CommandCenter® NOC Virtual Appliance

Quick Setup Guide

Copyright © 2007 Raritan, Inc.

Copyright and Trademark Information

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Raritan, Inc.

© Copyright 2007 Raritan, CommandCenter, and the Raritan company logo are trademarks or registered trademarks of Raritan, Inc. All rights reserved. VMware is a registered trademark of VMware, Inc. All other marks are the property of their respective owners.

For assistance the Raritan CommandCenter NOC Technical Support Team by telephone (732) 764-8886, by fax (732) 764-8887, or by e-mail

tech-ccnoc@raritan.com

Ask for Technical Support – Monday through Friday, 8:00am to 8:00pm, Eastern.

CC-NOC VMware Virtual Appliance – Quick Setup Guide

VMware Host Requirements:

CC-NOC VMware Virtual Appliance environment consists of the following components:

- VMware Player: Version 1.0.3 or higher or VMware ESX Server.
- CC-NOC VMware Image
- A networked host to run the CC-NOC VMware Image
- Managed network

To use VMware Player, you will need to download both the VMware Player software and the CC-NOC VMware image to the networked host, which can be either a Linux or Windows PC. This host computer should meet the following specifications:

- 1 GHz Processor
- 1GB available RAM.
- 80 GB of free hard drive space
- 1 network port
- Optional 2nd network port for Traffic Analysis and Intrusion Detection.

Customers with existing VMware ESX Server hosts can also use the CommandCenter NOC Virtual Appliance. See the **Using CC-NOC Virtual Appliance with VMware ESX Server** supplement for installation instructions with VMware ESX Server.

CC-NOC Virtual Appliance Network Connection

CC-NOC monitors your managed network over the network port (the host computer's primary Ethernet port). An available static IP address is required - which you will assign to the port as part of CC-NOC's configuration.

Optionally, for Traffic Analysis and Intrusion Detection, connect the host computer's secondary Ethernet port to a mirrored port on a switch or router to capture traffic.

Download VMware Player

VMware Player allows you to run CC-NOC in a virtual environment on your host computer. You can download a copy of the player (version 1.0.3 or higher) from the following site:

http://www.vmware.com/download/player/

1. Visit the site above and download a copy of the player to the host computer.
2. Install VMware player on the host computer.
3. Double-click on the VMware player icon to verify that it runs on the host computer.

Download the CC-NOC Virtual Appliance & License

To obtain a copy of the CC-NOC virtual appliance:

1. Visit the following site and fill in the request form:
   http://download.commandcenter-noc.com/
2. We will email you a CC-NOC license and the URL where you can download the CC-NOC Virtual Appliance and (this) Quick Setup Guide.
3. Save the zip file attached to the email to the host computer and then unzip it. This saves the license to the host computer.
4. If you received the CC-NOC virtual appliance on CD or DVD, you do not need to follow the link to obtain the Virtual Appliance. Instead, copy the CC-NOC Virtual Appliance image file (also a zip file) from the CD to the host computer and then unzip it.

   If you did not receive the virtual appliance on disc, follow the link in the email to download a copy to your host computer.

Configuring VMware Player for Traffic Analysis

For customers that want to use CC-NOC's traffic analysis and intrusion detection abilities, additional configuration of the VMware Player host is required. To configure VMware ESX Server for Traffic Analysis, refer to the **Using CC-NOC Virtual Appliance with VMware ESX Sever** supplement.

Note that the host machine will also need two network interfaces.

These steps should be completed before Installing and Running the CC-NOC Virtual Appliance image for the first time.

1. In the directory where VMware Player was installed, run the program called **vmnetcfg.exe**.
2. Select the **Automatic Bridging** tab.
3. Uncheck the **Automatic Bridging** option.
4. Select the **Host Virtual Network Mapping** tab.
5. Select a VM network (VMnet0, VMnet1, etc) that is listed as **Not bridged,** then use the drop-down menu to select a physical network adapter.

6. Select a second VM network that is listed as **Not bridged**, then use the drop-down menu to select a different physical network adapter from the first.
7. Note which VM networks were configured to use the physical network adapters than click **OK**.
8. In the directory where the CC-NOC Virtual Appliance image was unzipped, locate the Virtual Appliance's configuration file (ccnoc.vmx) and open it in a text editor.
9. Add the following lines to the ccnoc.vmx file:

```
ethernet0.vnet = "[VMnetN1]"
ethernet0.connectionType="custom"
ethernet1.vnet = "[VMnetn2]"
ethernet1.connectionType="custom"
```

   where [VMnetN1] and [VMnetN2] are the VM networks mapped to the host's primary and secondary network interfaces in steps 5 and 6. For example, they could be "VMnet2" and "VMnet0"
10. Save the changes to the ccnoc.vmx configuration file and close it.

Note: These steps may cause problems for other images loaded on to VMware Player.

Installing and Running the CC-NOC Virtual Appliance

The directions below assume you are using the free VMware Player to run the CC-NOC Virtual Appliance. If you intend to load the Virtual Appliance on VMware ESX Server, please refer to the **Using CC-NOC Virtual Appliance with VMware ESX Server** supplement.

Installation

1. Open the ccnoc folder and locate the VMware configuration file (ccnoc.vmx). Double click on the configuration file to start up CC-NOC. Alternatively, you can launch VMware Player first and use its built-in browser to locate and start up the CC-NOC configuration file.
2. The first time you launch CC-NOC, the player will ask if you want to create a new UUID. Answer **YES**.
3. CC-NOC will start its boot process – first the BIOS then Linux. Ignore any "**failed**" warning messages; these are normal. Wait until you see the login prompt.
4. At the login prompt, type **config**. No password is necessary. The network configuration program starts up automatically.
5. Highlight (use up/down arrow keys) the **Setup IP Addresses** menu option and press Enter to select it.
6. Enter the (static) IP address and your network's network mask, gateway and DNS addresses.
7. Select **OK** – the screen displays the progress as CC-NOC's network settings are reconfigured. The display returns you to the main menu.

8. (Optional and recommended) select **Test Network Connectivity**. Run the **Ping Diagnostic** to insure CC-NOC can communicate over the network.
9. When you are confident that CC-NOC's network is up and running exit the network configuration program. This completes all configuration steps performed from the VMware player console.

Note: From this point on, accessing the CC-NOC occurs from any client PC on the network, not the console in the VMware player, (though the VMware player must still be running the image).

Configuration from CC-NOC Web Interface

You can configure CC-NOC using a web browser on any machine on the network – but Raritan recommends you run a browser on the host computer - as your first task will require you to upload the license we sent you.

1. Open a web browser on the host computer.
2. In the browser's address bar, enter the IP address you assigned to CC-NOC. For example: `http://192.168.1.10`
3. Answer **YES** to any security alerts and accept all certificates.
4. When greeted by the login page use the login: **admin** and the password: **raritan**.
5. You will be prompted for a license. Click **Browse** and select the license file that you unzipped earlier.
6. Click **Load This License**.
7. The First Time Configuration Wizard displays. Follow the wizard's instructions and provide the necessary data.

A few items to note:

- **Discovery Range** – Devices found (discovered) with IP addresses in the discovery range are managed by CC-NOC. The larger the range, the longer it takes CC-NOC to complete discovery.
- **Default SNMP community strings -** The default SNMP community string is 'public". If yours is different you can change it for each range of IP addresses.
- **Secondary DNS & WINS Server Addresses -** Optionally, specify any Secondary DNS and WINS Server Addresses. WINS Server are used in windows networking to resolve NetBiosName across subnet boundaries.
- **SMTP Server & Email Communication Settings** - Optionally, specify an external SMTP Server or accept the built-in SMTP server. Specify an admin email address to which CC-NOC status information will be sent. **Email As** should be either a valid email address or left blank so that NOC uses a default address.

Windows Configuration

If you have windows systems in your discovery range, you need to configure a Windows Proxy in order to gather WMI (Windows Management Instrumentation) information for those devices. WMI provides a wide ranged of detailed information, from the system name of the device to a list of services present.

Users who do not have Windows devices in the discovery range can skip this section.

Configuring Windows Proxy System

1. Select a Proxy System with the following configuration.

   ```
   1GHz CPU or higher
   512MB available RAM or higher
   Windows XP Professional with SP2
   ```

   If your VMware Player is running on a powerful Windows system, it can be configured as the Proxy.

2. Download ProxyInstaller from
   `http://<address_of_noc>/public/ProxyInstaller.zip`
3. Unzip the `ProxyInstaller` archive on your Windows machine and move the directory to a location where you would like to keep the program.
4. Double-click on `ProxyInstaller.exe` to run the program.
5. Specify the machine administrator password
6. select **Stand-alone** Network Management setup
7. Type in the CC-NOC IP address
8. Click **Install** to configure your proxy Windows machine with the latest proxy settings

Configuring CC-NOC-Proxy Communication

1. Login to CC-NOC via web Interface
2. Click on the **Admin** tab in the top navigation bar.
3. Click **Windows Management Configuration**.
4. Click **Windows Management Configuration Wizard**.
5. Click **Configure** to launch the wizard.
6. Select **Add New External Proxy** to add the proxy system
7. Type IP Address for the Proxy
8. Type values for **domain**, **username**, **password**, and confirm the password. Note that the username must be a local user on that system, which is a member of the Local Administrators group.

Specifying Windows Ranges

Specify IP Addresses of windows systems that are managed using Microsoft's Windows Management Instrumentation (WMI).

Adding Authentication Credentials

Domain-based authentication is the most commonly used form of authentication in Windows environments. Select appropriate authentication mechanism. If Domain based authentication selected, add domain name, username, and password. Note Domain name has no suffix (for example: the domain “raritan.com” will be specified as “raritan”).

Optional Configuration Tasks

Intrusion Detection Configuration

CC-NOC can act as a network-based intrusion detection system (NIDS), listening to network traffic and indicating when certain behaviors are identified, traffic patterns appear, or recognized character strings are passed. Configuring CC-NOC for intrusion detection occurs in two main steps:

Setting the Home Network

Setting the Home Network identifies devices on your network as trusted. Traffic generated from these systems will be evaluated appropriately.

1. Click on the **Admin** tab.
2. Click **Intrusion Detection Configuration**.
3. Click **Configure Appliance Home Network**.
4. Click **Select** for the CC-NOC appliance listed in the table.
5. Follow the on screen instructions to specify trusted networks by subnet or by address range.

Configuring the Intrusion Detection Signature Profiler

The IDS profiler designates what types of network traffic to watch for and how it applies to various devices on your network. To configure:

1. Click on the **Admin** tab.
2. Click **Intrusion Detection Configuration**.
3. Click **Intrusion Detection Signature Profiler**.
4. Check the **Select** box for the CC-NOC appliance listed in the table and click **Next**.
5. The Profiler will step you through configuration pages covering traffic signatures, the types of devices on the network and the applications they run. Check the items that apply, or simply accept the default.

Adjusting the Memory Available to Your Virtual Appliance

To increase (or decrease) the amount of memory allocated to the CC-NOC virtual appliance:

1. Launch VMware player and the CC-NOC virtual appliance.
2. Select the **Player** menu from the menu bar of VMware Player.
3. Under **Troubleshoot**, select **Change Memory Allocation**.
4. Move the slider to adjust the amount of memory the CC-NOC virtual appliance will use, then click **OK**.

Note that you will have to reboot your CC-NOC virtual appliance for the changes to take affect.

CC-NOC User Guide

For more details, please refer to CC-NOC User Guide at
http://www.raritan.com/support/productdocumentation

Things To Do With Your CC-NOC Virtual Appliance

Connect to the CC-NOC web interface by entering the IP address of your Virtual Appliance in a web browser and logging in. From there, you can explore the CC-NOC interface. Task are grouped into tabs by subject at the top and clicking a tab will bring up relevant items below.

Also, in general you will find:

- Most pages have help text on the screen explaining the various options or items that are available.
- Many status page items are links that lead to more detail on that item.

Some things you may want to try are:

- Listing the discovered devices.
- Viewing details about a particular (windows) device.
- View traffic analysis.

Note: Because of resources required from your network and the VMware host, Raritan does not recommend running a Vulnerability Scan using the Virtual Appliance.

Listing Discovered Devices

A search bar is available at the far left of the interface. Clicking **Search** lists all devices the virtual appliance has discovered, along with some basic information. Entering parameters in the bar will list devices that contain those parameters in their name.

View (Windows) Device Details

Click the name of a device on the list. If available, click a Windows device with a **Server** license. A Node Info screen appears with more details about that device, including what services are available, what recent events have occurred to it, and possibly more.

If available, click on **More Windows Management Information** link. More details about the device are revealed. Click **More Service Information**. A list of Windows Services running on this device will appear along with parameters for starting, stopping and resetting these services.

View Traffic Analysis

1. Click the **Reports** tab at the top.
2. Click **Network Report Card**. The Network Report Card appears with summaries for the availability of managed devices, security events that have occurred and the type of traffic that has been monitored.

World Headquarters

Raritan, Inc.
400 Cottontail Lane
Somerset, NJ 08873
USA
Tel. (732) 764-8886
Fax (732) 764-8887
Email: sales@raritan.com
www.raritan.com

Raritan OEM Division

Peppercon USA, Inc.
111 E. Wacker Dr, Suite 2626
Chicago, IL 60601
Tel. (847) 466-1392
Fax (312) 729-1375
Email: info@peppercon.com
www.peppercon.com

Asia Pacific Headquarters

Raritan Taiwan, Inc.
5F, 121, Lane 235, Pao-Chiao Road
Hsin Tien Taipei
Taiwan, ROC
Tel. (886) 2 8919-1333
Fax (886) 2 8919-1338
Email: sales.asia@raritan.com
http://www.rcit.com.tw

Raritan China Offices

Shanghai Representative Office of Raritan, Inc.
Rm 17E Cross Region Plaza
899 Lingling Rd., Shanghai
China 200030
Tel. (86) 21 5425-2499
Fax (86) 21 5425-3992
Email: sales.china@raritan.com
http://www.raritan.china.cn

Guangzhou Representative Office of Raritan, Inc.
1205/F, Metro Plaza
183 Tian He Bei Road
Guangzhou
China 510075
Tel. (86-20)8755 5581
Fax (86-20)8755 5571
Email: sales.china@raritan.com
http://www.raritan.com.cn

Beijing Representative Office of Raritan, Inc.
Unit 1310, Air China Plaza
No.36 XiaoYun Road, Chaoyang District
Beijing
China 100027
Tel. (86) 10 8447-5706
Fax (86) 10 8447-5700
Email: sales.china@raritan.com
http://www.raritan.com.cn

Raritan Korea

Raritan Korea Inc.
#3602, Trade Tower, World Trade Center
Samsung-dong, Kangnam-gu
Seoul, Korea
Tel. (82) 2 557-8730
Fax (82) 2 557-8733
Email: sales.korea@raritan.com
http://www.raritan.co.kr

Raritan Japan, Inc.

4th Floor, Shinkawa NS Building
1-26-2 Shinkawa, Chuo-ku
Tokyo, Japan 104-0033
Tel. (81) 03-3523-5991
Fax (81) 03-3523-5992
Email: sales@raritan.co.jp
http://www.raritan.co.jp

Raritan Japan Osaka Office
Honmachi Phoenix Bldg 8F
1-15-8 Nishihonmachi Nishi-ku
Osaka, Japan 550-0005
Tel. (81) (6) 4391-7752
Fax (81) (6) 4391-7761
Email: sales@raritan.co.jp
http://www.raritan.co.jp

Raritan Australia

Level 2, 448 St Kilda Road
Melbourne, VIC3004
Australia
Tel. (61) 3 9866-6887
Fax (61) 3 9866-7706
Email: sales.au@raritan.com
http://www.raritan.com

Raritan Taiwan Inc India Liaison Office

210 2nd Floor Orchid Square
Sushant Lok 1, Block B, Mehrauli
Gurgaon Rd, Gurgaon 122 002
Haryana
India
Tel. (91) 124 510 7881
Fax (91) 124 510 7880
Email: sales.india@raritan.com
http://www.raritan.com

European Headquarters

Raritan Europe, B.V.
Eglantierbaan 16
2908 LV Capelle aan den IJssel
The Netherlands
Tel. (31) 10-284-4040
Fax (31) 10-284-4049
Email: sales.europe@raritan.com
http://www.raritan.com

Raritan France

120 Rue Jean Jaurés
92300 Levallois-Perret
France
Tel. (33) 14-756-2039
Fax (33) 14-756-2061
Email: sales.france@raritan.com
http://www.raritan.fr

Raritan Deutschland GmbH

Lichtstraße 2
D-45127 Essen
Germany
Tel. (49) 201-747-98-0
Fax (49) 201-747-98-50
Email: sales.germany@raritan.com
http://www.raritan.de

Raritan Italia

Via dei Piatti 4
20123 Milan
Italy
Tel. (39) 02-454-76813
Fax (39) 02-861-749
Email: sales.italy@raritan.com
http://www.raritan.com

Raritan Canada

Raritan Inc.
2085 Hurontario St., Suite 300
Mississauga, Ontario
Canada
L5A4G1
Tel. (905) 949-3650
Fax (905) 949-3651
Email: sales.canada@raritan.com
http://www.raritan.com

Raritan U.K. Limited

36 Great St. Helen's
London EC3A 6AP
United Kingdom
Tel. (44) 20-7614-7700
Fax (44) 20-7614-7701
Email: sales.uk@raritan.com
http://www.raritan.com