PercentageUsed* capacity. Transfers will be resumed. Transfers will however be suspended again if use exceeds 85%.

Cause: onQ has a built-in policy whereby if its repository disk space utilization exceeds 85% onQ begins to “free up” space by suspending transfers of backups from the HA to the DR. In this case, this threshold has not yet been reached, and so onQ continues to transfer snapshots until use exceeds 85%. This suspension policy attempts to prevent your DR Appliance from using 100% of its repository's disk space.

Solution: Contact Sales to discuss options for expanding disk space.

13.21 onQ Disk Space Alerts

The onQ Appliance needs a certain amount of disk space to do its job. Fortunately, there are ways to free up disk space. For example, you can change your backup retention policy.

For specific alerts:

- A0201
- A0301
- A0302

13.21.1 A0201

Message: The free OS disk space on the onQ appliance *ApplianceName* has fallen to critical limits and the automated cleanup process was unable to resolve the issue.

Cause: The onQ Appliance needs a certain amount of disk space to do its job.

Solution: Contact Quorum Support immediately.

13.21.2 A0301

Message: While in critically low free disk space state, current policy allowed no backups to be expired on *ApplianceName* appliance. The condition will remain, please add physical disk space to the appliance.

Cause: The onQ Appliance needs a certain amount of disk space to do its job. onQ relies on the ability to expire backups in an effort to “free up” disk space. Your retention policy forbids expirations.

Solution: Change your policy to allow for expirations. Go to Change Backup Retention Policy.

13.21.3 A0302

Message: While in critically low free disk space state, attempt to expire oldest snapshots failed. Protection is being stopped.

Cause: The onQ Appliance needs a certain amount of disk space to do its job. onQ relies on the ability to expire backups in an effort to recover disk space; however, it was unable to do so.

Solution: Contact Quorum Support immediately.

13.22 Connection Alerts

onQ sends connection alerts when the DR system loses its connection with the HA Appliance, then re-establishes the connection. Depending on the circumstances, you might need to exercise your Disaster Recovery procedures.

For specific alerts:

- A0705
- A0706
- A0707
- A0708

13.22.1 A0705

Message: The onQ HA Manager *onQHostName* cannot be contacted. If this is confirmed to be a site failure, you will need to start Disaster Recovery protection from *ApplianceName*.

Cause: Possible causes are:

The HA appliance is completely down (unavailable) – including protection. However, DR is up and running.

The ‘Linkmon’ service on DR Appliance cannot start or isn’t working properly.

The onQ (Remote) configuration on DR Appliance does not have correct hostname or IP address for HA Appliance.

Solution: If this is a site failure, go to “(Workflow) Fail over HA to DR Appliance” on page 332.

13.22.2 A0706

Message: The onQ Manager *onQHostName* cannot be contacted.

Cause: Possible causes are:

- The DR Appliance is completely down (unavailable) – including protection. However, the onQ Archive Vault is up and running.
- The ‘Linkmon’ service on AV virtual machine cannot start or isn’t working properly.

Solution: Restart the DR Appliance (see To restart the onQ Appliance:), if it isn’t online. If the DR Appliance is up and running, restart protection on the AV: (1) From the drop-down menu > **Stop Archive Protection**, then (2) drop-down menu > **Start Archive Protection**.

13.22.3 A0707

Message: The link between the onQ Managers *onQHostName* and *ApplianceName* has been re-established. If any RNs on *ApplianceName* were being used in production mode, you will need to schedule your failback procedure before bringing up your PNs to minimize data loss.

Cause: Possible causes are:

- The HA appliance is completely down (unavailable), including protection. However, DR is up and running.
- The ‘Linkmon’ service on DR Appliance cannot start or isn’t working properly.
- The onQ (Remote) configuration on DR Appliance does not have correct hostname or IP address for HA Appliance.

Solution: If this was a site failure, "(Workflow) Fail back DR to HA" on page 335.

13.22.4 A0708

Message: The link to the onQ Manager *onQHostName* has been re-established.

Cause: Disconnects can happen for a variety of reasons.

Solution: Nothing. This message is for informational purposes only. The HA is now accessible and the DR Appliance has re-established a connection with the HA.

13.23 Self-Test Alerts

Some self-test failures can easily be resolved by making sure that the RN has the correct network configuration. However, other failures are quite complicated because there are third party applications that can interfere with self-tests.

For specific alerts:

- A1001
- A1002
- A1003

13.23.1 A1001

Message: The automated self-test of *RNName* running on *ApplianceName* was successful. The snapshot level was *time timeZone mm/dd/yy*. No further notifications will be sent unless a self-test failure is detected.

Cause: The self-test started per the testing policy set in Configure automatic testing of RNs.

Solution: Nothing. Self-test is running as expected.

13.23.2 A1002

Message: The automated self-test of *RNName* running on *ApplianceName* failed. The failed snapshot level was *time timeZone mm/dd/yy*. No further notifications will be sent unless a self-test of this RN is successful.

Cause: onQ defines a failure as any self-test that doesn’t complete successfully within a 15-minute period.

Solution: Perform the series of solutions outlined in Self-Test and RN Boot Problems. If these solutions don’t work, contact Quorum Support.

13.23.3 A1003

Message: The automated self-test of *RNName* running on *ApplianceName* was terminated before completion due to resource constraints. Self-test will continue when sufficient resources are available.

Cause: Possible causes are:

- onQ doesn’t have sufficient resources; as such, self-test termination is expected behavior. The self-test will work next time.
- The same or a different RN was brought up in production mode. Any running self-tests terminate immediately.

Solution: If there are insufficient resources, you don’t need to do anything: the self-test will restart on its own. If due to another RN in production, the self-tests will not run until you turn off the RN in production mode.

3.

14

User Management

14.1 Add users

By default, the onQ Appliance provides pre-defined user names (`VARAdmin`, `Admin`, `onQRestore`, `Operator`, and `archiveuser`.

However, you can add to this list if you have additional administrators that need access to the onQ Appliance; for auditing purposes, this approach is a best practice.

To add a user:

1. Log on to either the HA's onQ Portal or the DR Appliance's onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **Users** page.

   You see the list of users at or below your login privilege level.
3. Click the plus button (**+**).
4. Specify username and password. User names are not case sensitive, but passwords are case sensitive.
5. Choose a user role:

   User roles provide the privileges for a user. By default, onQ provides pre-defined user roles:
   - **Administrator** - can add/modify PN configurations (i.e. change backup parameters), but cannot set up the onQ Appliance. In addtion, users with this role can upload packages.
   - **Monitor** - cannot make changes (read-only).
   - **Operator** - cannot make changes (read-only), but can start RNs.

- **Restore** - can set up a share. This role is used by onQ only; you cannot assign users this role.
- **VARAdmin** - can do anything, the only one that can modify/reconfigure the onQ Appliance (software, settings). VAR is short for Value-Added Reseller. If you use Hybrid Cloud, you cannot assign users this role. This user cannot be deleted.

6. Specify a timeout value, then **SAVE**.

   onQ automatically logs off this user after this many seconds of inactivity. For security purposes, don’t set `Admin` or `VARAdmin` to `0`, which means never automatically log off. Ideally, retain the default of `300` seconds.

Related Topics

Delete users

14.2 Delete users

You cannot delete the pre-defined users named *archiveuser* or *VARAdmin*.

To delete a user:

1. Log on to either the HA Appliance’s onQ Portal or the DR Appliance’s onQ Portal.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **Users** page.
3. Select a user, then click the minus button (**-**).
4. Click **Yes** to confirm.

Related Topics

Add users

14.3 Change user passwords

For security purposes, the default password for your Appliance(s) cannot be made public. If you do not know your default password, contact Quorum Support.

When you first configured your Appliance(s), you logged on as `VARAdmin` or, in the case of Hybrid Cloud, `Admin` using the default password.

After you configure your Appliance(s) and, if applicable, the onQ Archive Vault, you must immediately change the default passwords for these users. The user ID is not case-sensitive, but the password is case sensitive.

Note: It is critical that you remember your VARAdmin password: Quorum Support cannot recover it and cannot perform certain support tasks without it. VARAdmin is not needed for day-to-day administration and operation. This caveat does not apply to Hybrid Cloud users as you do not have access to VARAdmin credentials.

To change a user password:

1. Log on to the HA's onQ Portal or the DR Appliance's onQ Portal as `VARAdmin`, or `Admin`. Each Appliance has its own password.
2. Go to **APPLIANCE CONFIG** tab > **ADVANCED** button > **Users** page.
3. Select a user, then **MODIFY**.
4. Specify a new username and password.

   Best practice is to use a strong password.

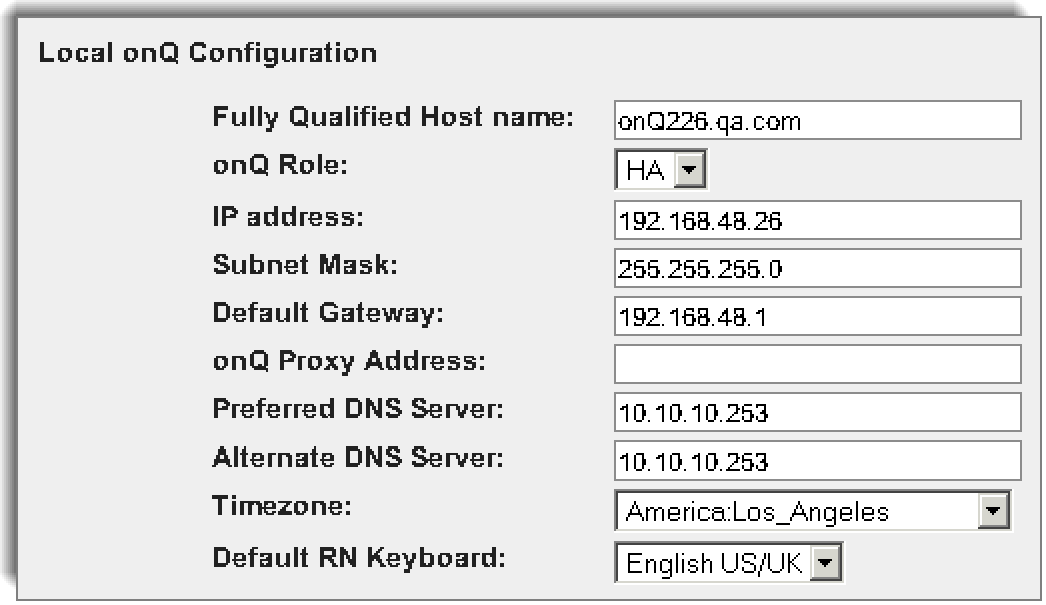
15

Example Configurations

15.1 Local onQ Appliance Configurations

- Local: Example of DR Appliance
- Local: Example of DR Mirror

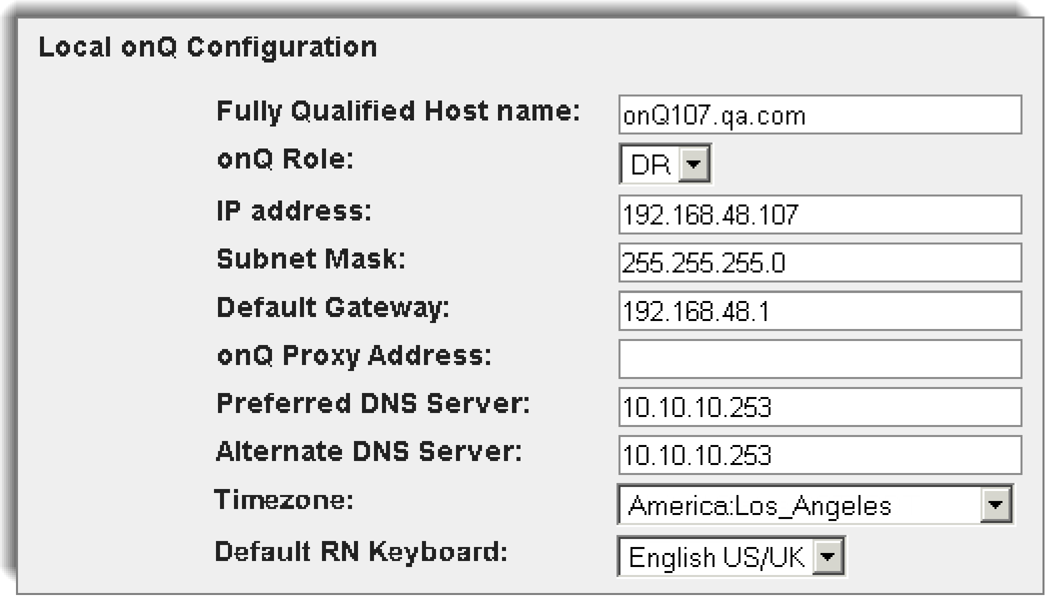
15.1.1 Local: Example of HA



Local onQ Configuration

Fully Qualified Host name:	onQ226.qa.com
onQ Role:	HA
IP address:	192.168.48.26
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.48.1
onQ Proxy Address:	
Preferred DNS Server:	10.10.10.253
Alternate DNS Server:	10.10.10.253
Timezone:	America:Los_Angeles
Default RN Keyboard:	English US/UK

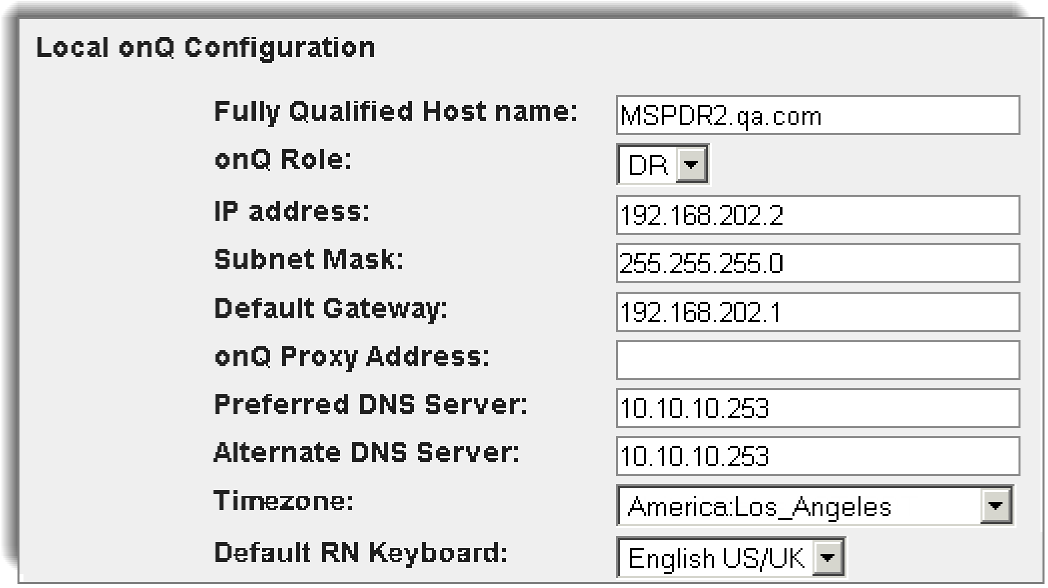
15.1.2 Local: Example of DR Appliance



Local onQ Configuration

Fully Qualified Host name:	onQ107.qa.com
onQ Role:	DR
IP address:	192.168.48.107
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.48.1
onQ Proxy Address:	
Preferred DNS Server:	10.10.10.253
Alternate DNS Server:	10.10.10.253
Timezone:	America:Los_Angeles
Default RN Keyboard:	English US/UK

15.1.3 Local: Example of DR Mirror



Local onQ Configuration

Fully Qualified Host name:	MSPDR2.qa.com
onQ Role:	DR
IP address:	192.168.202.2
Subnet Mask:	255.255.255.0
Default Gateway:	192.168.202.1
onQ Proxy Address:	
Preferred DNS Server:	10.10.10.253
Alternate DNS Server:	10.10.10.253
Timezone:	America:Los_Angeles
Default RN Keyboard:	English US/UK

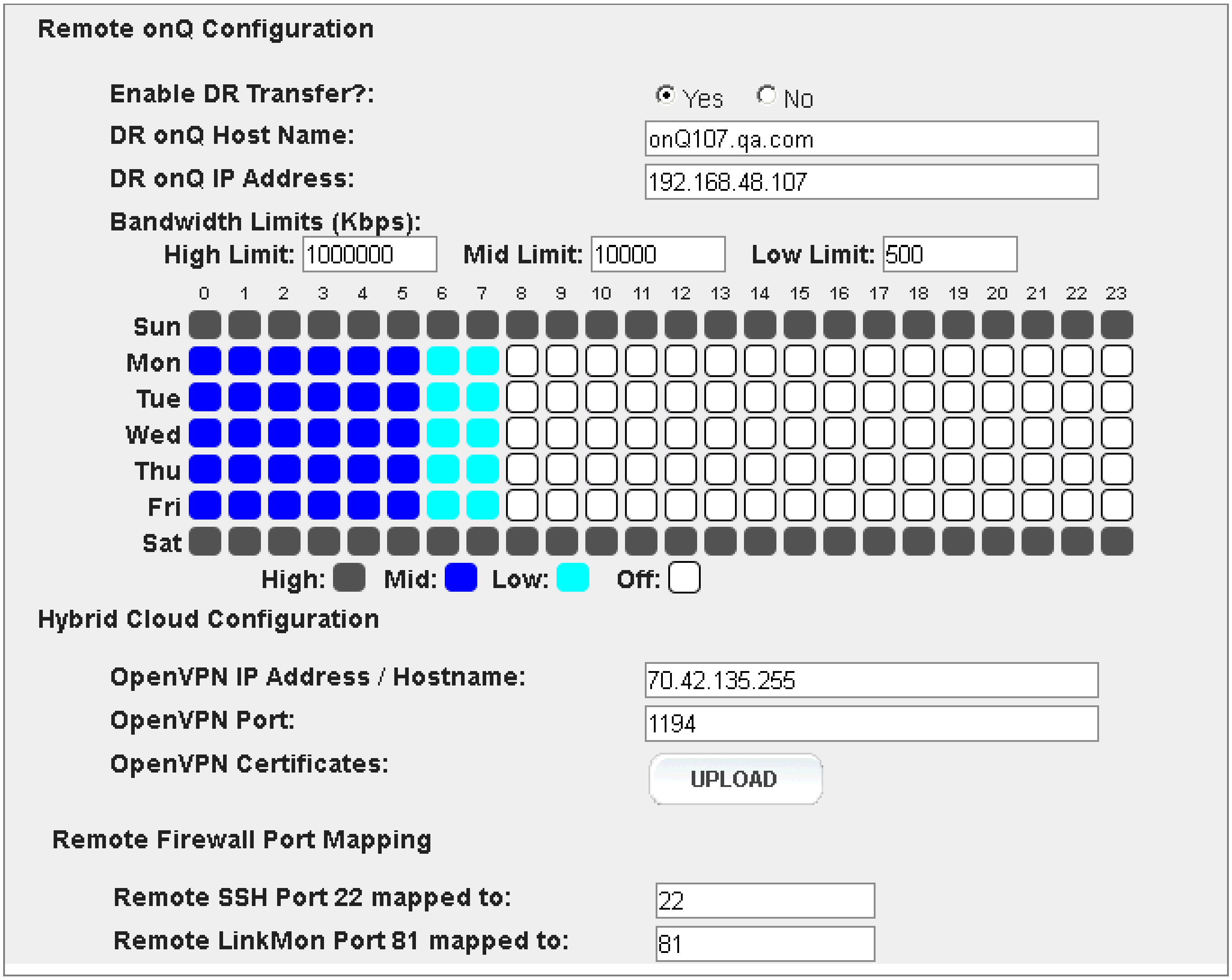
15.2 Remote onQ Appliance Configurations

- Remote: Example of HA with Hybrid Cloud
- Remote: Example of HA with Remote DR Appliance
- Remote: Example of DR Appliance with DR Mirror
- Remote: Example of DR Mirror

15.2.1 Remote: Example of HA with Hybrid Cloud

In order for the HA Appliance to communicate with the DR Appliance, via a secure VPN connection, you must provide the following information for the remote Appliance.

- DR onQ IP Address/Hostname - Quorum-assigned private IP address. If you do not know your IP address, contact Quorum Support.
- OpenVPN IP Address/Hostname - Quorum-assigned public IP address so that the HA Appliance can VPN to the DR Appliance. If you do not know your IP address, contact Quorum Support.
- DR OpenVPN Port - 1194
- OpenVPN Certificates - Quorum-provided certificates. In some cases, Quorum Support might upload these for you in advance.



Remote onQ Configuration

Enable DR Transfer?: ● Yes ○ No

DR onQ Host Name: onQ107.qa.com

DR onQ IP Address: 192.168.48.107

Bandwidth Limits (Kbps):

High Limit: 1000000 Mid Limit: 10000 Low Limit: 500

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛
Mon	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Tue	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Wed	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Thu	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Fri	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Sat	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛

High: ⬛ Mid: 🟦 Low: ▨ Off: □

Hybrid Cloud Configuration

OpenVPN IP Address / Hostname: 70.42.135.255

OpenVPN Port: 1194

OpenVPN Certificates:

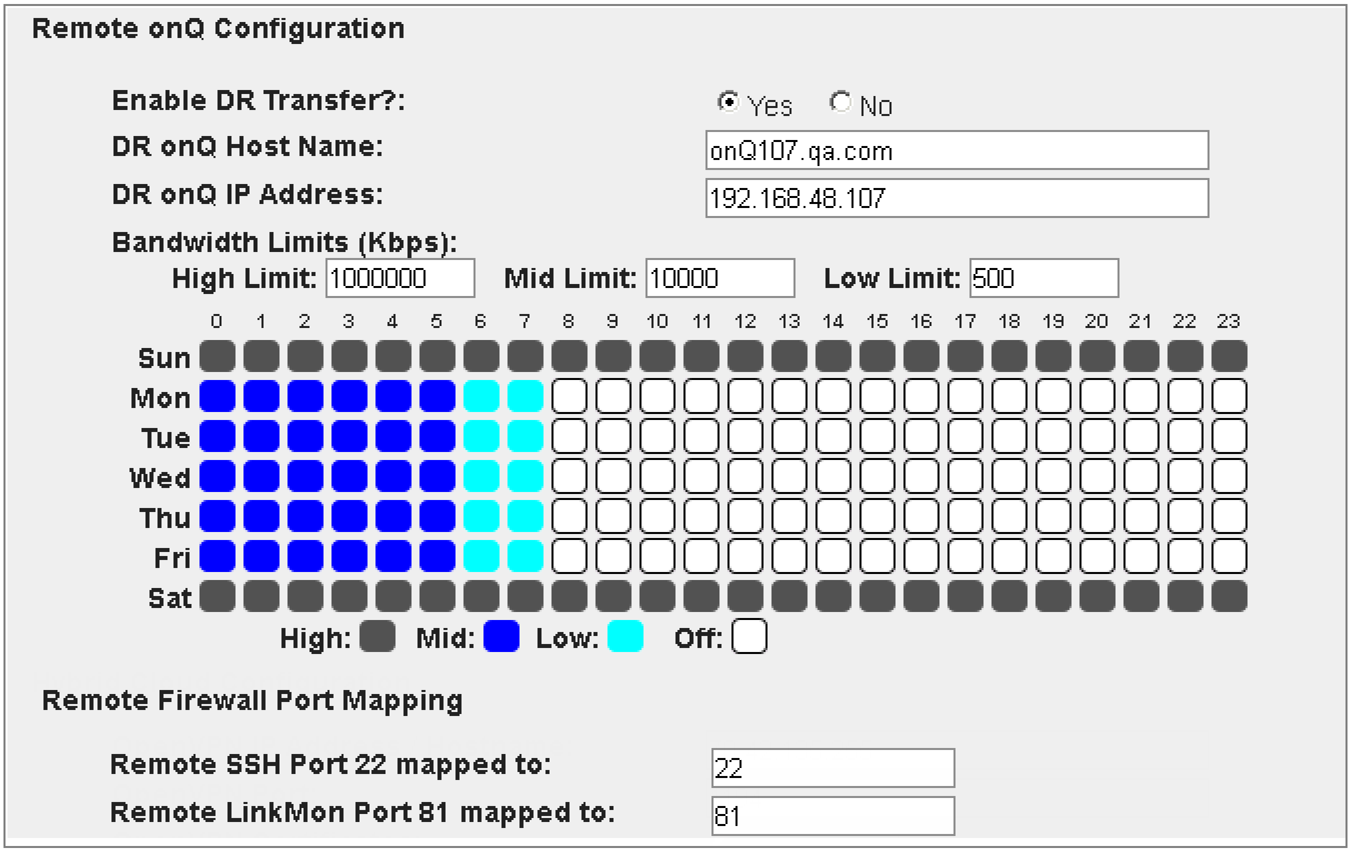
Remote Firewall Port Mapping

Remote SSH Port 22 mapped to: 22

Remote LinkMon Port 81 mapped to: 81

15.2.2 Remote: Example of HA with Remote DR Appliance

Warning: Enable DR Transfer?. After an initial configuration, do not disable DR transfers as outlined in Disable replication globally. If you do so, your repositories will be out of sync.



Remote onQ Configuration

Enable DR Transfer?: ● Yes ○ No

DR onQ Host Name: onQ107.qa.com

DR onQ IP Address: 192.168.48.107

Bandwidth Limits (Kbps):

High Limit: 1000000 Mid Limit: 10000 Low Limit: 500

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Mon	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Tue	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Wed	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Thu	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Fri	🟦	🟦	🟦	🟦	🟦	🟦	▨	▨	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
Sat	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

High: ■ Mid: 🟦 Low: ▨ Off: □

Remote Firewall Port Mapping

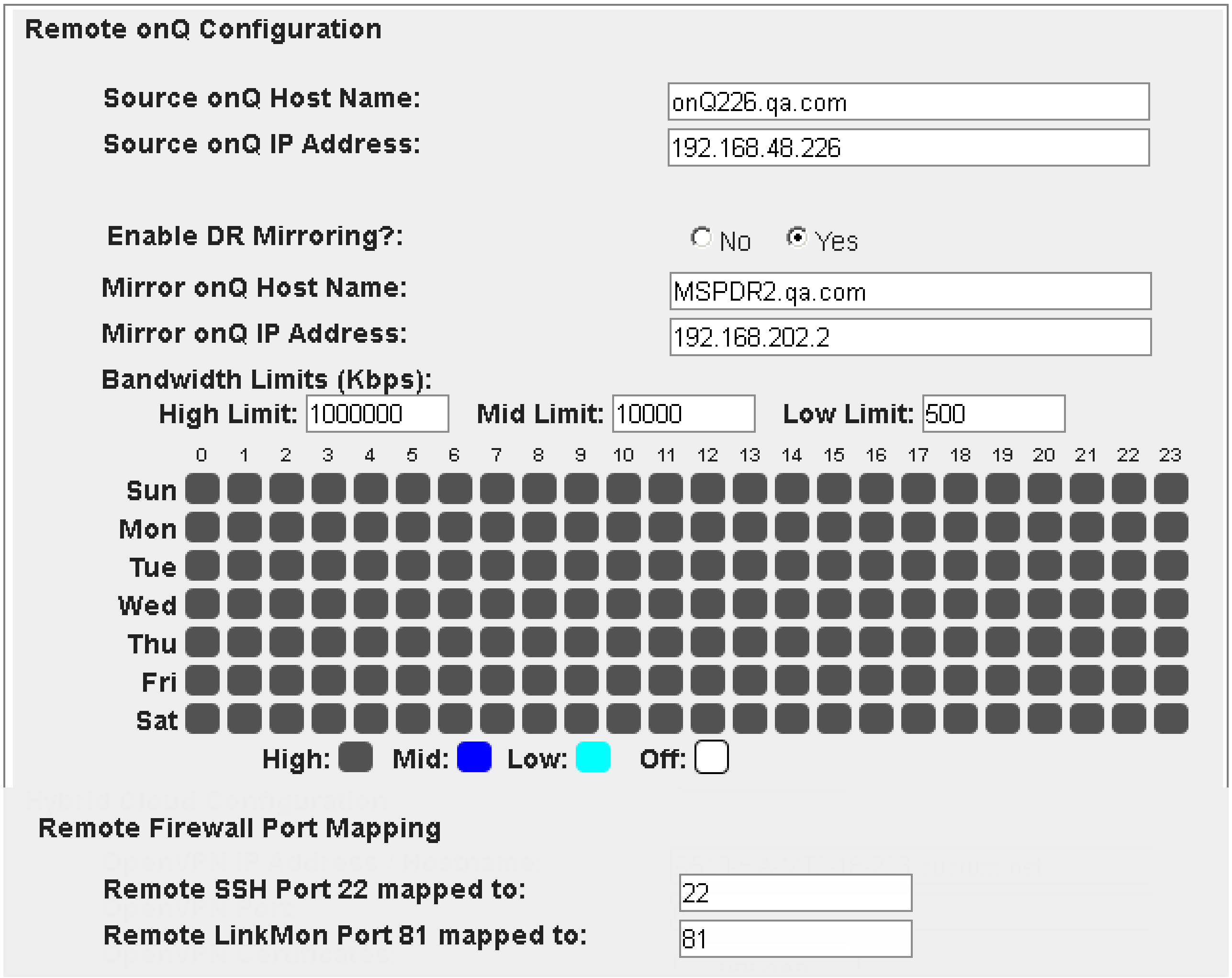
Remote SSH Port 22 mapped to: 22

Remote LinkMon Port 81 mapped to: 81

15.2.3 Remote: Example of DR Appliance with DR Mirror

Warning: Enable DR Mirroring? After an initial configuration, do not disable DR mirroring as outlined in Enable and disable DR Mirroring. If you do so, your repositories will be out of sync.

Warning: Do not use HA information in place of DR mirroring information. Doing so creates an endless loop between HA and DR Appliance.



Remote onQ Configuration

Source onQ Host Name: onQ226.qa.com

Source onQ IP Address: 192.168.48.226

Enable DR Mirroring?: ○ No ● Yes

Mirror onQ Host Name: MSPDR2.qa.com

Mirror onQ IP Address: 192.168.202.2

Bandwidth Limits (Kbps):

High Limit: 1000000 Mid Limit: 10000 Low Limit: 500

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Mon	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Tue	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Wed	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Thu	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Fri	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
Sat	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■

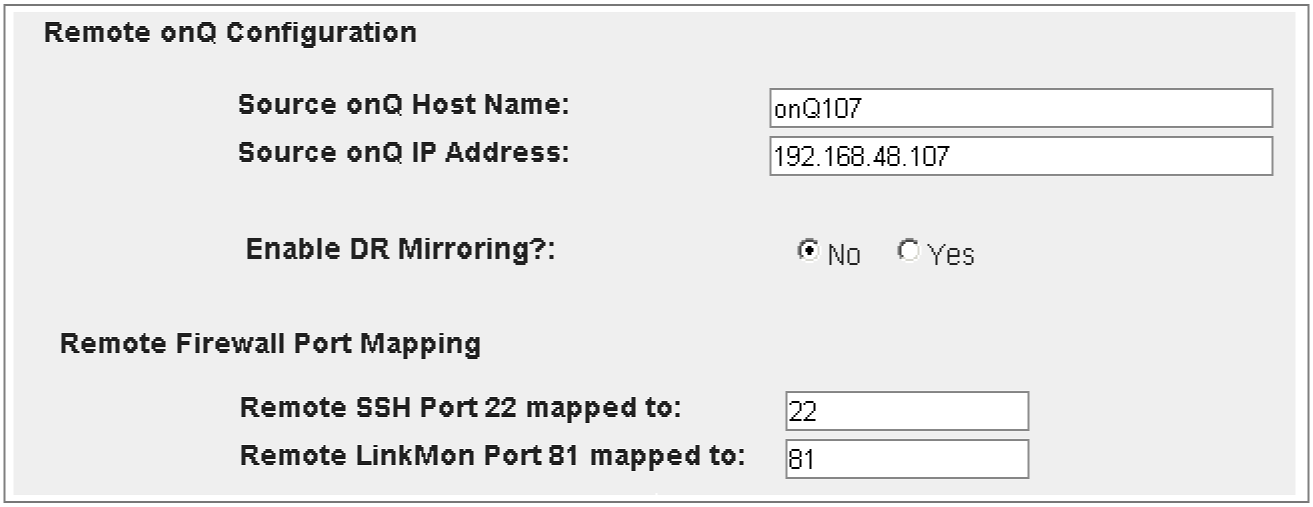
High: ■ Mid: 🟦 Low: ▧ Off: □

Remote Firewall Port Mapping

Remote SSH Port 22 mapped to: 22

Remote LinkMon Port 81 mapped to: 81

15.2.4 Remote: Example of DR Mirror



Remote onQ Configuration

Source onQ Host Name: onQ107

Source onQ IP Address: 192.168.48.107

Enable DR Mirroring?: ● No ○ Yes

Remote Firewall Port Mapping

Remote SSH Port 22 mapped to: 22

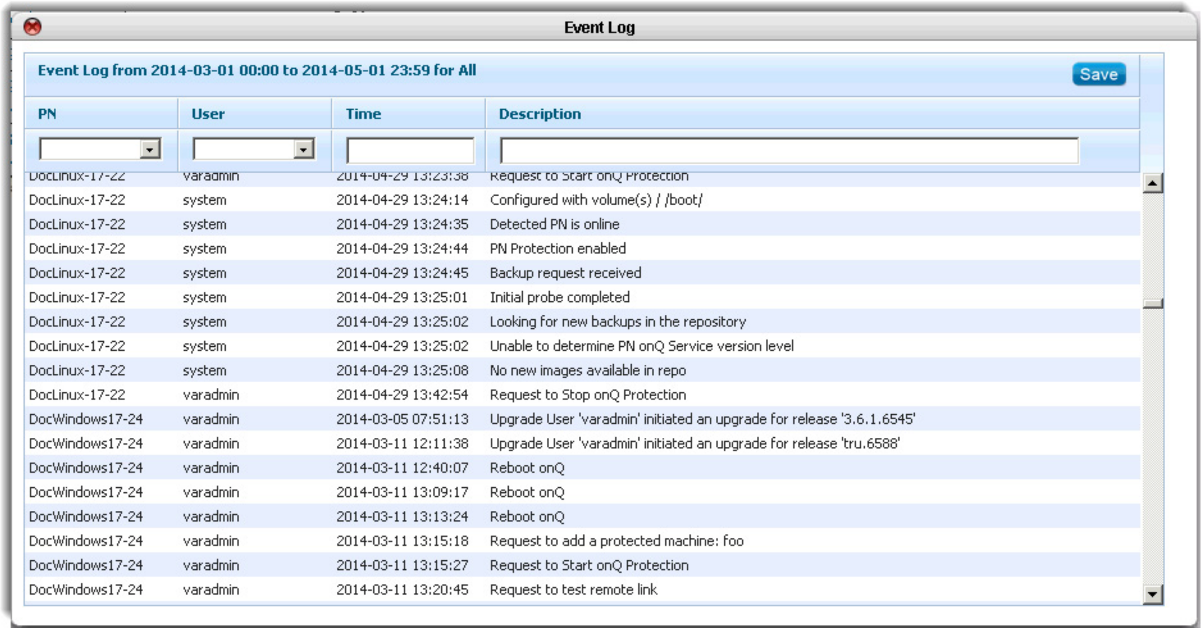
Remote LinkMon Port 81 mapped to: 81

16

Example Logs

The following screen shots represent example logs.

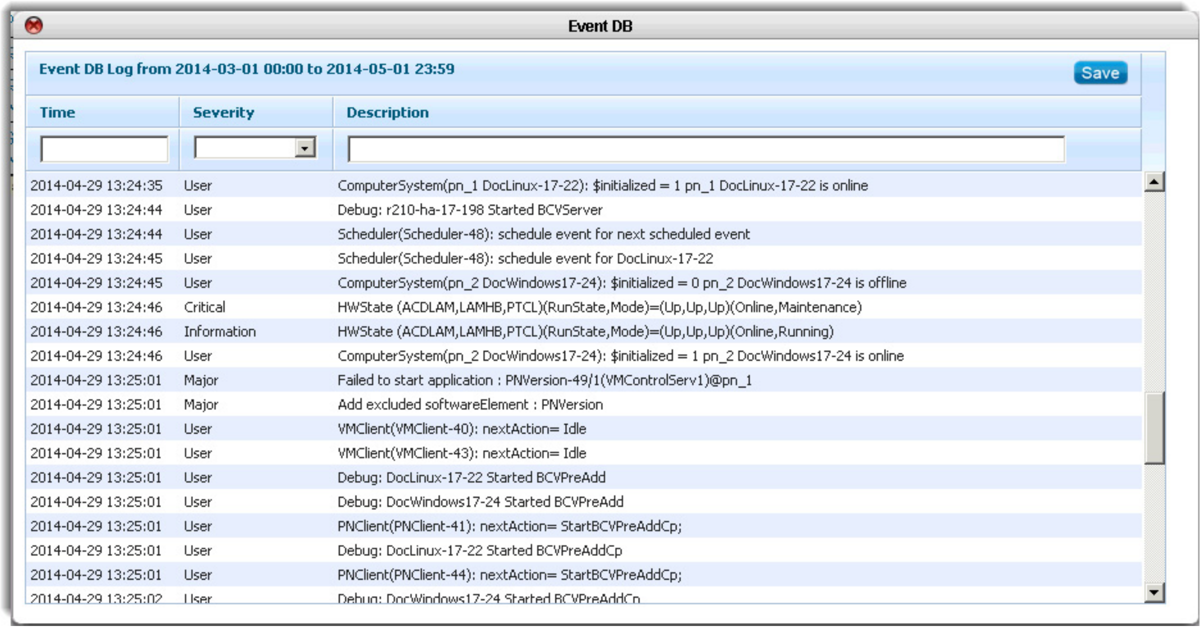
16.1 Example Event Log



Event Log from 2014-03-01 00:00 to 2014-05-01 23:59 for All

PN	User	Time	Description
DocLinux-17-22	varadmin	2014-04-29 13:23:38	Request to Start onQ Protection
DocLinux-17-22	system	2014-04-29 13:24:14	Configured with volume(s) / /boot/
DocLinux-17-22	system	2014-04-29 13:24:35	Detected PN is online
DocLinux-17-22	system	2014-04-29 13:24:44	PN Protection enabled
DocLinux-17-22	system	2014-04-29 13:24:45	Backup request received
DocLinux-17-22	system	2014-04-29 13:25:01	Initial probe completed
DocLinux-17-22	system	2014-04-29 13:25:02	Looking for new backups in the repository
DocLinux-17-22	system	2014-04-29 13:25:02	Unable to determine PN onQ Service version level
DocLinux-17-22	system	2014-04-29 13:25:08	No new images available in repo
DocLinux-17-22	varadmin	2014-04-29 13:42:54	Request to Stop onQ Protection
DocWindows17-24	varadmin	2014-03-05 07:51:13	Upgrade User 'varadmin' initiated an upgrade for release '3.6.1.6545'
DocWindows17-24	varadmin	2014-03-11 12:11:38	Upgrade User 'varadmin' initiated an upgrade for release 'tru.6588'
DocWindows17-24	varadmin	2014-03-11 12:40:07	Reboot onQ
DocWindows17-24	varadmin	2014-03-11 13:09:17	Reboot onQ
DocWindows17-24	varadmin	2014-03-11 13:13:24	Reboot onQ
DocWindows17-24	varadmin	2014-03-11 13:15:18	Request to add a protected machine: foo
DocWindows17-24	varadmin	2014-03-11 13:15:27	Request to Start onQ Protection
DocWindows17-24	varadmin	2014-03-11 13:20:45	Request to test remote link

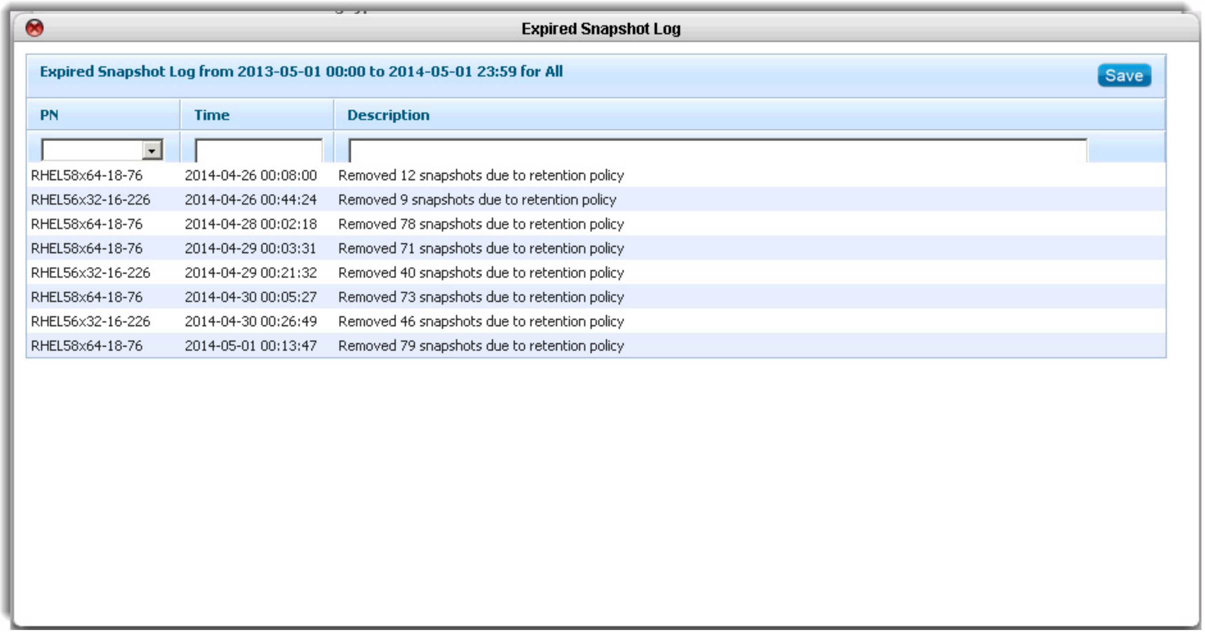
16.2 Example Event DB Log



Event DB Log from 2014-03-01 00:00 to 2014-05-01 23:59

Time	Severity	Description
2014-04-29 13:24:35	User	ComputerSystem(pn_1 DocLinux-17-22): $initialized = 1 pn_1 DocLinux-17-22 is online
2014-04-29 13:24:44	User	Debug: r210-ha-17-198 Started BCVServer
2014-04-29 13:24:44	User	Scheduler(Scheduler-48): schedule event for next scheduled event
2014-04-29 13:24:45	User	Scheduler(Scheduler-48): schedule event for DocLinux-17-22
2014-04-29 13:24:45	User	ComputerSystem(pn_2 DocWindows17-24): $initialized = 0 pn_2 DocWindows17-24 is offline
2014-04-29 13:24:46	Critical	HWState (ACDLAM,LAMHB,PTCL)(RunState,Mode)=(Up,Up,Up)(Online,Maintenance)
2014-04-29 13:24:46	Information	HWState (ACDLAM,LAMHB,PTCL)(RunState,Mode)=(Up,Up,Up)(Online,Running)
2014-04-29 13:24:46	User	ComputerSystem(pn_2 DocWindows17-24): $initialized = 1 pn_2 DocWindows17-24 is online
2014-04-29 13:25:01	Major	Failed to start application : PNVersion-49/1(VMControlServ1)@pn_1
2014-04-29 13:25:01	Major	Add excluded softwareElement : PNVersion
2014-04-29 13:25:01	User	VMClient(VMClient-40): nextAction= Idle
2014-04-29 13:25:01	User	VMClient(VMClient-43): nextAction= Idle
2014-04-29 13:25:01	User	Debug: DocLinux-17-22 Started BCVPreAdd
2014-04-29 13:25:01	User	Debug: DocWindows17-24 Started BCVPreAdd
2014-04-29 13:25:01	User	PNClient(PNClient-41): nextAction= StartBCVPreAddCp;
2014-04-29 13:25:01	User	Debug: DocLinux-17-22 Started BCVPreAddCp
2014-04-29 13:25:01	User	PNClient(PNClient-44): nextAction= StartBCVPreAddCp;
2014-04-29 13:25:02	User	Debug: DocWindows17-24 Started BCVPreAddCp

16.3 Example Expired Snapshot Log



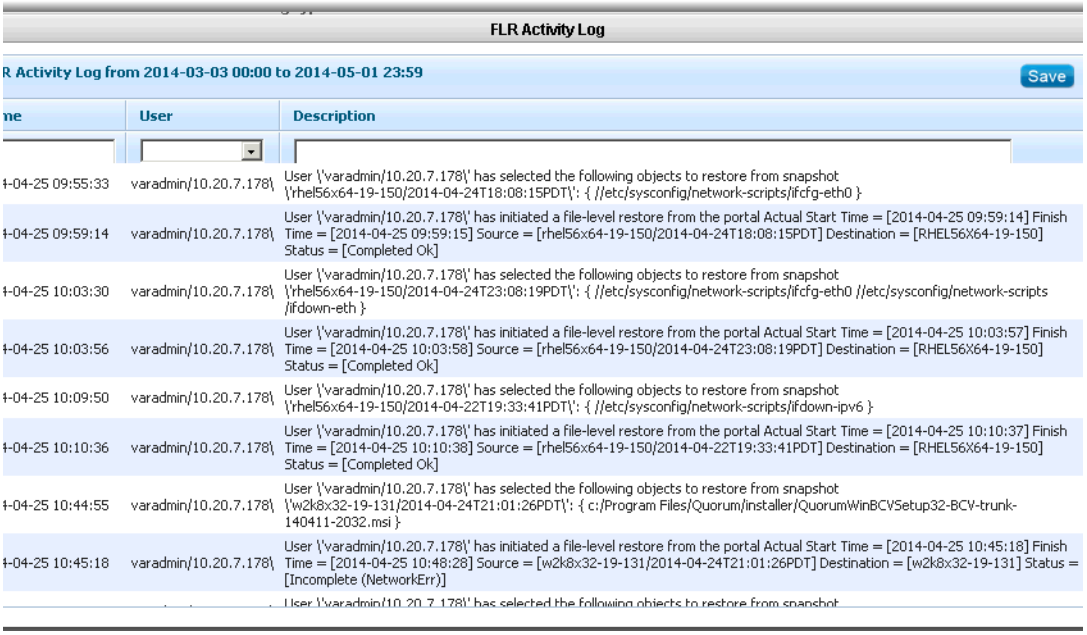
Expired Snapshot Log from 2013-05-01 00:00 to 2014-05-01 23:59 for All

PN	Time	Description
RHEL58x64-18-76	2014-04-26 00:08:00	Removed 12 snapshots due to retention policy
RHEL56x32-16-226	2014-04-26 00:44:24	Removed 9 snapshots due to retention policy
RHEL58x64-18-76	2014-04-28 00:02:18	Removed 78 snapshots due to retention policy
RHEL58x64-18-76	2014-04-29 00:03:31	Removed 71 snapshots due to retention policy
RHEL56x32-16-226	2014-04-29 00:21:32	Removed 40 snapshots due to retention policy
RHEL58x64-18-76	2014-04-30 00:05:27	Removed 73 snapshots due to retention policy
RHEL56x32-16-226	2014-04-30 00:26:49	Removed 46 snapshots due to retention policy
RHEL58x64-18-76	2014-05-01 00:13:47	Removed 79 snapshots due to retention policy

16.4 Example FLR Activity Log

If you'd like to see a graphical representation of this data, consider using the

Restore Detail Report outlined in Generate on-demand reports.

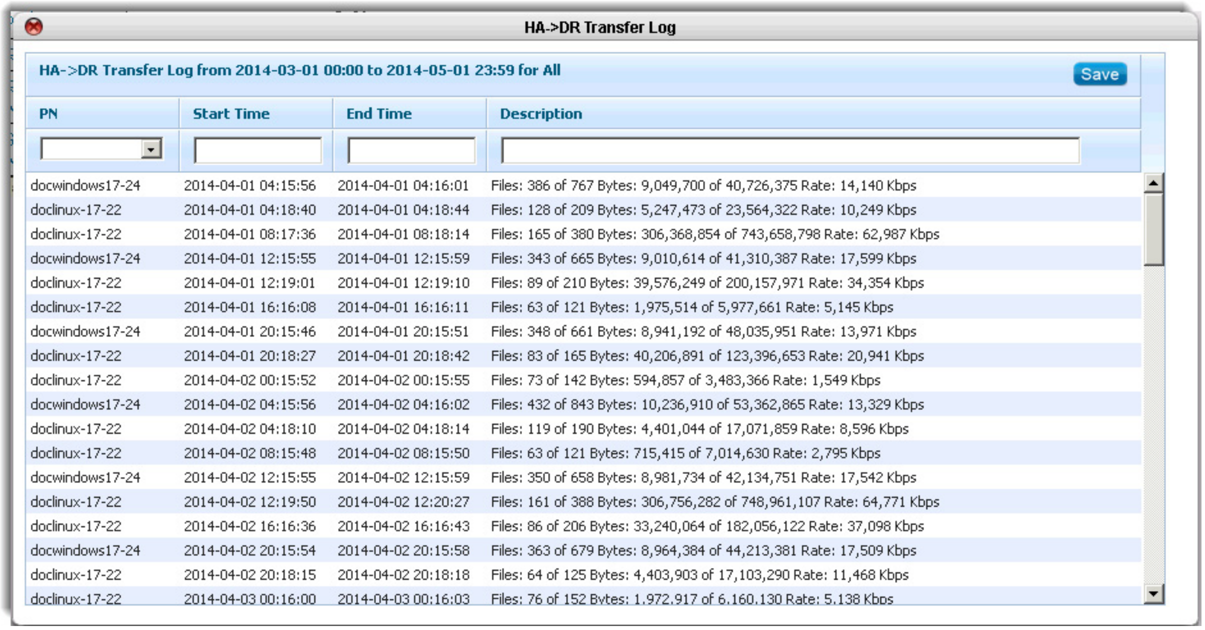


FLR Activity Log

R Activity Log from 2014-03-03 00:00 to 2014-05-01 23:59

ne	User	Description
4-04-25 09:55:33	varadmin/10.20.7.178\	User \'varadmin/10.20.7.178\' has selected the following objects to restore from snapshot \'rhel56x64-19-150/2014-04-24T18:08:15PDT\': { //etc/sysconfig/network-scripts/ifcfg-eth0 }
4-04-25 09:59:14	varadmin/10.20.7.178\	User \'varadmin/10.20.7.178\' has initiated a file-level restore from the portal Actual Start Time = [2014-04-25 09:59:14] Finish Time = [2014-04-25 09:59:15] Source = [rhel56x64-19-150/2014-04-24T18:08:15PDT] Destination = [RHEL56X64-19-150] Status = [Completed Ok]
4-04-25 10:03:30	varadmin/10.20.7.178\	User \'varadmin/10.20.7.178\' has selected the following objects to restore from snapshot \'rhel56x64-19-150/2014-04-24T23:08:19PDT\': { //etc/sysconfig/network-scripts/ifcfg-eth0 //etc/sysconfig/network-scripts /ifdown-eth }
4-04-25 10:03:56	varadmin/10.20.7.178\	User \'varadmin/10.20.7.178\' has initiated a file-level restore from the portal Actual Start Time = [2014-04-25 10:03:57] Finish Time = [2014-04-25 10:03:58] Source = [rhel56x64-19-150/2014-04-24T23:08:19PDT] Destination = [RHEL56X64-19-150] Status = [Completed Ok]
4-04-25 10:09:50	varadmin/10.20.7.178\	User \'varadmin/10.20.7.178\' has selected the following objects to restore from snapshot \'rhel56x64-19-150/2014-04-22T19:33:41PDT\': { //etc/sysconfig/network-scripts/ifdown-ipv6 }
4-04-25 10:10:36	varadmin/10.20.7.178\	User \'varadmin/10.20.7.178\' has initiated a file-level restore from the portal Actual Start Time = [2014-04-25 10:10:37] Finish Time = [2014-04-25 10:10:38] Source = [rhel56x64-19-150/2014-04-22T19:33:41PDT] Destination = [RHEL56X64-19-150] Status = [Completed Ok]
4-04-25 10:44:55	varadmin/10.20.7.178\	User \'varadmin/10.20.7.178\' has selected the following objects to restore from snapshot \'w2k8x32-19-131/2014-04-24T21:01:26PDT\': { c:/Program Files/Quorum/installer/QuorumWinBCVSetup32-BCV-trunk-140411-2032.msi }
4-04-25 10:45:18	varadmin/10.20.7.178\	User \'varadmin/10.20.7.178\' has initiated a file-level restore from the portal Actual Start Time = [2014-04-25 10:45:18] Finish Time = [2014-04-25 10:48:28] Source = [w2k8x32-19-131/2014-04-24T21:01:26PDT] Destination = [w2k8x32-19-131] Status = [Incomplete (NetworkErr)]
		User \'varadmin/10.20.7.178\' has selected the following objects to restore from snapshot

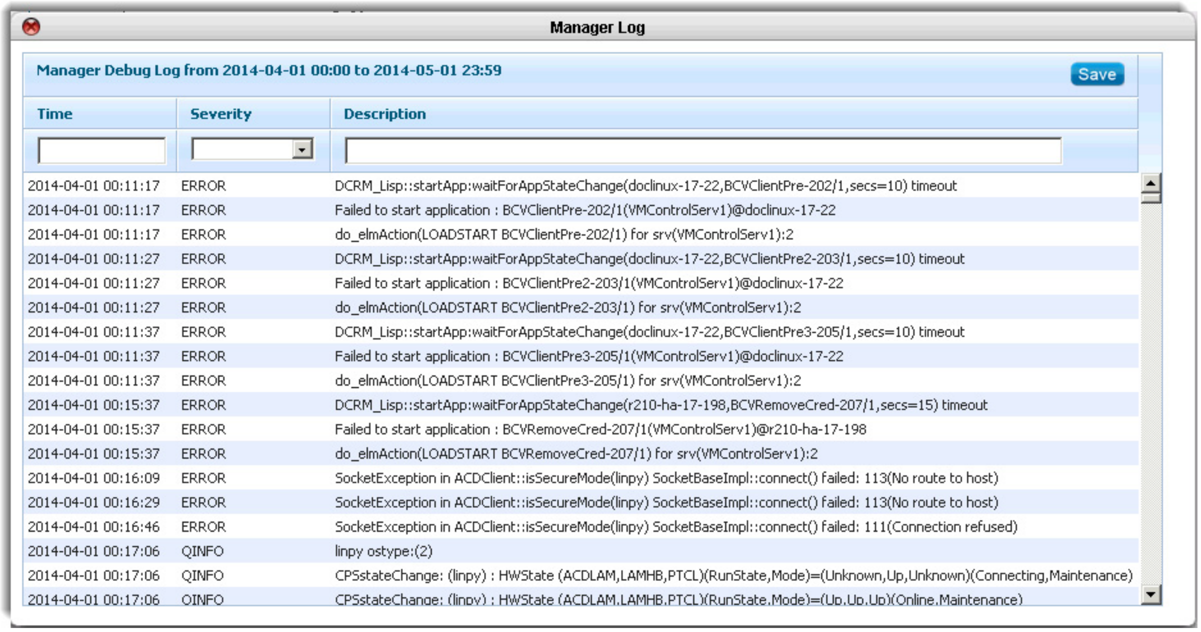
16.5 Example HA -> DR Transfer Log



HA->DR Transfer Log from 2014-03-01 00:00 to 2014-05-01 23:59 for All

PN	Start Time	End Time	Description
docwindows17-24	2014-04-01 04:15:56	2014-04-01 04:16:01	Files: 386 of 767 Bytes: 9,049,700 of 40,726,375 Rate: 14,140 Kbps
doclinux-17-22	2014-04-01 04:18:40	2014-04-01 04:18:44	Files: 128 of 209 Bytes: 5,247,473 of 23,564,322 Rate: 10,249 Kbps
doclinux-17-22	2014-04-01 08:17:36	2014-04-01 08:18:14	Files: 165 of 380 Bytes: 306,368,854 of 743,658,798 Rate: 62,987 Kbps
docwindows17-24	2014-04-01 12:15:55	2014-04-01 12:15:59	Files: 343 of 665 Bytes: 9,010,614 of 41,310,387 Rate: 17,599 Kbps
doclinux-17-22	2014-04-01 12:19:01	2014-04-01 12:19:10	Files: 89 of 210 Bytes: 39,576,249 of 200,157,971 Rate: 34,354 Kbps
doclinux-17-22	2014-04-01 16:16:08	2014-04-01 16:16:11	Files: 63 of 121 Bytes: 1,975,514 of 5,977,661 Rate: 5,145 Kbps
docwindows17-24	2014-04-01 20:15:46	2014-04-01 20:15:51	Files: 348 of 661 Bytes: 8,941,192 of 48,035,951 Rate: 13,971 Kbps
doclinux-17-22	2014-04-01 20:18:27	2014-04-01 20:18:42	Files: 83 of 165 Bytes: 40,206,891 of 123,396,653 Rate: 20,941 Kbps
doclinux-17-22	2014-04-02 00:15:52	2014-04-02 00:15:55	Files: 73 of 142 Bytes: 594,857 of 3,483,366 Rate: 1,549 Kbps
docwindows17-24	2014-04-02 04:15:56	2014-04-02 04:16:02	Files: 432 of 843 Bytes: 10,236,910 of 53,362,865 Rate: 13,329 Kbps
doclinux-17-22	2014-04-02 04:18:10	2014-04-02 04:18:14	Files: 119 of 190 Bytes: 4,401,044 of 17,071,859 Rate: 8,596 Kbps
doclinux-17-22	2014-04-02 08:15:48	2014-04-02 08:15:50	Files: 63 of 121 Bytes: 715,415 of 7,014,630 Rate: 2,795 Kbps
docwindows17-24	2014-04-02 12:15:55	2014-04-02 12:15:59	Files: 350 of 658 Bytes: 8,981,734 of 42,134,751 Rate: 17,542 Kbps
doclinux-17-22	2014-04-02 12:19:50	2014-04-02 12:20:27	Files: 161 of 388 Bytes: 306,756,282 of 748,961,107 Rate: 64,771 Kbps
doclinux-17-22	2014-04-02 16:16:36	2014-04-02 16:16:43	Files: 86 of 206 Bytes: 33,240,064 of 182,056,122 Rate: 37,098 Kbps
docwindows17-24	2014-04-02 20:15:54	2014-04-02 20:15:58	Files: 363 of 679 Bytes: 8,964,384 of 44,213,381 Rate: 17,509 Kbps
doclinux-17-22	2014-04-02 20:18:15	2014-04-02 20:18:18	Files: 64 of 125 Bytes: 4,403,903 of 17,103,290 Rate: 11,468 Kbps
doclinux-17-22	2014-04-03 00:16:00	2014-04-03 00:16:03	Files: 76 of 152 Bytes: 1,972,917 of 6,160,130 Rate: 5,138 Kbps

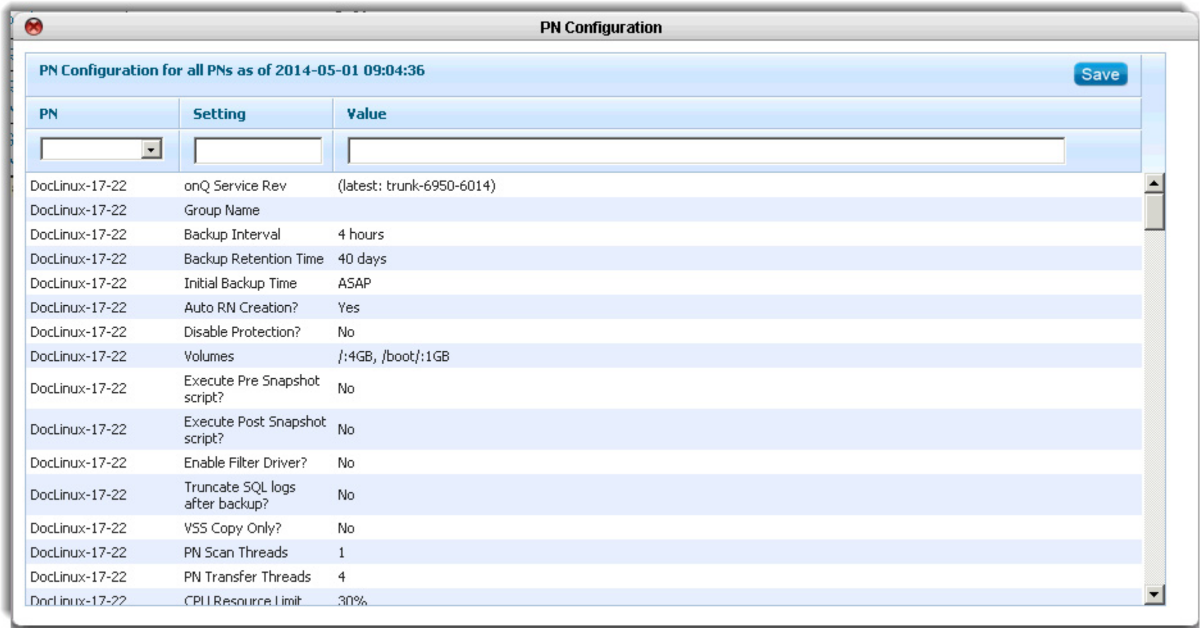
16.6 Example Manager Debug Log



Manager Debug Log from 2014-04-01 00:00 to 2014-05-01 23:59

Time	Severity	Description
2014-04-01 00:11:17	ERROR	DCRM_Lisp::startApp:waitForAppStateChange(doclinux-17-22,BCVClientPre-202/1,secs=10) timeout
2014-04-01 00:11:17	ERROR	Failed to start application : BCVClientPre-202/1(VMControlServ1)@doclinux-17-22
2014-04-01 00:11:17	ERROR	do_elmAction(LOADSTART BCVClientPre-202/1) for srv(VMControlServ1):2
2014-04-01 00:11:27	ERROR	DCRM_Lisp::startApp:waitForAppStateChange(doclinux-17-22,BCVClientPre2-203/1,secs=10) timeout
2014-04-01 00:11:27	ERROR	Failed to start application : BCVClientPre2-203/1(VMControlServ1)@doclinux-17-22
2014-04-01 00:11:27	ERROR	do_elmAction(LOADSTART BCVClientPre2-203/1) for srv(VMControlServ1):2
2014-04-01 00:11:37	ERROR	DCRM_Lisp::startApp:waitForAppStateChange(doclinux-17-22,BCVClientPre3-205/1,secs=10) timeout
2014-04-01 00:11:37	ERROR	Failed to start application : BCVClientPre3-205/1(VMControlServ1)@doclinux-17-22
2014-04-01 00:11:37	ERROR	do_elmAction(LOADSTART BCVClientPre3-205/1) for srv(VMControlServ1):2
2014-04-01 00:15:37	ERROR	DCRM_Lisp::startApp:waitForAppStateChange(r210-ha-17-198,BCVRemoveCred-207/1,secs=15) timeout
2014-04-01 00:15:37	ERROR	Failed to start application : BCVRemoveCred-207/1(VMControlServ1)@r210-ha-17-198
2014-04-01 00:15:37	ERROR	do_elmAction(LOADSTART BCVRemoveCred-207/1) for srv(VMControlServ1):2
2014-04-01 00:16:09	ERROR	SocketException in ACDClient::isSecureMode(linpy) SocketBaseImpl::connect() failed: 113(No route to host)
2014-04-01 00:16:29	ERROR	SocketException in ACDClient::isSecureMode(linpy) SocketBaseImpl::connect() failed: 113(No route to host)
2014-04-01 00:16:46	ERROR	SocketException in ACDClient::isSecureMode(linpy) SocketBaseImpl::connect() failed: 111(Connection refused)
2014-04-01 00:17:06	QINFO	linpy ostype:(2)
2014-04-01 00:17:06	QINFO	CPSstateChange: (linpy) : HWState (ACDLAM,LAMHB,PTCL)(RunState,Mode)=(Unknown,Up,Unknown)(Connecting,Maintenance)
2014-04-01 00:17:06	QINFO	CPSstateChange: (linpy) : HWState (ACDLAM,LAMHB,PTCL)(RunState,Mode)=(Up,Up,Up)(Online,Maintenance)

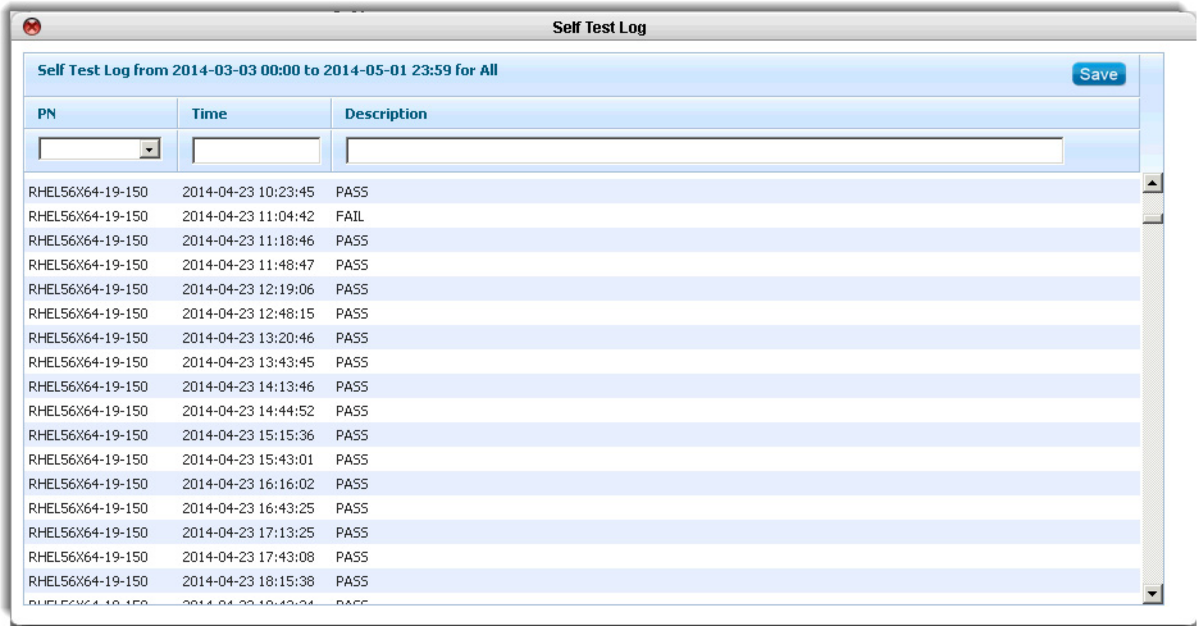
16.7 Example PN Configuration Log



PN Configuration for all PNs as of 2014-05-01 09:04:36

PN	Setting	Value
DocLinux-17-22	onQ Service Rev	(latest: trunk-6950-6014)
DocLinux-17-22	Group Name	
DocLinux-17-22	Backup Interval	4 hours
DocLinux-17-22	Backup Retention Time	40 days
DocLinux-17-22	Initial Backup Time	ASAP
DocLinux-17-22	Auto RN Creation?	Yes
DocLinux-17-22	Disable Protection?	No
DocLinux-17-22	Volumes	/:4GB, /boot/:1GB
DocLinux-17-22	Execute Pre Snapshot script?	No
DocLinux-17-22	Execute Post Snapshot script?	No
DocLinux-17-22	Enable Filter Driver?	No
DocLinux-17-22	Truncate SQL logs after backup?	No
DocLinux-17-22	VSS Copy Only?	No
DocLinux-17-22	PN Scan Threads	1
DocLinux-17-22	PN Transfer Threads	4
DocLinux-17-22	CPU Resource Limit	30%

16.8 Example Self Test Log

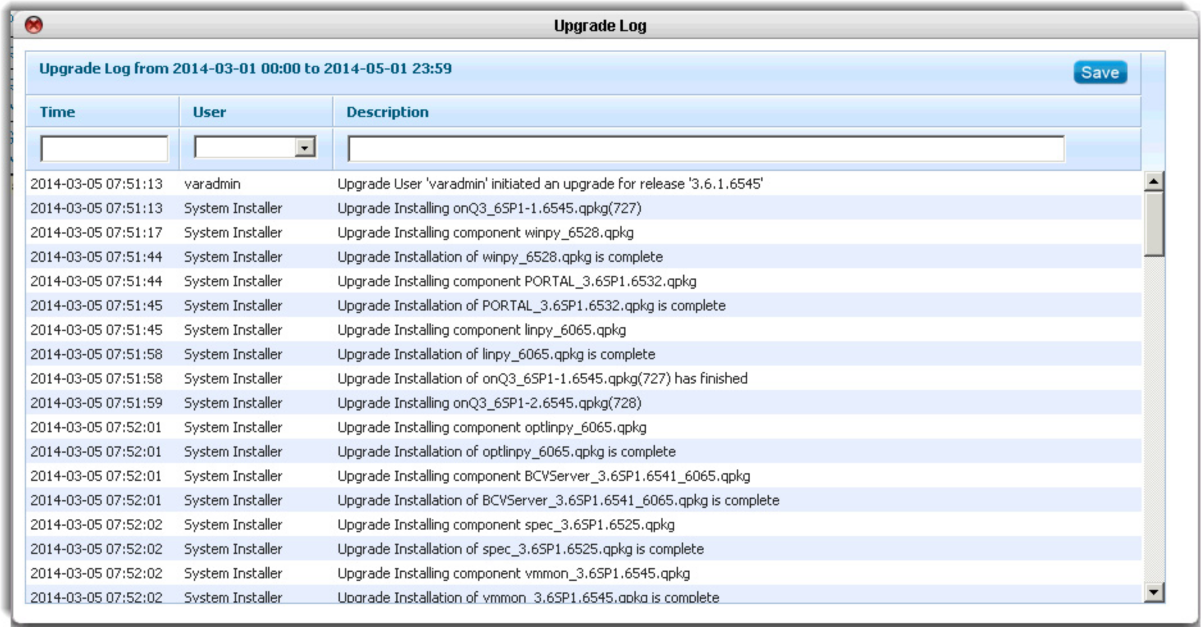


Self Test Log

Self Test Log from 2014-03-03 00:00 to 2014-05-01 23:59 for All

PN	Time	Description
RHEL56X64-19-150	2014-04-23 10:23:45	PASS
RHEL56X64-19-150	2014-04-23 11:04:42	FAIL
RHEL56X64-19-150	2014-04-23 11:18:46	PASS
RHEL56X64-19-150	2014-04-23 11:48:47	PASS
RHEL56X64-19-150	2014-04-23 12:19:06	PASS
RHEL56X64-19-150	2014-04-23 12:48:15	PASS
RHEL56X64-19-150	2014-04-23 13:20:46	PASS
RHEL56X64-19-150	2014-04-23 13:43:45	PASS
RHEL56X64-19-150	2014-04-23 14:13:46	PASS
RHEL56X64-19-150	2014-04-23 14:44:52	PASS
RHEL56X64-19-150	2014-04-23 15:15:36	PASS
RHEL56X64-19-150	2014-04-23 15:43:01	PASS
RHEL56X64-19-150	2014-04-23 16:16:02	PASS
RHEL56X64-19-150	2014-04-23 16:43:25	PASS
RHEL56X64-19-150	2014-04-23 17:13:25	PASS
RHEL56X64-19-150	2014-04-23 17:43:08	PASS
RHEL56X64-19-150	2014-04-23 18:15:38	PASS

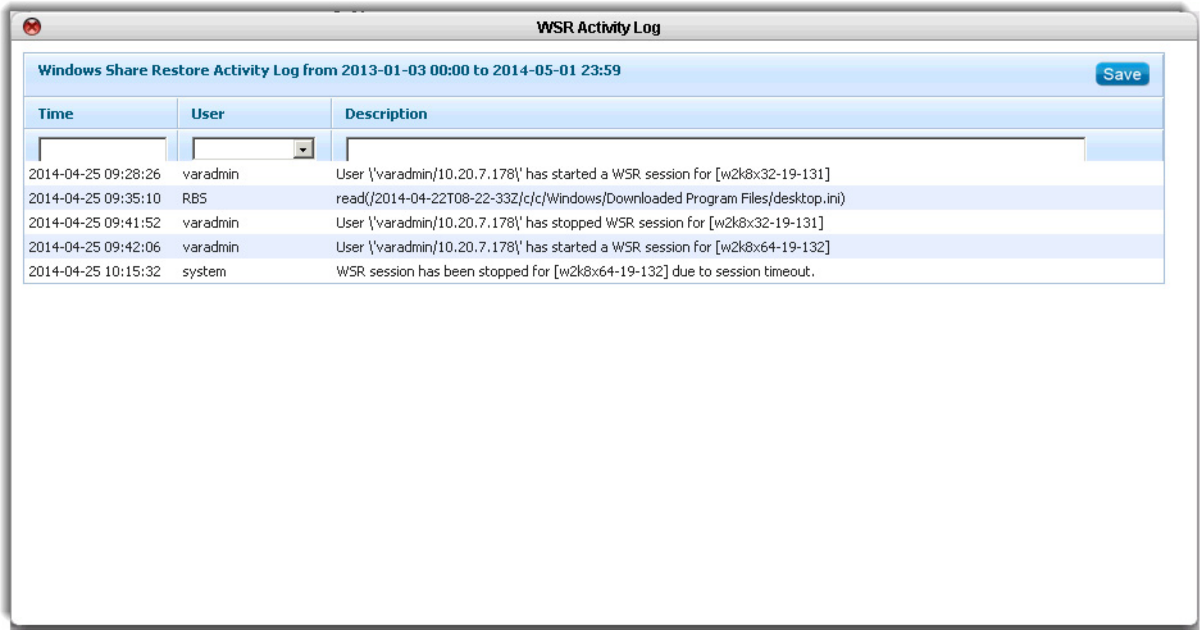
16.9 Example Upgrade Log



Upgrade Log from 2014-03-01 00:00 to 2014-05-01 23:59

Time	User	Description
2014-03-05 07:51:13	varadmin	Upgrade User 'varadmin' initiated an upgrade for release '3.6.1.6545'
2014-03-05 07:51:13	System Installer	Upgrade Installing onQ3_6SP1-1.6545.qpkg(727)
2014-03-05 07:51:17	System Installer	Upgrade Installing component winpy_6528.qpkg
2014-03-05 07:51:44	System Installer	Upgrade Installation of winpy_6528.qpkg is complete
2014-03-05 07:51:44	System Installer	Upgrade Installing component PORTAL_3.6SP1.6532.qpkg
2014-03-05 07:51:45	System Installer	Upgrade Installation of PORTAL_3.6SP1.6532.qpkg is complete
2014-03-05 07:51:45	System Installer	Upgrade Installing component linpy_6065.qpkg
2014-03-05 07:51:58	System Installer	Upgrade Installation of linpy_6065.qpkg is complete
2014-03-05 07:51:58	System Installer	Upgrade Installation of onQ3_6SP1-1.6545.qpkg(727) has finished
2014-03-05 07:51:59	System Installer	Upgrade Installing onQ3_6SP1-2.6545.qpkg(728)
2014-03-05 07:52:01	System Installer	Upgrade Installing component optlinpy_6065.qpkg
2014-03-05 07:52:01	System Installer	Upgrade Installation of optlinpy_6065.qpkg is complete
2014-03-05 07:52:01	System Installer	Upgrade Installing component BCVServer_3.6SP1.6541_6065.qpkg
2014-03-05 07:52:01	System Installer	Upgrade Installation of BCVServer_3.6SP1.6541_6065.qpkg is complete
2014-03-05 07:52:02	System Installer	Upgrade Installing component spec_3.6SP1.6525.qpkg
2014-03-05 07:52:02	System Installer	Upgrade Installation of spec_3.6SP1.6525.qpkg is complete
2014-03-05 07:52:02	System Installer	Upgrade Installing component vmmon_3.6SP1.6545.qpkg
2014-03-05 07:52:02	System Installer	Upgrade Installation of vmmon_3.6SP1.6545.qpkg is complete

16.10 Example WSR Activity Log



Windows Share Restore Activity Log from 2013-01-03 00:00 to 2014-05-01 23:59

Time	User	Description
2014-04-25 09:28:26	varadmin	User \'varadmin/10.20.7.178\' has started a WSR session for [w2k8x32-19-131]
2014-04-25 09:35:10	RBS	read(/2014-04-22T08-22-33Z/c/c/Windows/Downloaded Program Files/desktop.ini)
2014-04-25 09:41:52	varadmin	User \'varadmin/10.20.7.178\' has stopped WSR session for [w2k8x32-19-131]
2014-04-25 09:42:06	varadmin	User \'varadmin/10.20.7.178\' has started a WSR session for [w2k8x64-19-132]
2014-04-25 10:15:32	system	WSR session has been stopped for [w2k8x64-19-132] due to session timeout.

17

Tech Notes

17.1 Install kernel-xen RPM package

RNs that are running Redhat 5.x depend on a kernel-xen RPM package. If you are running Redhat 6.x this package is installed by default; as such, you don't need to perform the following procedure.

Perform this procedure if you enrolled your PNs without having previously installed the kernel-xen RPM package, or if you're attempting to restore a Recovery PN as part of a BMR. Redhat 5.x RNs will not boot without this package.

To install the kernel-xen RPM package:

The following procedure works on `kernel-xen-2.6.18`, and should work for all subsequent revisions.

1. Determine if you need the kernel-xen RPM package and, if so, which package:

   a. Verify the OS version. Again, the PN must be Redhat 5.x version.

```
# cat /etc/redhat-release
Red Hat Enterprise Linux Server release 5.7 (Tikanga)
```

b. Determine if the PN’s OS is 32-bit or 64-bit.

```
# uname -a
Linux RHEL57x64-18-178 2.6.18-274.el5 #1 SMP Fri
Jul 8 17:36:59 EDT 2011 x86_64 x86_64 x86_64
GNU/Linux
```

In this case, `x86_64` means the 64-bit package is required.

2. Download the kernel-xen package for RedHat 5.x PN (x32 or x64).

- For 32-bit, go to http://mirror.centos.org/centos-5/5/os/i386/CentOS/, scroll down to view the complete package name for the latest `kernel-xen` package, then run the following command:

```
# wget
http://mirror.centos.org/centos/5/os/i386/CentOS
/kernel-xen-<latestRelease>-
<latestRevision>.el5.i686.rpm
```

- For 64-bit, go to http://mirror.centos.org/centos-5/5/os/x86_64/CentOS/, scroll down to view the complete package name for the latest `kernel-xen` package, then run the following command:

```
# wget
http://mirror.centos.org/centos/5/os/x86_64/Cent
OS/kernel-xen-<latestRelease>-
<latestRevision>.el5.x86_64.rpm
```

3. Install the kernel-xen package.

- For 32-bit:

```
# rpm -iv kernel-xen-<latestRelease>-
<latestRevision>.el5.i686.rpm
```

- For 64-bit:

```
# rpm -iv kernel-xen-<latestRelease>-
<latestRevision>.el5.x86_64.rpm
```

4. Make the `initrd` file, which will be used to build the RN.

```
#mkinitrd -v -f --preload=xennet --preload=xenblk
--omit-scsi-modules --omit-raid-modules
/boot/initrd-<latestRelease>-
<latestRevision>.el5xen.img.5 <latestRelease>-
<latestRevision>.el5xen
```

5. Make the `/boot/grub/grub.conf.xvf5` file, which signals the RN to use it as grub boot menu.

   The `/boot/grub/grub.conf`.xvf and `/boot/grub/grub.conf.xvf[1-4]` must not be installed because they have higher priority than `/boot/grub/grub.conf.xvf5`.

```
# vi /boot/grub/grub.conf.xvf5
```

6. Cut and paste the following line to the file.

```
# grub.conf generated by Quorum onQ

# The root device path is not important and will
be changed automatically during RN build.

default=0

timeout=5

hiddenmenu

title Red Hat Enterprise Linux Server by Quorum
onQ (<latestRelease>-<latestRevision>.el5xen)

        root (hd0,0)

        kernel /vmlinuz-<latestRelease>-
<latestRevision>.el5xen ro root=/dev/xvda1
rd_NO_LUKS rd_NO_MD rhgb crashkernel=auto
rd_NO_LVM
       initrd /initrd-<latestRelease>-<latestRev-
ision>.el5xen.img.5
```

If you’re performing this procedure on the RN (not the PN), back up and build the RN.

To uninstall the kernel-xen RMP package:

1. Uninstall the kernel-xen rpm:

```
# rpm -e kernel-xen-<latestRelease>-
<latestRevision>.el5
```

2. Remove the `/boot/grub/grub.conf.xvf5` file.

```
# \rm -f /boot/grub/grub.conf.xvf5
```

17.2 Add Company Logo to User Interface

If you’re an OEM, you might want to upload your company’s logo to replace the default Quorum logo. The onQ Portal supports such images in `.png` format. To do so, you must have permissions to access the onQ Appliance’s or onQ Archive Vault’s hypervisor. If you are not an OEM, Quorum discourages making any changes on the hypervisor as such actions are risky and can result in configuration issues.

To replace the default logo:

1. Rename your `.png` logo `oem_logo.png`. Filename must be in lower case letters, including file extension.
2. On each onQ Appliance or onQ Archive Vault, save the file to the `/var/www/html/images` folder .

18

Glossary

onQ Appliance ......A separate hardware component designed to host a specific computing resource. onQ Appliance is a separate computer system hosting a virtualization hypervisor, OS, Quorum-specific monitoring and other software, and sufficient resources to be able to support intermediate backups and when recovery is required, able to run a large number of nodes as virtual machines.

business continuity The totality of policies and actions put in place by a business in order to maintain its operations and relationships with partners and clients even when interruptions or disasters occur.

de-duplication .... The elimination of redundant blocks of data across PNs to reduce storage and bandwidth requirements. De-duplication is important in backup systems where timely recovery is a concern.

disaster recovery .. The ability to recover business systems at an off-site facility in the event of a primary site failure.

DR Appliance .... The DR Appliance provides disaster recovery protection for your nodes. Often the DR Appliance is truly remote, being located in a different geographical location and connected through a separate WAN, but a more important distinction is the role it plays as the provider of disaster recovery protection.

HA Appliance .... The HA is the one connected directly to the network on which the Protected Nodes are located. The HA provides high availability protection.

high availability..... Protection of nodes by onQ located on the same LAN as the nodes it protects. When HA recovery is required, Recovery Nodes are started on the HA.

hypervisor ....hypervisor is software platform that allows multiple operating systems to run concurrently as virtual machines on a host computer.

incremental backupsonQ uses a backup scheme wherein a full backup is followed by a series of incremental backups, meaning backups that consist only of changes since the preceding backup. A Recovery Node can be quickly updated by simply merging the latest changes.

onQ Appliance...... onQ Appliance refers to the hardware on which onQ Manager runs.

onQ Central.......... onQ Central is Quorum's support management system. onQ Central manages alert notifications, licenses, and updates.

onQ Manager .... onQ Manager is the service that runs on an onQ Appliance coordinating all protection activities. onQ Manager sends alerts to onQ Central for processing.

onQ Service .... onQ Service is the secure, lightweight software agent running on an agent-based Protected Node. It communicates with the onQ Manager.

onQ Monitor.......... onQ Monitor is a tool designed to enable you to monitor multiple onQ Appliances from one user interface.

onQ Portal .... onQ Portal is the Web-based user interface used for all monitoring and management functions.

onQ virtual machine onQ virtual machine (also known as the *onQ instance)* is a separate operating system implemented in software. An onQ Appliance can host more than one onQ virtual machine. Each onQ instance provides an onQ Portal. An MSP (Managed Service Provider) configuration hosted by a single onQ Appliance can have several onQ instance

protection.............. Any node on your network for which onQ provides a virtual image that can be run is said to be protected by onQ.

Protected Node..... The physical or virtual machine to be protected by onQ. Abbreviated **PN**.

R2V .... client process launched at the onQ side to push data to the target (in the case of FLR the target is the running PN and, in the case of a BMR, the target is the BMR target machine).

Recovery Node ..... The up-to-date ready-to-run copy of the Protected Node. Abbreviated **RN**.

replication .... The process of reproducing a Recovery Node where the original image is on an HA and is replicated on the DR Appliance.

repository.............. The deduplicated archive of all snapshots of all of your

Protected Nodes. From the repository (aka *snapshot repository*), onQ can reproduce a complete system image from any snapshot.

squirtcopy ....onQ's backup utility/client. squirtcopy performs backups of the PNs to squirtserver. squirtcopy is packaged with linpy/winpy.

test mode...............Test mode means that a Recovery Node runs in a private network environment isolated from production facilities.

throttling................Bandwidth throttling is a technique for limiting the amount of transfer bandwidth available for data transfer on a network.

WVHDS ....a server process launched at the target (in the case of FLR the target is the running PN and, in the case of a BMR, the target is the BMR target machine) side waiting for data.