RPC3

Network Attached Storage

User Manual

RPC3 NAS
User Manual

Table of Contents

INTRODUCTION

The RPC3 Network Attached Storage (NAS) System is optimized for Size, Weight and Power (SWaP) in a 1U form factor. The RPC3 provides multiple protocols to present robust storage across Ethernet networks. An easy to use Graphic User Interface (GUI) is provided to allow for configuration and administration of its high performance data storage through commonly available Internet browsers.

This manual will provide an overview of the system and its configuration at an essential level. Tuning and configuring the system for specific environments and applications can be accomplished by working with Phoenix International's technical team, though a majority of requirements will be met by utilizing the information in this manual.

SAFETY PRECAUTIONS

Proper and safe operation of the unit requires proper transportation and storage, installation by qualified personnel, and operation within design limits.

- The user is solely responsible for proper and safe operation.
- The user is responsible for:
    - Maintaining the system in proper condition.
    - Continuously monitoring the operation of the system.
    - Initiating and executing required maintenance and repair work immediately.
    - Being aware of and follow any required safety measures.

WARNINGS

- Do not attempt to alter any part of the product.
- Do not allow the product to come into contact with water or any other. In the event that water or other liquids enter the interior of the system, immediately power down and unplug the product. Continued use of the product may result in fire or electrical shock.
- Do not handle the product with wet hands.
- Do not place the product near excessive heat sources or expose to direct flame.
- Ensure that the product is provided with a proper protective earth (PE) ground connection.
- Do not unmount, delete, or in any way modify "/dev/sda". This is the systems OS drive. Any changes to this system device can render the NAS inoperable.
- The boot drive of the NAS must be installed in the far left slot of the chassis. If not, the system will not recognize the boot drive and will not function properly.

DEFAULT SYSTEM CONFIGURATION

Default Network Configuration			
Description	**Physical Name**	**O/S Name**	**IP Address**
Management Port/GUI	Gigabit Ethernet #1	eno1	10.0.0.1
Network Data/Mgmt.	Gigabit Ethernet #2	eno2	10.0.1.1
Network Data	10Gb Ethernet #1	eno3	10.0.2.1
Network Data	10Gb Ethernet #2	eno4	10.0.3.1
IPMI Management	GbE IPMI	-	10.0.0.100

Default User Credentials		
Username	**Password**	**Where Used**
root	password	Operating system 'root' user
admin	password	GUI administration login
user	password	Network share default credentials
ADMIN	ADMIN	IPMI system management

The system is delivered with a pre-initialized RAID0 configuration that contains an EXT4 file system. This is to allow for rapid deployment of network storage after some basic configuration of protocols and network shares.

The default configuration of the two 10Gb Ethernet ports includes "Jumbo Frames" being enabled (MTU=9000).

NAS ADMINISTRATION

Administration of the RPC3 is done through a Graphical User Interface (GUI) that can be accessed with a standard Internet Browser (e.g. Firefox, Chrome, Explorer). Point the browser to the IP address of the GUI (default: 10.0.0.1), and log into the interface using the administration login credentials (default: admin, password).

Once logged in, there are two main sections to the GUI. On the left of the GUI window there is an array of Tools which can be selected to administer the NAS. On the right of the screen is the window that displays information and/or options for the items that are selected on the left. At the upper right of the Information window there is a button that, when selected, pulls down a menu that allows the user to shutdown, reboot, or logout of the RPC3.
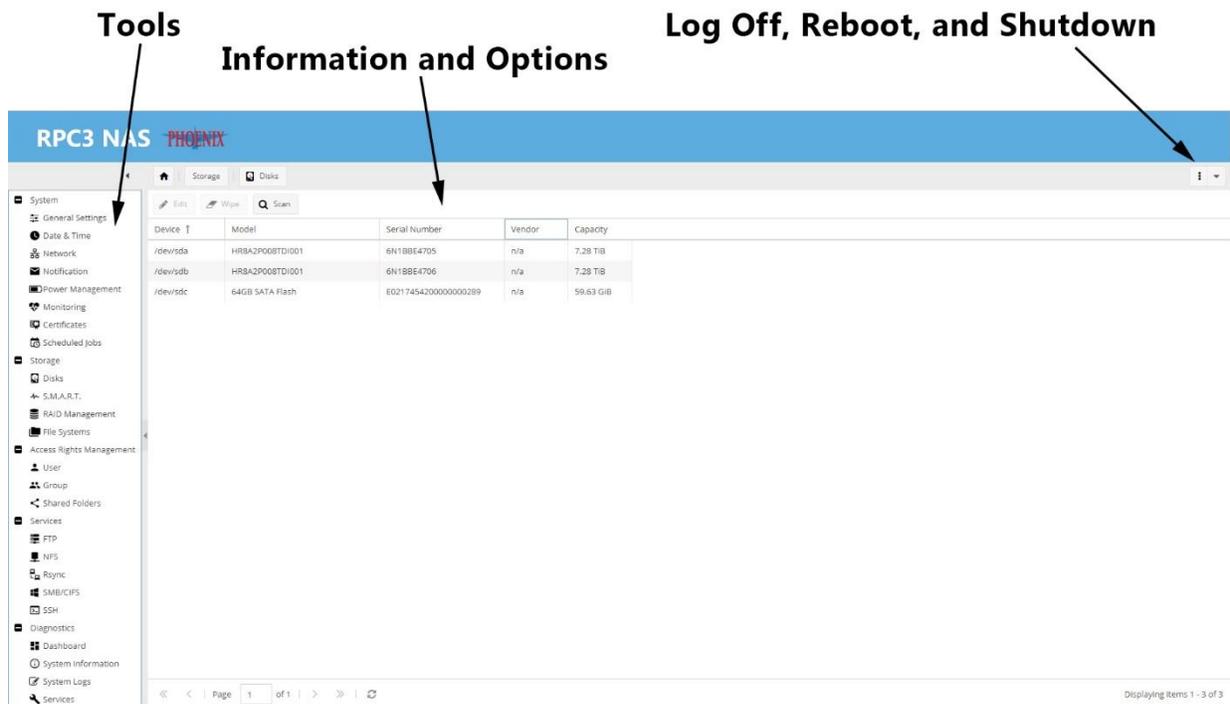
Quick Start - Connecting storage to the network:

The following steps, explained below, will allow the sharing of the data drives that are installed in the RPC3 via an Ethernet network. If a RAID set and Files System have been pre-built on the system from the factory, skip to step 4.

1. Create RAID set.
2. Create a File System (FS) on the RAID set.
3. Mount the File System.

4. Create a Share (shared folder) on the FS.
5. Assign user permissions to the Share.
6. Enable a file transfer Network Protocol.
7. Assign the Share to a Network Protocol (NFS/CIFS).

WARNING: Do not unmount, delete, or in any way modify "/dev/sda". This is the systems OS drive. Any changes to this system device can render the NAS inoperable.

Note: After each configuration change, apply the changes via the yellow banner at the top of the information window before making further modifications.

1. Create a RAID Set

A RAID set is a group of disk drives that are logically connected together to allow for greater capacity and/or redundancy than an individual disk drive. The RPC3 supports two levels of RAID:

- RAID0 - combines the capacity of two disk drives together to create one, larger, disk. Provides a fast storage pool, but is not redundant. If one disk fails, all data is lost.
- RAID1 – Mirrors two disks so that if one disk fails, all data is still persevered. Only has the capacity of one of the two disks. Enhanced read performance to multiple clients.

To create a RAID set with the two data drives installed in the RPC3, select the "RAID Management" tool under "Storage" on the left side of the GUI.

- Once in the RAID Management window, select the "Create" button. This will open a new window that will allow the user to assign a name to the RAID set, select the RAID level, and assign the storage devices to be used.
- Assign a name to the RAID set.
- Select the RAID level from the pull down menu. Select either Stripe (RAID0) or Mirror (RAID1). Other RAID levels are either not supported due to the number of drives installed in the RPC3, or are not recommended.
- Select the checkboxes next to the two drives (/dev/sdb and /dev/sdc) that are displayed to use the drives in the RAID set.
- Select "Create" and wait for RAID set to complete building before continuing on to creating a file system on the RAID set. When the RAID set is done building, a new storage device will be presented to the NAS called /dev/md0, this is the new RAID set that the File System will be built on in the next step.

- Apply the changes via the yellow banner at the top of the information window before making further modifications.

2. Create a File System on the RAID set

WARNING: Do not unmount, delete, or in any way modify "/dev/sda". This is the systems OS drive. Any changes to this system device can render the NAS inoperable.

To create a File System on the RAID set, select the "File Systems" tool under "Storage" on the left side of the GUI.

- Once in the File Systems window, select the "Create" button. This will open a new window that will allow the user to assign a label to the File System, select the File System type, and assign the RAID set (Device) the File System will be written to.
- Select the Device from the pull-down menu (/dev/md0).
- Assign a "Label" to the File System.
- Select the File System type from the pull-down menu. EXT4 is recommended for most applications.
- Select the "OK" button and wait for the file system to complete building. This can take a very long time depending on the RAID level and capacity of the storage devices.

3. Mount the File System

After the File System creation has completed successfully, select "/dev/md0" from the File System list and select the "Mount" button.

Apply the changes via the yellow banner at the top of the information window before making further modifications.

Caution: When mounting a file system, only press the "Mount" button once. It may take several minutes for the system to react to the mount request. Clicking on the Mount button more than once at this stage will cause OS errors.

4. Create a Share (shared folder) on the FS

The next step is to create a Shared Folder on the Files System/RAID set. To create a Shared Folder on the File System, select the "Shared Folders" tool under "Access Rights Management" on the left side of the GUI.

- Select the "Add" button in the upper left of the Information window. This will pull up a window that allow the user to configure the Shared Folder.
- Enter a name for the new Shared Folder in the "Name" field. This will automatically populate the "Path" field in the same window. This "Path"

name is the name of the folder on the RAID set that is being shared, and is the name used when connecting to the share when using SMB/CIFS.
- Select the device the new Shared Folder will be created on. This will be the name of the File System that was just created.
- Assign the desired permission levels from the "Permissions" pull-down menu. The default setting is sufficient in most applications.
- Select the "Save" button at the bottom of the "Add shared folder" window and apply the changes via the yellow banner at the top of the information window before making further modifications.

5. Assign user permissions to the Share

After adding the Shared Folder, select the folder just created and then select the "privileges" button above it.

- Select the "Read/Write" checkbox next to the default "user" accounts and then select the "Save" button. This will assign read/write access to the newly created share for the username "user" (default password = password).
- Apply the changes via the yellow banner at the top of the information window before making further modifications.

If other usernames are needed for access to the share, select the "User" tool under "Access Rights Management" on the left side of the GUI. This will allow you to create and/or modify User information. After creating a new user, permissions have to be assigned to a share before that user can access the share.

6. Enable a file transfer Network Protocol

Under the "Services" tool on the left side of the screen, select the Protocol that the Shared Folder will be shared across the network with (e.g. SMB/CIFS, NFS, or FTP). For SMB/CIFS or FTP, the default setting will be sufficient for most applications.

- Select the "Enable" slider button and then select "Save" to enable and start the service/protocol. Apply the changes via the yellow banner at the top of the information window before making further modifications.

7. Assign the Share to the Network Protocol

The final step is to assign a share to the protocol/service that was just started.

- In the information window of the protocol that was just started, select the "Shares" tab.
- In the "Shares" window, select the "Add" button.
- Select a Shared Folder to share from the "Shared folder" pull-down menu.

- For SMB/CIFS, the default setting are sufficient for most applications and the "Save" button can be selected at this point. Apply the changes via the yellow banner at the top of the information window before making further modifications.
- For NFS, assign an IP address or IP range to the protocol "Client" field to allow clients at those addresses to access the share.
    - If only one client is desired, input the IP address for that client.
    - If multiple clients are to be allowed access, assign the range to allow. (e.g. "10.0.2.0/24" will allow clients with an IP address from 10.0.2.1 to 10.0.2.254 to access the share).
- For NFS, select the desired privileges from the "Privilege" pull-down menu and then select the "Save" button. Apply the changes via the yellow banner at the top of the information window before making further modifications.

Client Access:

Users can access these share by pointing the client to the IP address and directory of the share.

For SMB/CIFS through a Windows client:

- In Windows explorer select "Map network drive…"
- Assign/select a drive letter from the pull-down menu.
- Enter the IP address and folder of the share in the "Folder" field (e.g. \\10.0.2.1*sharename* where *sharename* is the name of the shared folder created earlier).
- Select "Connect using different credentials" if the credentials assigned to the share are different than the credentials used to sign into the client that is trying to attach to the share.
- Select "Finish" and the share will be attached to the client, or, if different credentials was selected, enter the user credentials that were assigned to the share.

For NFS:

Consult the instruction for The Linux or other operating system for the specifics of connecting that specific OS to NFS shares (they vary depending on the OS).

IPMI System Management:

The IPMI (Intelligent Platform Management Interface) port on the RPC3 is to allow for remote management and monitoring of the RPC3. Whenever power is applied to the RPC3, regardless of the NAS portion of the RPC3 being turned on or not, the IPMI allows the user to remotely access the RPC3 and accomplish tasks such as:

- Power the RPC3 NAS on, off, or reset it.
- Monitor power and temperature of the system.
- Remotely access the system using a virtual KVM interface.

To log into the IPMI, point an Internet browser to 10.0.0.100 and log on with the following credentials:

Username: ADMIN

Password: ADMIN