VI-CENTER™
ADMINISTRATOR GUIDE

Version: V4.5

Notice

Virtual Iron® Software, Inc.
900 Chelmsford Street
Tower I, Floor 2
Lowell, MA 01851
http://www.virtualiron.com

Trademarks

00010609R2

CONTENTS

Contents

PREFACE

Virtual Iron® VI-Center™ consists of a management server and a graphical client. The *VI-Center Administrator Guide* describes how to install and configure Virtual Iron® in an enterprise data center.

This guide also describes the functional relationships between Virtual Iron® software components. Procedures define how to use the VI-Center client to manage virtual servers and perform administrative tasks.

AUDIENCE

This guide is for experienced IT administrators with knowledge of the following:

- Server cabling and configuration
- LINUX® or Windows® administration
- Network configuration
- SAN set-up and management, including Fibre Channel administration

CONVENTIONS

This book uses the following conventions:

- **Bold** type highlights the names of fields, buttons, and navigation controls in the Virtual Iron® management client.
- Blue text indicates hyper-text links.
- Mono-spaced blue type is used for commands, filenames, and directories.
- *Italicized text* is used to define or emphasize key terms.

LICENSE INFORMATION

The following Third Party Software modules are incorporated in or shipped with the Virtual Iron® software and are subject to the following terms and conditions:

Linux®

Linux® is a registered trademark of Linus Torvalds.

Redistributing GPL Source Files

You can redistribute and/or modify General Public License (GPL) software under the terms of the GPL. You may obtain a copy of the source code corresponding to the binaries for the GPL Software (the “GPL Source Files”) by downloading the GPL Source Files from:

http://www.virtualiron.com/Support/Downloads/Open-Virtual-Iron/index.php

This offer to obtain a copy of the GPL Source Files is valid for three years from the date you acquired this software product.

TECHNICAL SUPPORT AND SELF SERVICE LINKS

Use the following link to access information, tools, and forums:

- Virtual Iron company and product information
- Virtual Iron Community
- Documentation
- Knowledge Base
- Forums
- User Groups

http://www.virtualiron.com/Support/

1

VIRTUAL IRON® OVERVIEW

Virtual Iron® ™ Extended Enterprise Edition (XEE) provides server virtualization software that enables companies of all sizes to reduce the cost and complexity of operating and managing their IT infrastructure. This chapter provides an overview of the Virtual Iron product.

This chapter contains the following sections:

ABOUT VIRTUAL IRON® XEE

Virtual Iron® is a virtualization product that enables IT administrators to increase the efficiency and flexibility of physical server resources. Virtual Iron® XEE runs across a set of physical servers, or *managed nodes*. IT administrators partition node resources so that each node supports n-*virtual servers*. The goal is to use each physical node at maximum efficiency, in a framework that uses processing power where and when it is needed.Virtual Iron software:

- Increases server utilization rates
- Cuts management complexity and costs
- Adapts to changing business needs
- Allows modification and reallocation of server resources
- Does not require intervention if there is a failure.

Virtual Iron's® Native Virtualization™ streamlines virtual infrastructure management and reduces operating costs by:

- Leveraging hardware-assisted virtualization capabilities from Intel and AMD for optimal efficiency
- Allowing 32- and 64-bit x86 operating systems to run unmodified and concurrently on a partitioned server
- Requiring no installation or management of the virtualization layer
- Virtualizing all data center resources, including servers, networks, and storage.

VI-Center

VI-Center provides an enterprise-class, transactional virtualization framework which consists of the following elements:

- A management server and integrated database
- A graphical client user interface that supports multiple concurrent users.

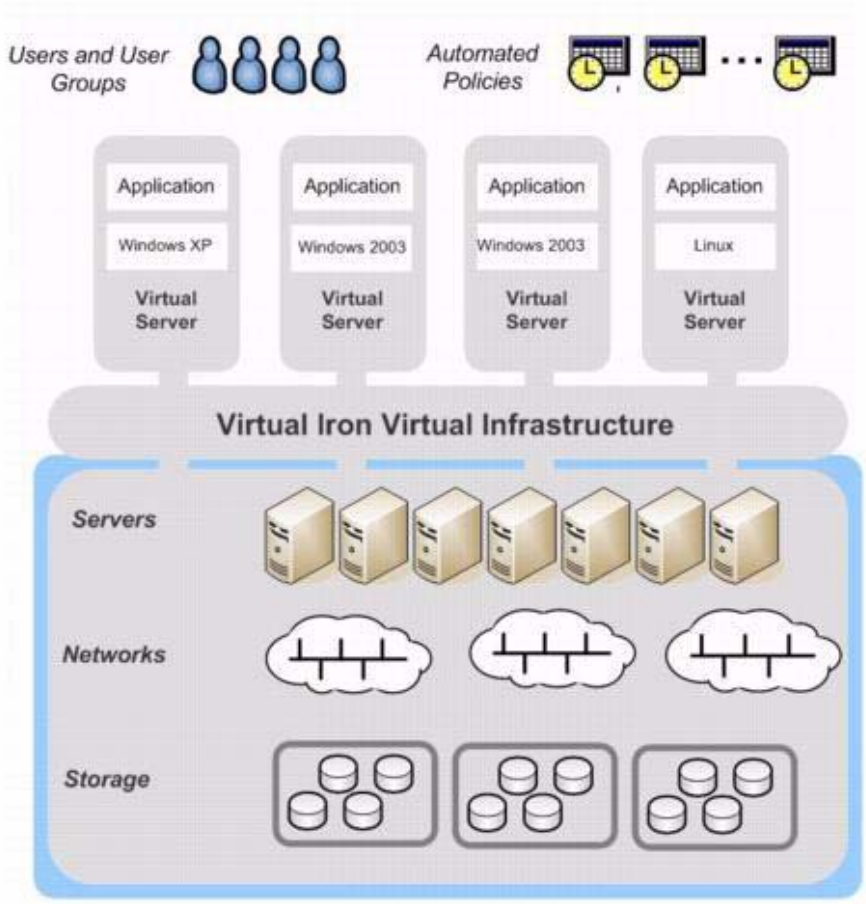
Within this framework, one or more clients connect to the Virtual Iron® VI-Center to manage the resources of a set of managed nodes.

DELIVERING VIRTUAL INFRASTRUCTURE

At the highest level, Virtual Iron® transforms a set of interconnected nodes (physical machines) into a virtual infrastructure. In this flexible framework, a set of physical servers supports a number of operating systems (OS) and application workloads, which can be configured, deployed, and adapted to business changes on demand.

Figure 1 provides a high-level view of a virtual infrastructure built with the Virtual Iron® solution.

Figure 1. Virtual Iron® Dynamic Infrastructure



Automated policies control the resources used by virtual servers, based on performance and other criteria. As application demands change, virtual servers are moved from one physical server to another. Configuration of access to networks and SANs, and of redundant paths to guard against failure, are greatly simplified. Virtual Iron® leverages the virtualization extensions built into the latest Intel® and AMD® processors so applications run in this framework with no special configuration or driver support.

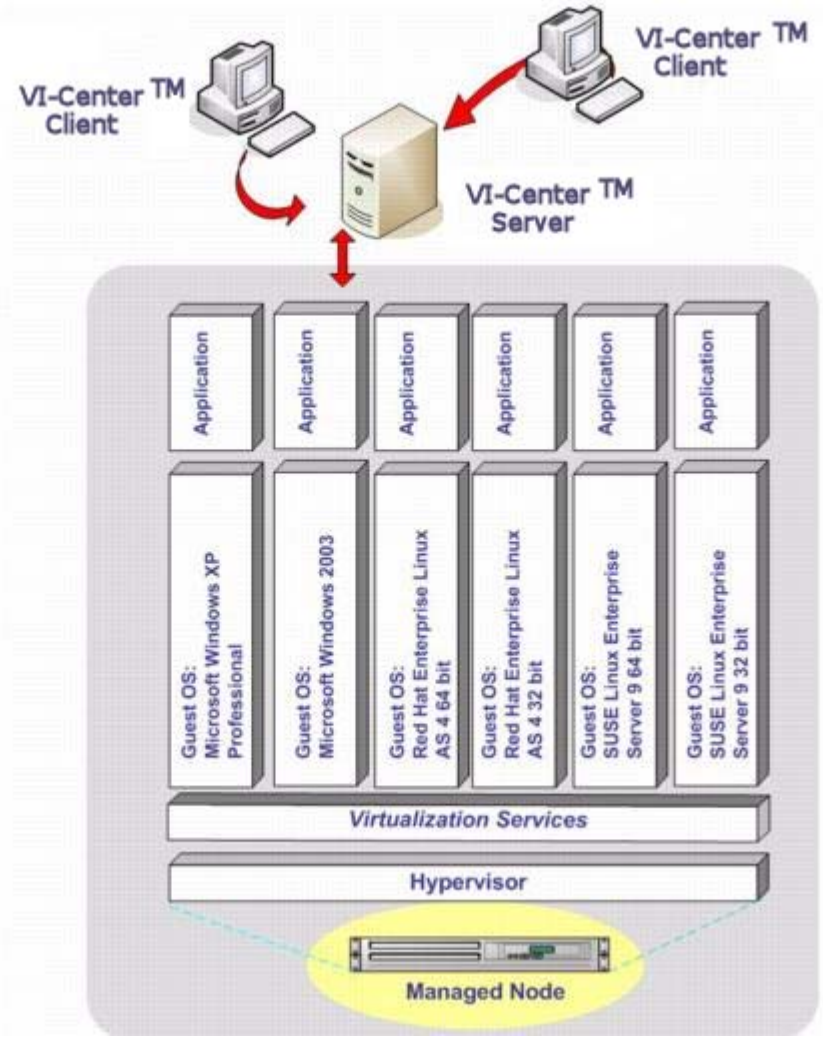
VIRTUAL IRON® ARCHITECTURE

Virtual Iron® comprises three components.

- Hypervisor—An abstraction layer that mediates between the physical hardware and the Virtualization Services component.
- Virtual Iron® Virtualization Services—A software component that performs many functions ordinarily provided by standard operating systems.
- The Virtual Iron® VI-Center—A high-performance client/server management framework.

Figure 2 shows a conceptual view of six virtual servers running on a single physical node.

Figure 2. Virtual Iron® Architecture

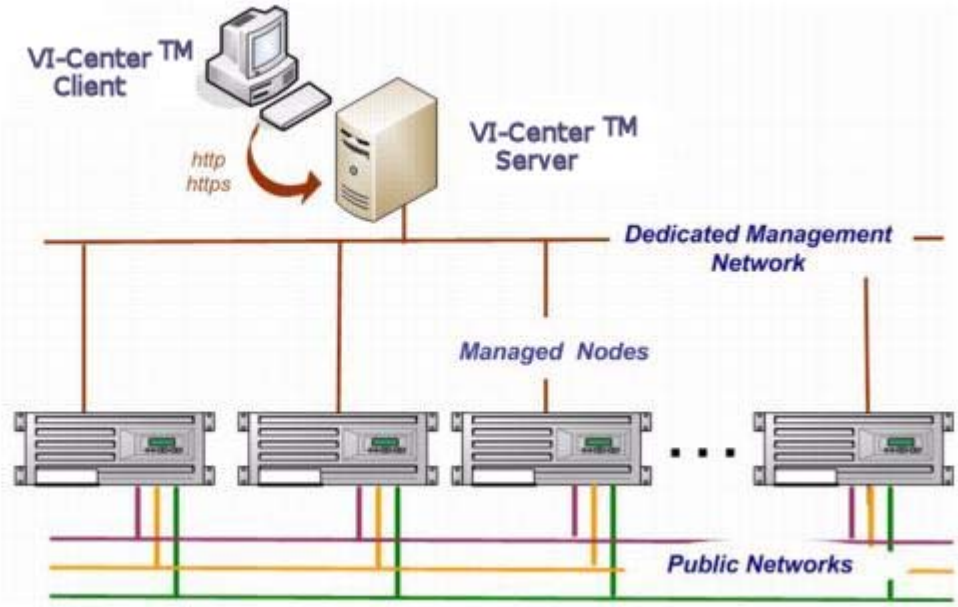


PRODUCT REQUIREMENTS

With Virtual Iron® XEE, you may virtualize the resources of one or more nodes. The number of nodes you can manage is processor-dependent and varies with the license you have purchased. See Determining What Your License Supports for information on product licensing.

As Figure 3 shows, the Virtual Iron® framework requires a single management server linked to one or more physical servers, or *nodes*, on an Ethernet network. Virtual Iron's management server, *VI-Center*™, communicates with each node over a dedicated management network. Nodes managed in this framework may also access SAN and network resources via one or more public networks.

Figure 3. Conceptual View of the Virtual Iron® Framework



OBJECT RELATIONSHIPS IN VI-CENTER

Virtual Iron® XEE manages a set of nodes, enabling the creation of virtual data centers (VDCs) and virtual servers. The sections that follow describe the relationships between managed nodes, VDCs, and virtual servers.

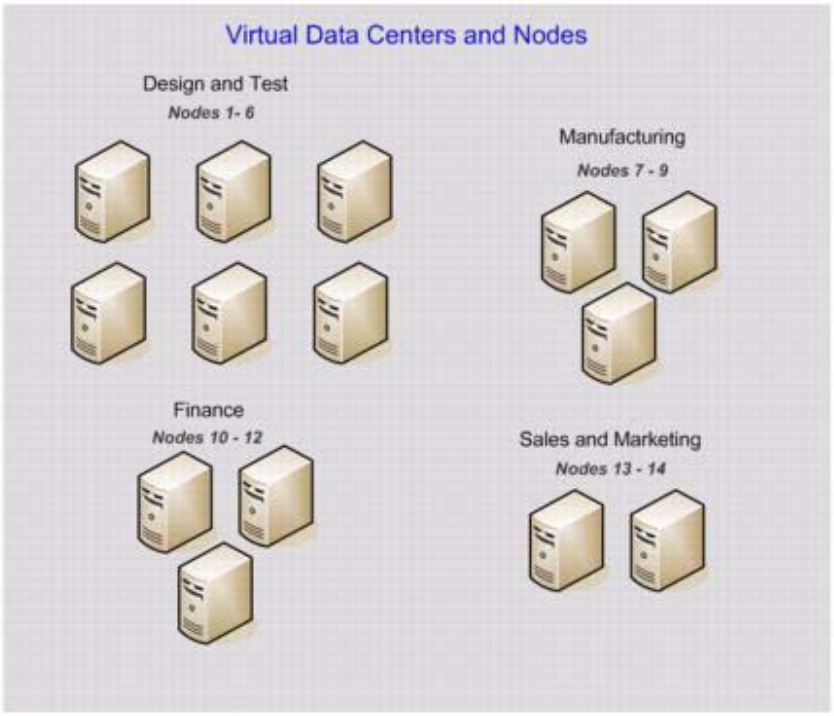
Managed Nodes and Virtual Data Centers

A *Virtual Data Center* (VDC) is an administrative container that refers to a group of managed nodes, their virtual servers, and applications. Each VDC houses a group of managed nodes used by a specific area of operations within an enterprise. Each VDC may need connections to specific networks

and SANs within the enterprise.

To illustrate what a VDC is and how to create and assign nodes to them, let's say your company has several departments: Design and Test, Manufacturing, Finance, and Sales. Each of these departments has different responsibilities and each will likely run a set of applications specific to its aims. The Design and Test organization may run CAD and other programs that are not used elsewhere in the organization. Manufacturing may run programs that link its production goals with existing inventories of materials. Finance runs small- and large-scale accounting applications. Therefore, your enterprise may, for example, divide a set of 14 nodes among four administrative groups, as shown in Figure 4.

Figure 4. Nodes And Virtual Data Centers



Virtual Data Centers and Virtual Servers

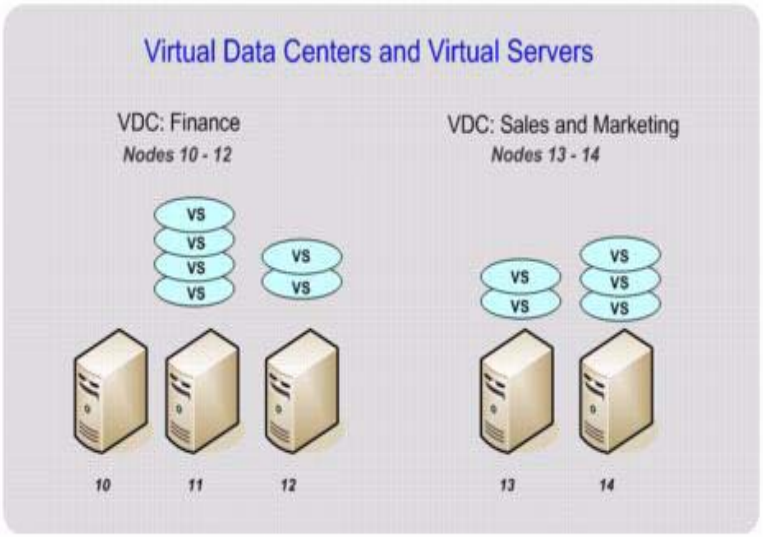
A virtual server is a virtual machine that runs an OS and its associated applications. Just as each VDC owns the resources of a set of nodes, each node in a VDC can host a set of virtual servers.

With Virtual Iron®, each node is partitioned into a set of functionally independent environments, or virtual servers. A number of virtual servers can run simultaneously on a single node. Just as each VDC may contain *n*-nodes, each node may host multiple virtual servers.

To understand the relationship between VDCs, the nodes they contain, and the virtual servers that run on these nodes, refer to Figure 5. This illustration shows two VDCs, Finance and Sales and Marketing. Finance contains three

managed nodes—10, 11, and 12. Of these, node 10 contains no virtual servers, while nodes 11 and 12 host four and two virtual servers respectively. Sales and Marketing contains nodes 13 and 14, which host two and three virtual servers.

Figure 5. VDCs, Nodes and VSs



VIRTUAL SERVER CHARACTERISTICS

A virtual server is an instance of an operating system and its applications. With Virtual Iron®, you can configure and run multiple virtual servers on each managed node. VI-Center™ provides control of virtual server characteristics, such as:

- Number of processors (default: 1)
- Processing priority (default 50)
- Memory (default: 256 MB)
- Network connections
- Disks (optional)
- Boot method

These characteristics are defined briefly below. For instructions on configuring them, see the integrated product tutorial.

Processors

Each virtual server uses some or all of the processors on the node hosting it. Virtual Iron® allows multiple virtual servers to share the same processors. If a node has four physical processors, the virtual servers configured on that node can each use part or all of them. You can assign the default minimum of one processor or assign a higher number. Virtual Iron® limits each virtual server to the number of processors available on its host node.

Processing Priority

When more than one virtual server is using the same processing resources, virtual servers assigned a higher priority are favored over another. For example, virtual servers A and B have the default priority of 50; C is assigned 100, the highest priority, Virtual Iron® allows C to run more frequently than A and B. See Creating a Virtual Server for details and procedure.

Memory

By default, each virtual server is allocated approximately one quarter Gigabyte (256 MB) of memory. You can increase or decrease the memory allocated to each virtual server to suit application requirements.

Unlike processors, memory is not shared among virtual servers, but is allocated to virtual servers at configuration time. Memory allocated to one virtual server cannot be used or borrowed by another, even if it is unused. Instead, memory is apportioned among virtual servers administratively, with each allocated a specific amount of the total available. The total of allocated memory cannot exceed 100% of the available physical memory. See Creating a Virtual Server for details and procedure.

Network Connections

Each virtual server uses a software object called a *virtual network interface card,* or **VNIC,** to connect to a specific subnet. Each VNIC has a unique MACaddress. You can assign multiple VNICs to each virtual server, enabling its applications to access multiple networks. Once a VNIC is assigned to a virtual server, it is bound to that virtual server, and cannot be used by any other. The total number of VNICs you can assign to all virtual servers is unlimited.

Disks

As the VI-Center administrator, you can assign disks to each virtual server. These disks can be raw SAN (Fibre Channel or iSCSI) volumes, or logical hard disks created on SAN or local drives. You can configure each virtual server to boot from, and access any disks visible to, the managed node hosting it. Virtual servers hosted by a node containing a *host bus adapter* (HBA) or access to an iSCSI network, can connect to SAN resources.

The Virtual Iron® administrator controls which *logical unit number* (LUN) to use as a boot disk, and the order in which LUNs are presented to the OS. You must provide the world wide node numbers (WWNN) associated with each HBA to the SAN administrator, so that switches may be programmed to provide the desired access. See Configuring Storage.

Boot Methods

Virtual servers can boot from logical disks on a SAN, from a local disk, or from a network boot device or from a CDROM. See the steps in Creating a Virtual Server for information on configuring boot parameters.

2

INSTALLING VIRTUAL IRON XEE

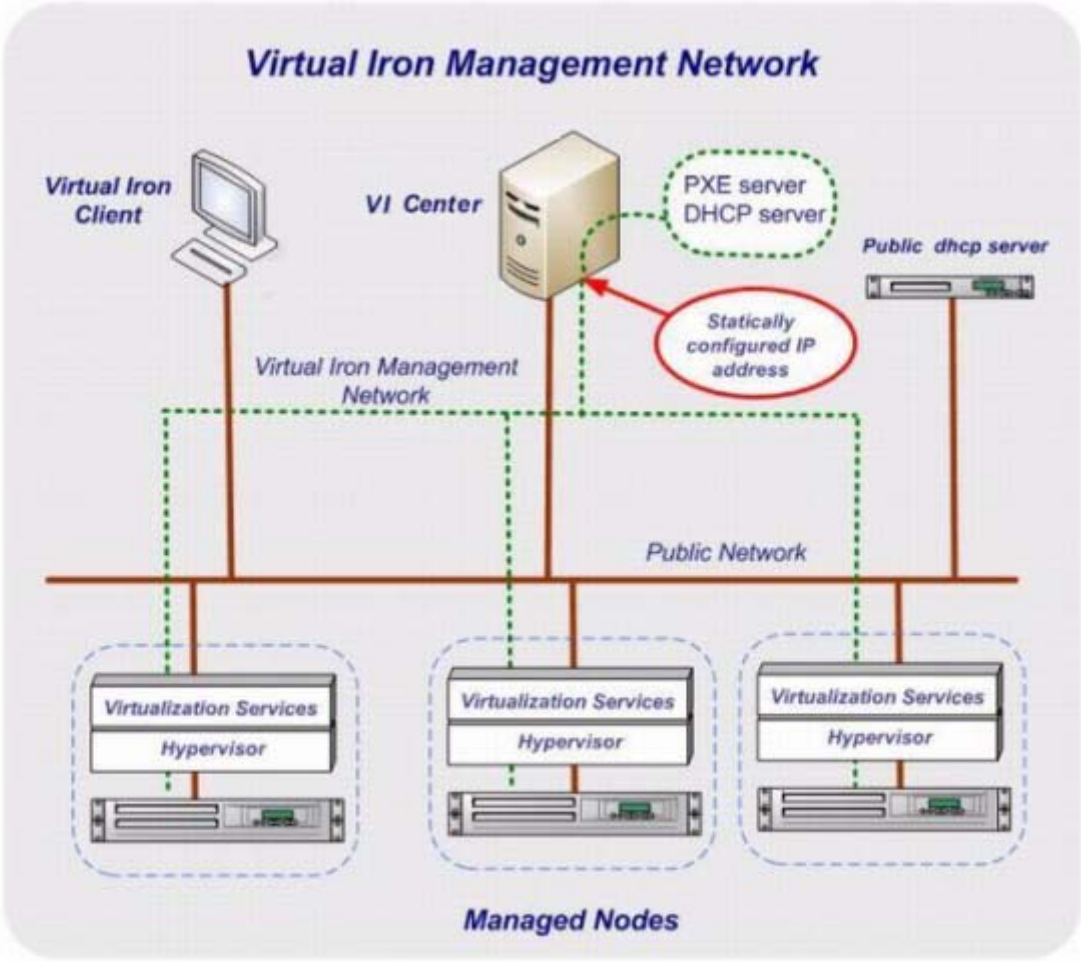
INSTALLATION OVERVIEW

Virtual Iron® Extended Enterprise Edition runs on one or more Intel or AMD-based servers called *managed node*s. These servers are managed by *VI-Center,* a web-based management application installed on a separate node running either Windows® or Linux®.

When running Virtual Iron® XEE, VI-Center and all managed nodes are interconnected by a dedicated management network, as shown in Figure 6. Note that the nodes in this illustration are connected to a public network, which hosts a DHCP server. With Virtual Iron® XEE, managed nodes can be connected with any number of public networks. However, these nodes can only be managed via a single dedicated management network.

From a management perspective, the product treats these nodes as a single pool of resources. Virtual servers created in this environment can migrate from one node to another in the event of a failure, and move non-disruptively to another node as needed.

Figure 6. Virtual Iron® Management Framework



HARDWARE AND SOFTWARE REQUIREMENTS

Virtual Iron® can run on a single node, or can comprise a management node (which runs VI-Center) interconnected with one or more managed nodes.

Note: The VI-Center can be installed onto a Linux or Windows platform. However, once installed, it can not be moved from one platform to another. Instead, uninstall it and reinstall it. The VI-Center can be upgraded per Virtual Iron's upgrade instructions.

Managed Servers, Minimum Requirements

Managed nodes have the following minimum requirements.

- Intel®-VT or AMD-V® based nodes
- 2 GB RAM
- Local SATA and SCSI drives (optional). IDE disk drives are not supported.
- Ethernet ports: 2; if using iSCSI, 3
- Fibre channel card (optional)

Management Server, Minimum Requirements

The management node hosts the Virtual Iron® VI-Center.

- 1 CPU (Intel Xeon or its equivalent or higher)
- 2 GB RAM
- 30 GB hard drive (7,200 RPM or higher, 10,000 RPM recommended)
- Ethernet ports: 2
- OSs supported:
  - Red Hat Enterprise Linux 5 32-bit and 64-bit (note: 64-bit RHEL-4 requires the compact-arch-support package)
  - SUSE Linux Enterprise Server 10, 32-bit and 64-bit
  - Windows Server 2003 or 2008 32-bit
  - Cent OS 5

Virtual Iron Maximum Limits

Component	Virtual Iron
CPUs per virtual server	8 maximum. Varies, depending on OS distribution.
Virtual RAM per virtual server	32 GB
Physical RAM per virtual server	64 GB
NICs per physical server	3 (5 ports)
VNICs per virtual server	5 (5 ports)
Disk size (iSCSI or Fibre Channel LUN, logical disk)	3 TB
Physical LUNs per node	500
Number of disks per virtual server	15
Number of virtual servers per physical server	Varies, depending on memory and CPU requirements.

VI-Center Client Requirements

The VI-Center client manages physical and virtual objects. The client requires the 32-bit version of JRE 1.6 or newer.

If you are installing the VI-Center on 64-bit RHEL-4 the compat-arch-support package is a prerequisite.

Note: If you are installing VI-Center on Linux, you must have **glib** installed on the management server to make use of the Network (Image) Boot feature. If your management server is running X Windows or Gnome you have glib installed. If **glib** is not installed, the following error message appears in the log:

/opt/VirtualIron/VirtualizationManager/system/log/nbd-server.log contains bin/nbd-server: error while loading shared libraries: libglib-2.0.so.0: cannot open shared object file: No such file or directory

GOSs Supported On Virtual Servers

Virtual Iron® Extended Enterprise Edition enables administrators to configure and manage multiple guest operating systems (GOSs), of different types and versions, on a single managed node.

Virtual Iron® supports virtual servers running the following OSs and versions.

- RHEL 3 U8 and U9 32-bit
- RHEL 4 U4, U5, and U6 AS 32-bit and 64-bit
- RHEL 5 U0 and U1 32-bit and 64-bit
- SUSE Linux Enterprise Server 9 SP3 and SP4 32-bit and 64-bit
- SUSE Linux Enterprise Server 10 SP1 and SP2 32-bit and 64-bit
- CentOS 4 U4, U5, and U6 32-bit and 64-bit
- CentOS 5 U0, U1 and U2 32-bit and 64-bit
- Windows 2000 SP4 32-bit
- Windows XP SP2 and SP3 32-bit
- Windows Server 2003 Standard and Enterprise Editions SP2 32-bit and 64-bit
- Windows Server 2008 Standard and Enterprise Editions SP1 32-bit and 64-bit
- Windows Vista SP1 32-bit and 64-bit

Languages Supported

In addition to English, in this release, Virtual Iron supports installations on Japanese and German operating systems. Expanded and localized support will be available in future releases.

MANAGEMENT OPERATIONS

When running Virtual Iron® XEE, a set of one or more managed nodes is interconnected with a management node. The following terms will be used in the configuration description.

- A **dedicated management network** is a network that is *entirely dedicated* to management traffic between VI-Center and managed nodes. In this scenario, it is advisable to use the dedicated network to PXE-boot the Virtual Iron® software on each node.
- A **public network** is a network that is used for ordinary network traffic by one or more nodes.

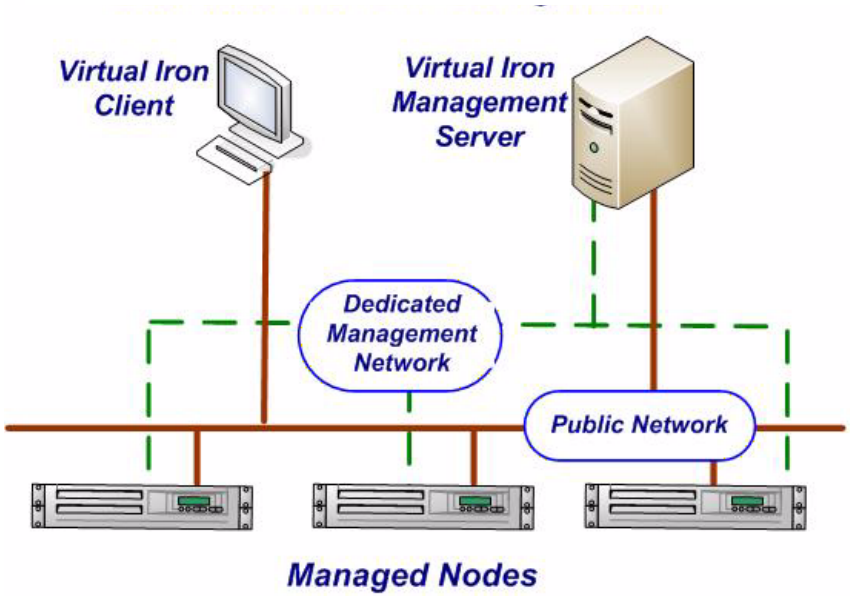
Product Configuration, Extended Enterprise Edition

If you are virtualizing multiple nodes, connect each managed node to the management server (via the dedicated management network), and to one or more *public networks*.

Figure 7 shows a typical configuration. In this case, three systems are connected by a *dedicated* management Ethernet network, which is used exclusively by VI-Center to PXE-boot and manage these nodes. This network is shown as a dashed green line.

The managed nodes are also connected to a public network; this connection is used by the virtual servers hosted on each managed node. It is never used for Virtual Iron® management traffic.

Figure 7. Three Managed Nodes, dedicated management network



MANAGED NODE CONFIGURATION

The managed nodes you will use in the Virtual Iron® framework need to be specially prepared by editing the BIOS setting of each node. The tasks you perform for each type of node will vary, depending on the vendor. They include:

- Virtualization Processor Settings of Each Node
- Configure IPMI or ILO for each Node
- Disabling Hyperthreading Support

Virtualization Processor Settings of Each Node

The Virtual Iron® framework operates only in Intel® and AMD® nodes with virtualization technology (VT) support. In nodes sold by some vendors, the Intel®-VT extensions for the node are set to OFF. Be sure the Intel®-VT extensions for each node are set to ON when checking the node's BIOS settings.

Configure IPMI or ILO for each Node

Some servers are designed to be started up or shut down from a remote console. Two protocols commonly used to provide this capability are IPMI (Intelligent Platform Management Interface) and ILO (Integrated Lights Out). However, some nodes do not support either of these protocols.

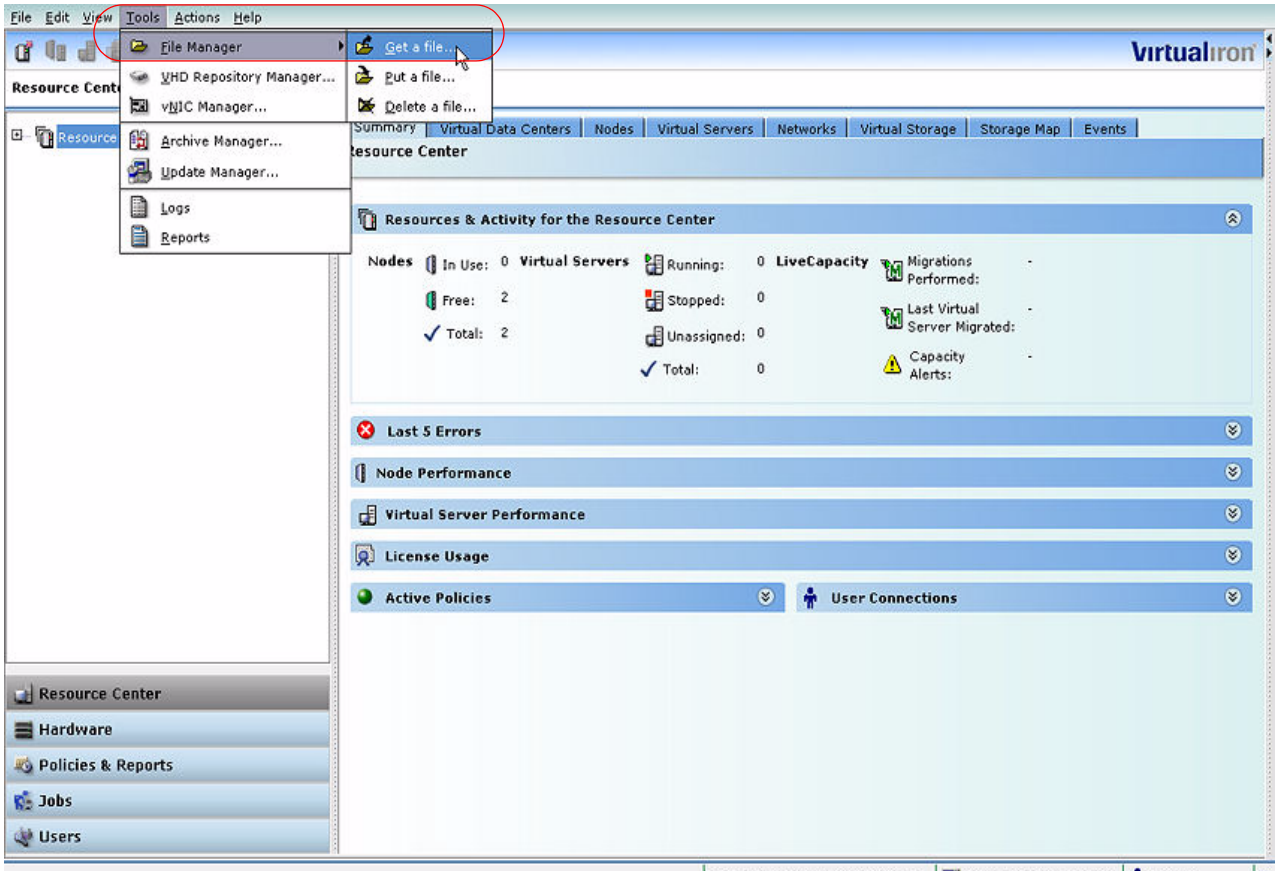
If the node or nodes you are managing with Virtual Iron® support one of these protocols, you need to configure the node so Virtual Iron® is enabled to start up and shut down the node from VI-Center™. Please consult the manufacturer's hardware documentation for details on configuring IPMI and ILO on the node.

CONFIGURING IPMI

To configure IPMI for a node, after logging in:

Step 1. In the **Tools** menu, select **Get a file**. See Figure 8.

Figure 8. Tools Menu, Get a file... option



Step 2. Navigate to the install directory of the server:

VirtualIron\VirtualizationManager\system\generic_ipmi.xml

Step 3. Open this file and edit the following command options with your User Name and Password:

<command-options>-U (Your UserID) -P (Your Password) </command-options>

To view IPMI information, select a node in the navigation tree and click **Hardware.** The information appears in the **Info** pane. See Figure 9.

CONFIGURING ILO

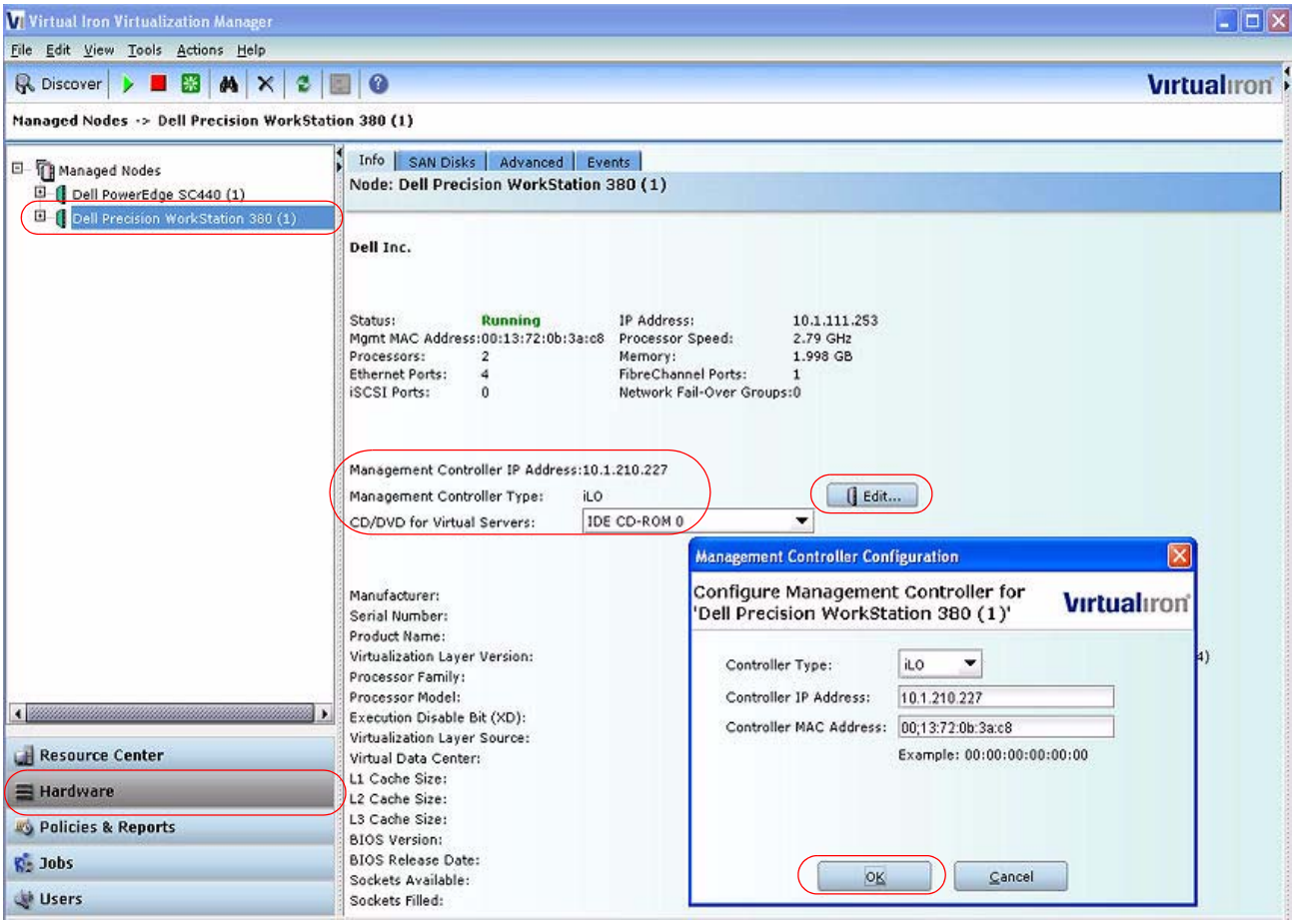
To configure ILO for a node:

Step 1. Click **Hardware** and select a node in the navigation tree.

Step 2. In the Info pane, click **Edit.**

Step 3. Select iLO from Controller Type and provide iLO MAC address. See Figure 9.

Figure 9. Configuring IPMI or ILO Information



Disabling Hyperthreading Support

Virtual Iron® recommends that hyperthreading be set to OFF on Intel® nodes. To do this, restart your managed node and enter the BIOS on startup. Disable the hyperthreading support in BIOS. On most computers hyperthreading is located in the Main BIOS Settings menu. On HP servers it is in the Advanced menu-->Power-On Options submenu.

Note: Turning Hyperthreading ON may adversely affect the performance of certain classes of applications.

BIOS Setting for Managed Nodes

When you add nodes to the VDC, make sure that the NX bit is set to the same value among all the nodes—either all ON or all OFF. Speed Stepping (Power Now on AMD machines) should always be turned off in the BIOS for all new nodes.

PXE Booting Managed Nodes

To PXE-boot managed nodes, follow these steps:

Step 1. Connect all nodes to the machine hosting Virtual Iron® VI-Center.

Step 2. Make sure the BIOS of each node is configured so that PXE or Network boot precedes other methods in the boot order.

Step 3. Boot each managed node.

SITE PREPARATION

The sections that follow cover the key considerations relating to the cabling of nodes in the Virtual Iron® framework.

Define the Physical Infrastructure

Before setting up a lab, adopt a set of cabling conventions to simplify troubleshooting and adding, replacing, or upgrading nodes.

Some additional planning is needed when implementing virtual infrastructure. In the open Virtual Iron® framework, virtualized nodes are partitioned into administrative entities called *virtual data centers*, or **VDCs**.

To derive maximum value from your virtual infrastructure, it is important to make network and SAN connections within each VDC in a consistent way. Set up the physical infrastructure that underlies each set of virtualized nodes so that all nodes in each VDC can access the same networks, and the same SAN resources.

To make efficient use of network resources, map out which nodes/ports are connected to which subnets. Use these guidelines:

- Connect each node to the same physical subnets.
- Connect the port/slots in each node in the same manner.

Details on planning these connections are included in the sections that follow.

Defining Network Connections

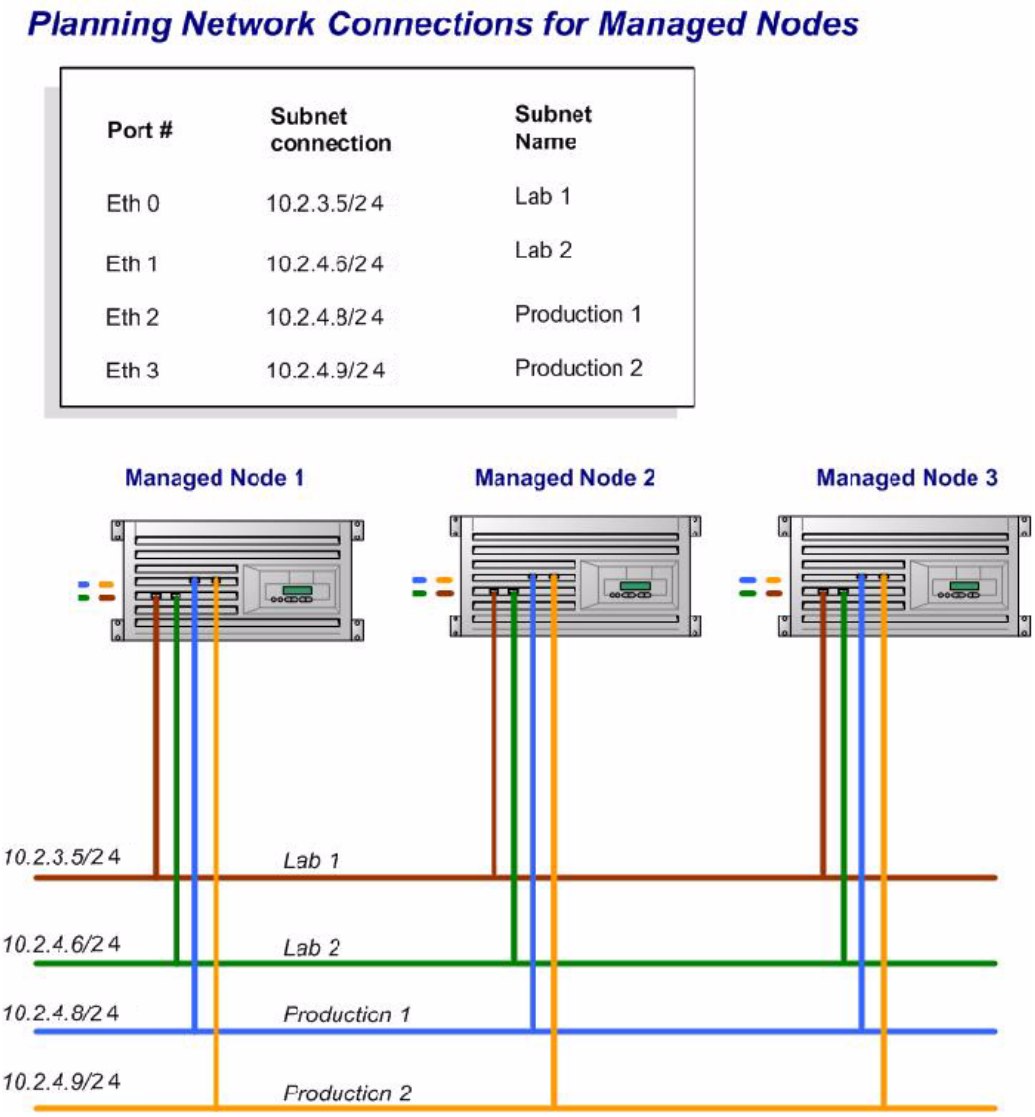
In each VDC, attach each node to the same subnets. As a best practice, each node should have the same connection scheme. For example, connect Eth0 on each node to subnet A, Eth1 to subnet B, and so on.

This scheme gives you the flexibility to migrate a virtual server on one node to another node without losing access to its network(s). In addition, having each node cabled to its subnets using the same-numbered ports simplifies the management, troubleshooting, and configuration of physical nodes.

For example, you may be running a data processing application on a node in network A. This application normally consumes a high-percentage of the cycles available on that node, but it is now running at 5% of capacity. To use resources more efficiently, redeploy the application to another node in the VDC, on network B, C, or D.

Figure 10 shows three nodes, each of which is connected to four subnets. Note that each same-numbered Ethernet port in each node is connected to the same subnet—Eth0 connects each node to subnet Lab 1, Eth1 connects each to Lab 2, and so on.

Figure 10. Network Connection Scheme for Managed Nodes

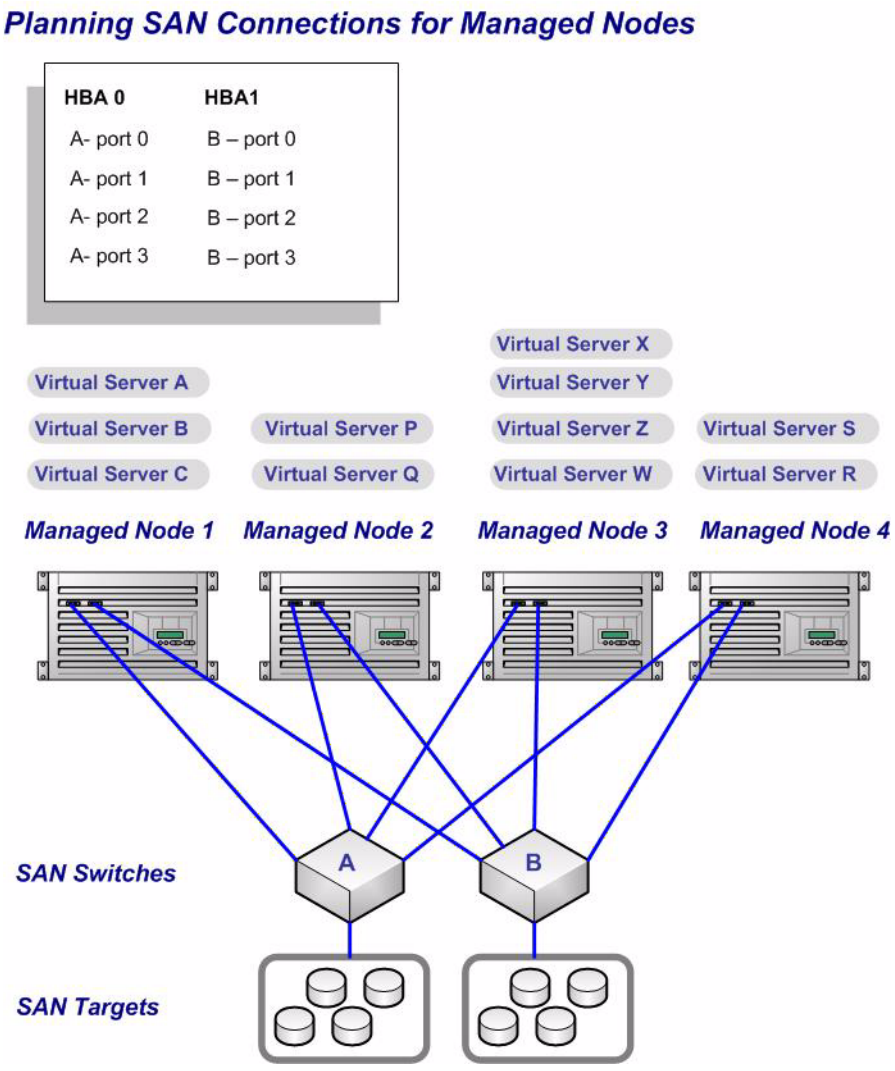


Connecting Nodes to the SAN Infrastructure

Before you connect nodes to the SAN infrastructure, bear the following considerations in mind.

- Adopt a consistent connection scheme between HBAs/ports and SAN switches.
- Be sure that each node is connected to each enterprise SAN switch. This assures that the virtual servers hosted by each node have access to all targets/LUNs. This is what enables LiveMigration, LiveCapacity®, and LiveRecovery between existing nodes.

Figure 11. SAN Connection Scheme per VDC



BEFORE YOU INSTALL VIRTUAL IRON®

There are a number of considerations you must make before installing Virtual Iron:

- Before installing the product, interconnect the *VI-Center node* with *managed nodes* in your data center, and set the managed nodes to PXE or network boot. See Managed Node Configuration for information on preparing managed nodes.
- Check the requirements provided in Product Requirements. For detailed hardware requirements, check

  http://www.virtualiron.com/Support/Compatibility-and-Requirements/index.php
- All anti-virus software applications must exclude the Management Server installation directory. This is because of file permission conflicts, which could cause data corruption. The VI-Center user interface may also run slowly if anti-virus software is running on the management server host. This may occur because some anti-virus software inspects Java applications, resulting in reduced VI-Center client performance. To prevent this, designate VI-Center as a trusted application in the virus-scanning software.
- You should use a dedicated ethernet port for the management network and not a VLAN.
- Bonded interfaces are not supported during installation.

INSTALLING VIRTUAL IRON®

The following instructions describe how to install Virtual Iron® on multiple managed nodes.

Install the software on the system designated as the *management server node* in Figure 6. This system hosts the VI-Center®, which is used to configure, start, and manage virtual servers on one or more nodes.

Step 1. To install Virtual Iron®, proceed as follows.

For Linux:

Execute the bin file as follows:

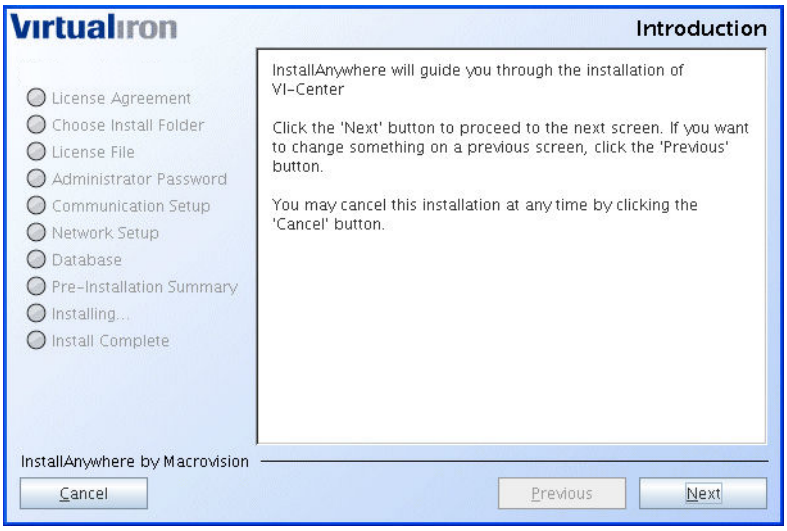
```
# sh ./VirtualIronInstall4xx.bin
```

For Windows®:

Double click this file:

VirtualIronInstall4xx.exe

Step 2. When the download completes, the introductory screen appears. Click **Next** to begin the installation.

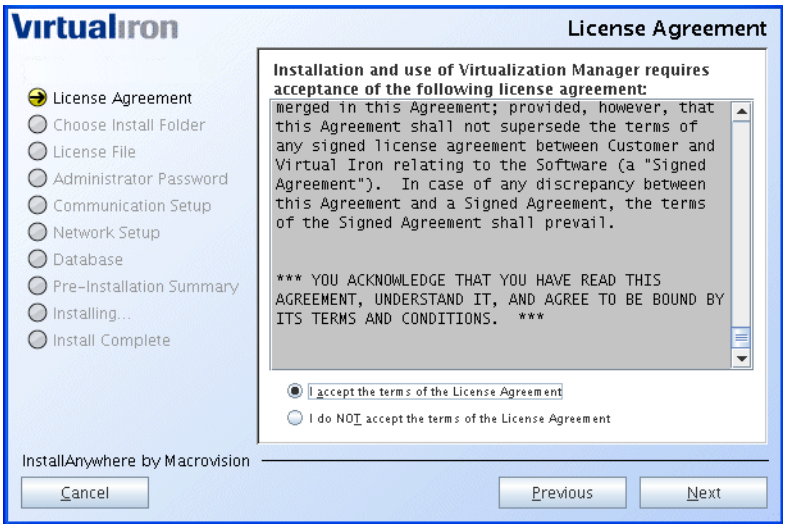


Step 3. At this point, the installation process checks to see whether standard DHCP port 67 or TFTP port 69 is in use on the installation host.

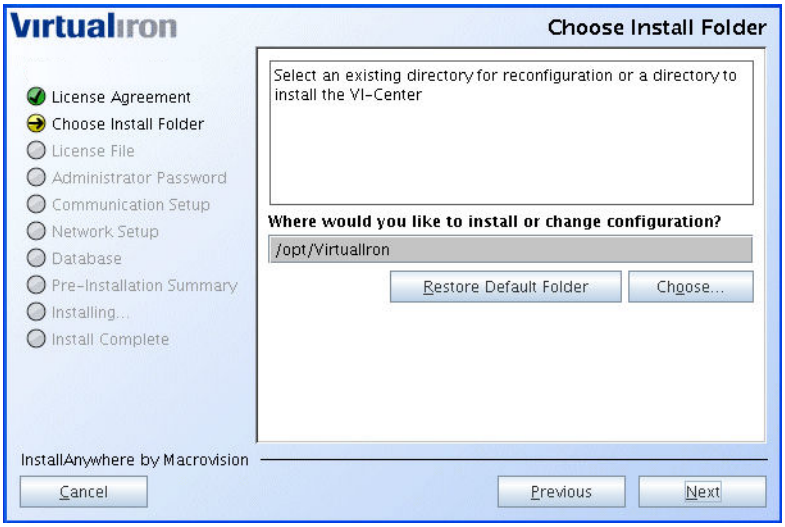
To PXE-boot managed nodes (as explained in Product Configuration, Extended Enterprise Edition), these ports are required. If either port is in use, a DHCP or TFTP Port in Use window appears warning that VI-Center may not function properly. Resolve this issue before continuing the installation.

Step 4. In the License Agreement dialog, you are prompted to read and accept the Virtual Iron® license agreement. You must accept the agreement to continue the installation.

Step 5. Click **Next**.



Step 6. Next, choose a location for the installation. You can enter a path for the installation, or choose the default folder. (For Linux, this is **/opt/VirtualIron**. After selecting a location, click **Next**.



Step 7. Enter the location of the Virtual Iron license file. This file is not included in the distribution, but is sent to you by Virtual Iron®. (The example

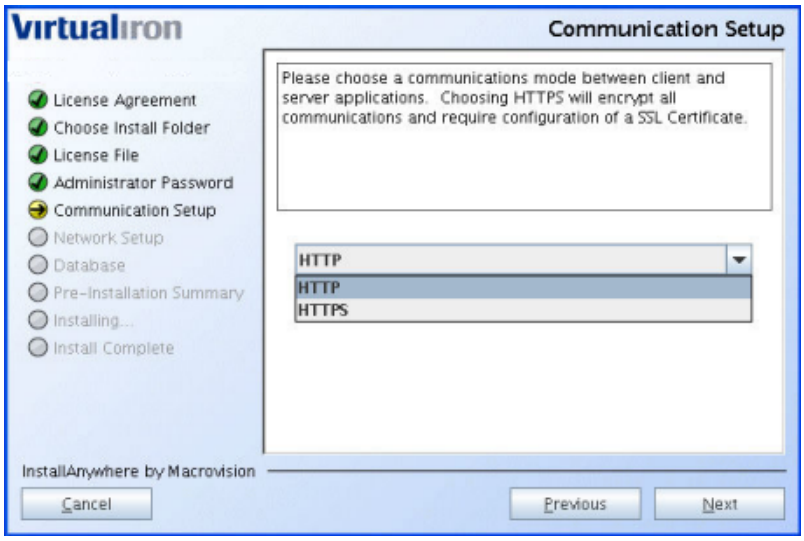
shown is from a Windows® installation.)

Step 8. Enter an Admin password. The password and confirmation password you choose must match be 6-32 characters long. *Remember this password as you will need it to log in to the system later!*

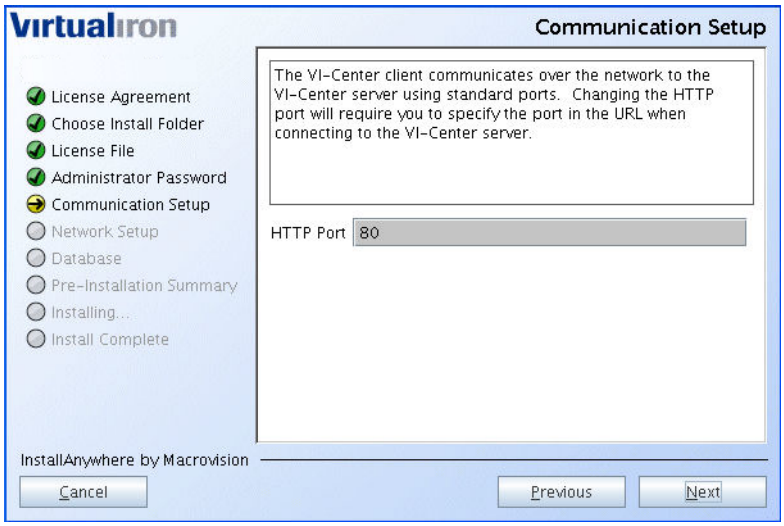
If your password and confirmation do not match, an error message appears prompting you to reenter the password.

Note: You can change the admin password at a later time, see Changing a User Password.

Step 9. Choose HTTP or HTTPS for the connection type to use between the VI-Center client and server.



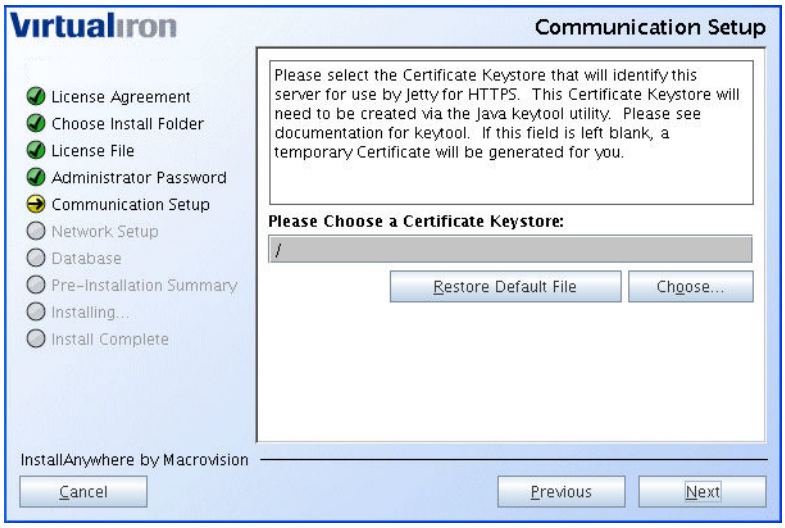
If you choose **HTTP**, the window shown below appears. This allows you to choose a port or use default port 80.



If you select **HTTPS**, select a port or use default port 443. You can also select your own keystore. If you choose to do this, you must provide passwords for the keystore.

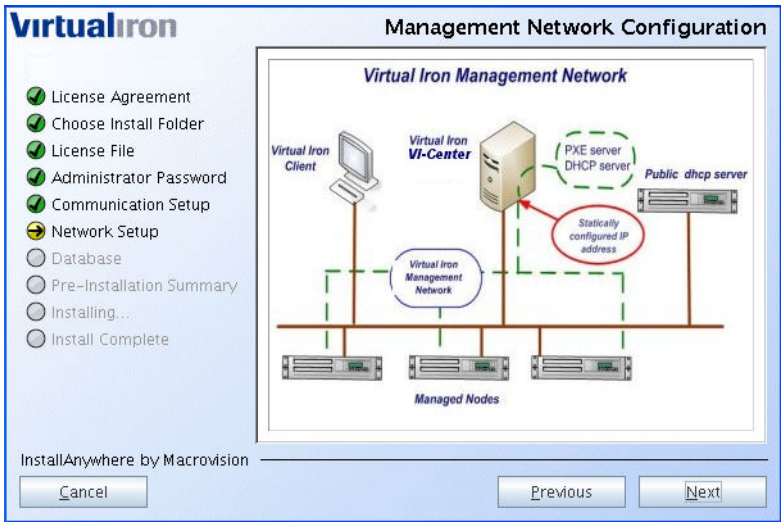
The installer validates the availability of the port you have chosen. If the port is unavailable, a pop-up window appears, informing you to choose an unused port.

Step 10. If you have chosen HTTPS, the following window appears. (The window shown is from a Linux installation.)



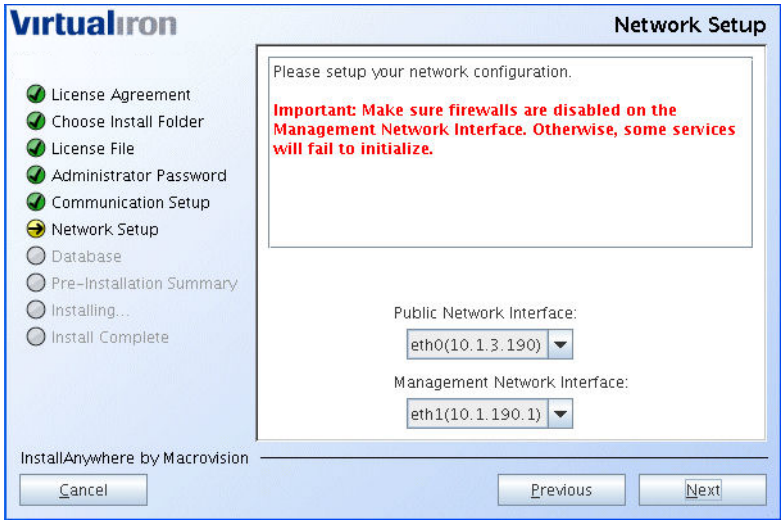
Step 11. If you chose a certificate keystore in the preceding step, enter passwords for the keystore and the certificate key.

Step 12. The illustration that appears at this point shows a representative configuration of the management network. Note that two networks are present. The Virtual Iron management network is a private network between the VI-Center and all managed nodes. These nodes are also connected to a public network.



Click **Next** to continue.

Step 13. Assign the IP addresses that the VI-Center uses to connect to the private management network and the public network.



VI-CENTER AND DATA PROTECTION

VI-Center needs to be deployed and running on a platform that is capable of maintaining critical applications. Although Virtual Servers continue to run even when the VI-Center is not, the VI-Center should be configured as an always-on product.

As with any database-based product, database corruption can occur if there is a loss of power or a management server connected to a storage subsystem configured with write-caching is improperly shut down. This could affect the most current statistics collection, configuration changes, and log file updates.

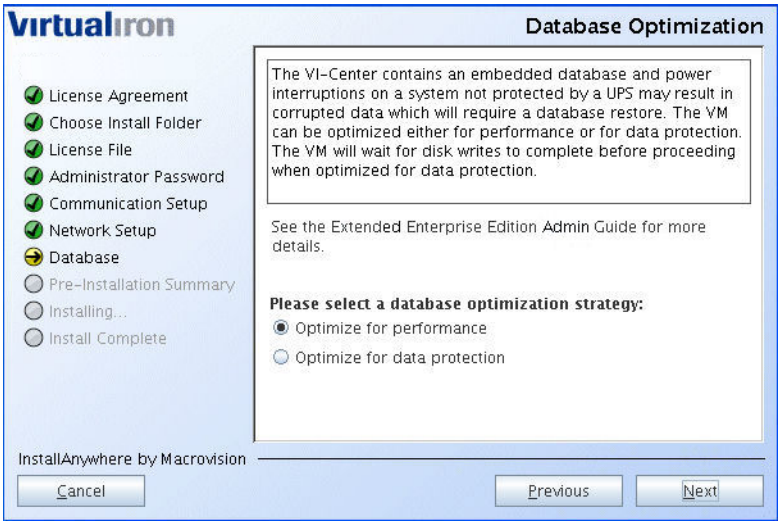
To be fully functional again may require restoring the database with a backup version. As a result, some critical data may be lost. It is a best practice to operate the VI-Center with a UPS (uninterruptible power supply) and to run regularly scheduled backups.

See Performing Backup and Restore Operations for additional information.

Step 14. If your system is not protected by a UPS, there is a risk of database corruption in the event of a power interruption. This would require restoring the database and could result in lost data.

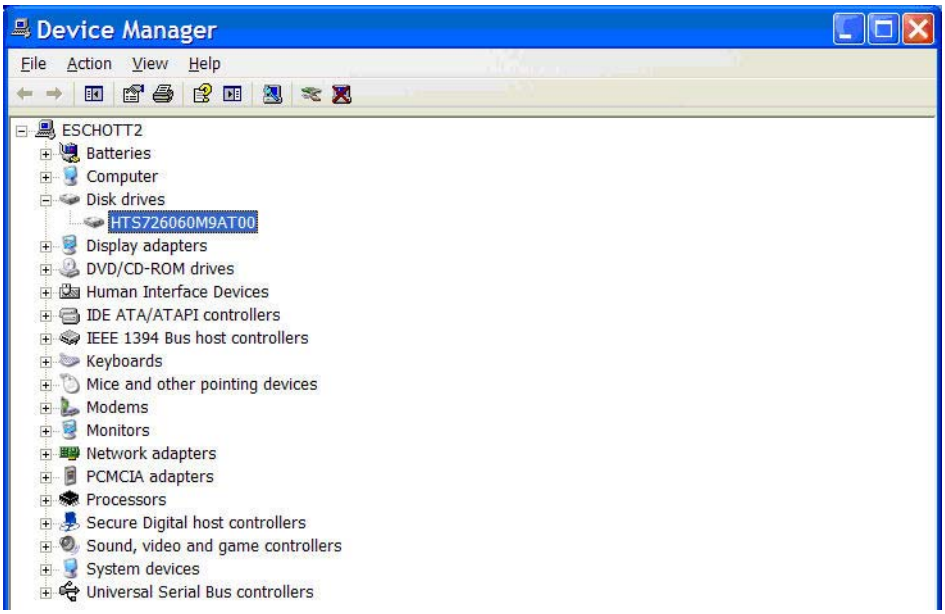
Select **Optimize for data protection** to reduce this risk. This causes VI-Center to wait until the data is completely written to the disk before proceeding. To ensure that performance is not adversely affected, Virtual Iron recommends disks capable of operating at a minimum of

7200 RPM.

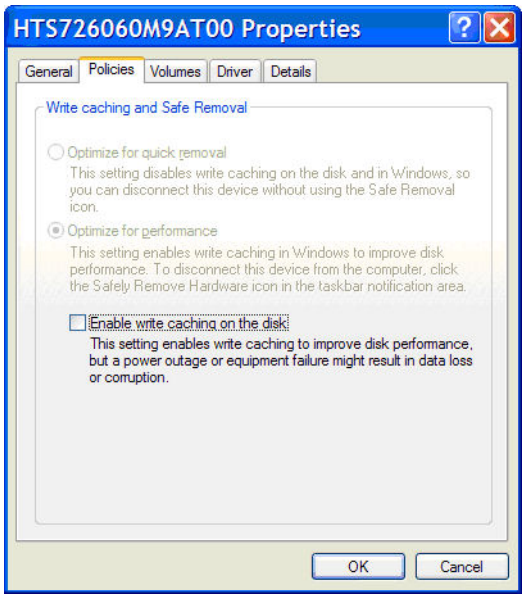


For systems running Windows, if you select **Optimize for data protection**, you also need to disable write caching on the disk that is used to store the VI-Center database. Do the following to navigate to the Device Manager:

- Right-click **My Computer** and then click **Properties**.
- Click the **Hardware** tab.
- Click **Device Manager**.
- Click the plus sign (**+**) next to the **Disk Drives** branch to expand it.
- Right-click the drive on which you want to enable or disable disk-write caching, and then click **Properties**.

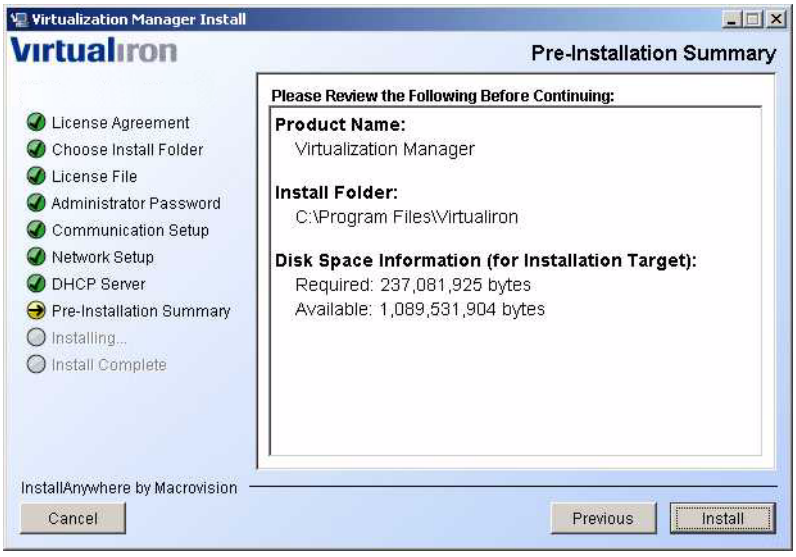


- Click the **Policies** tab.

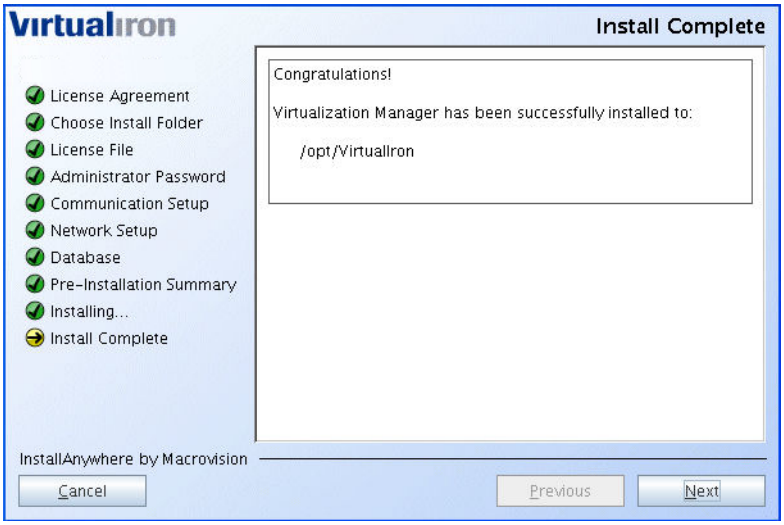


- Click to clear (uncheck) the **Enable** write caching option.
- Click **OK**.

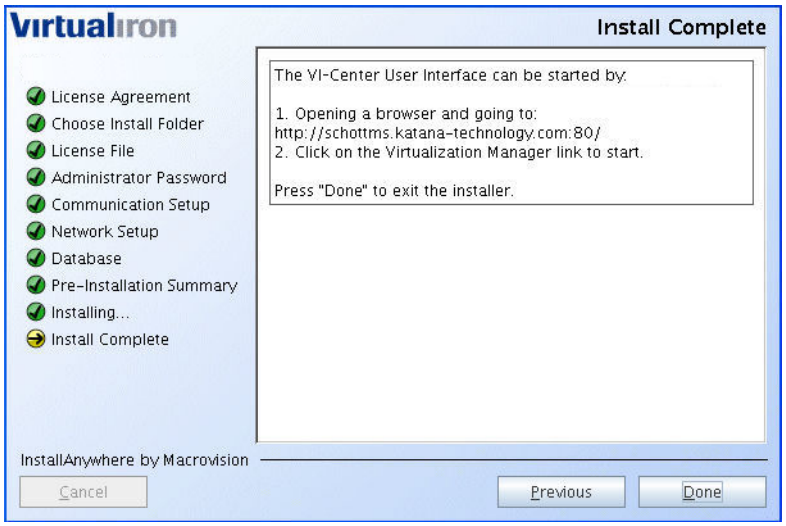
Step 15. After making your database optimization selection, the VI-Center Install window displays a pre-installation summary. To proceed with the installation, click **Install**. (The example shown here is for a Windows® installation.)



Step 16. A screen appears with the install location. Click **Next**.



Step 17. When the installation is complete, click **Done** to close the window. (Example: Windows® installation). VI-Center starts automatically.



Note: After installing VI-Center on a Management Server running Red Hat Linux, you must disable the firewall in order to access the NBD directory.

CONNECTING TO THE VI-CENTER

After installing Virtual Iron®, use a web browser to connect to the VI-Center node (the node on which you installed the product).

Step 1. For the URL, use the IP address of the management server's public network.

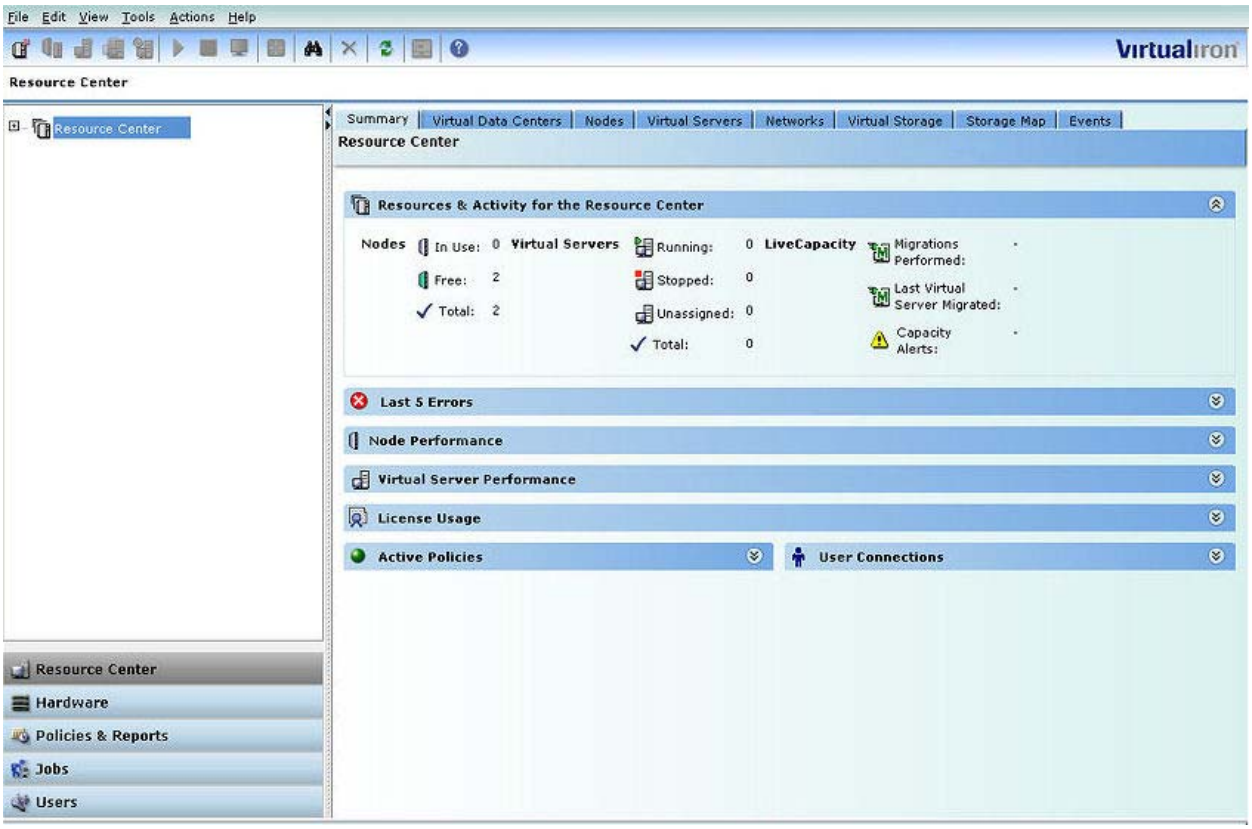
Step 2. On the Virtual Iron® screen, click **VI-Center**.

Step 3. The application starts, and you are presented with this login screen. Enter the Password you specified when you installed VI-Center, and click **OK**.

Figure 12. Login Screen

Step 4. VI-Center opens, as shown in Figure 13. If the Tutorial appears to the right of the Resource Center window, you may close it at any time by selecting **Help** and unchecking **Show Tutorial**.

Figure 13. .VI-Center Interface



3

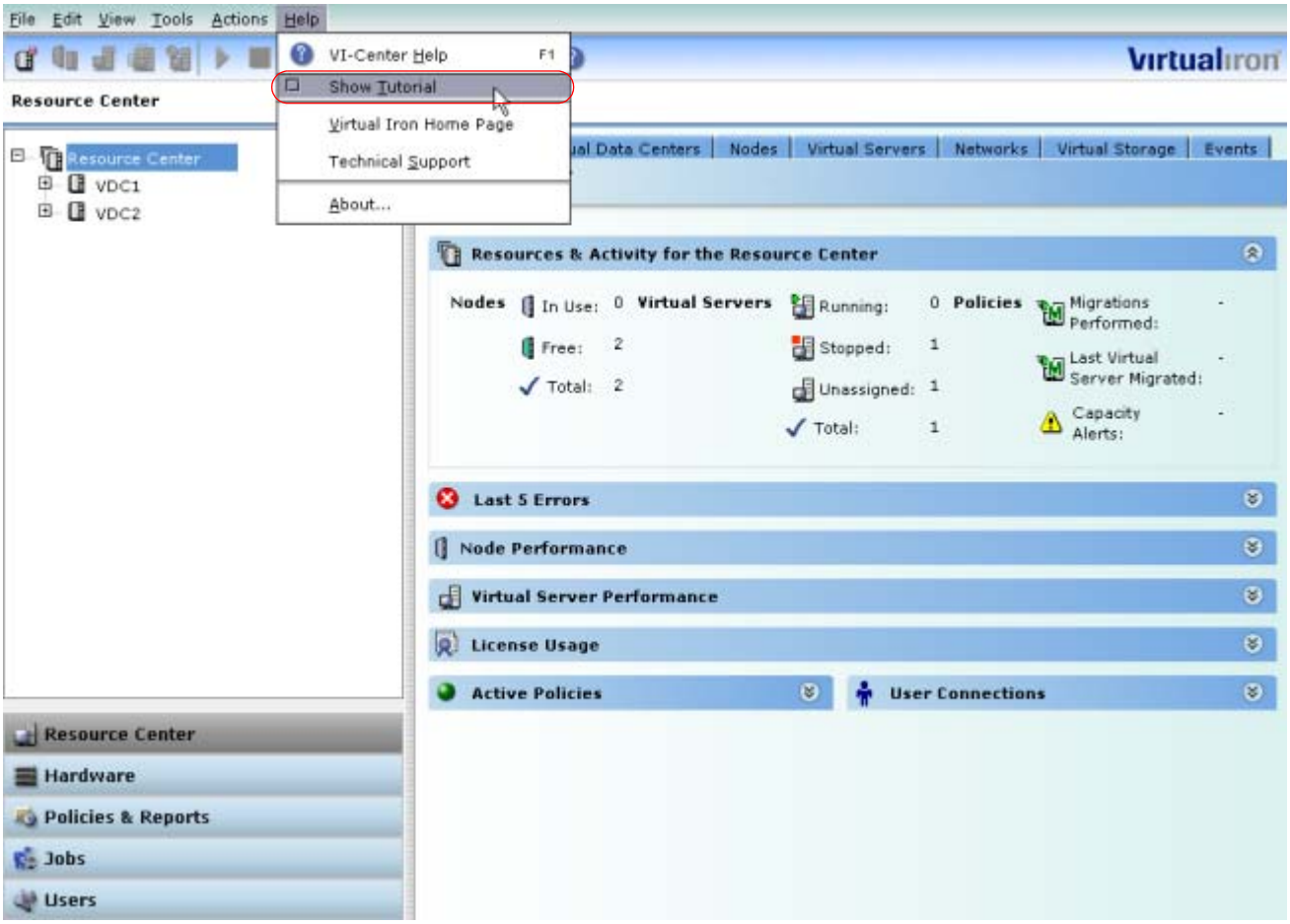
USING VI-CENTER®

USING THE INTEGRATED TUTORIAL

Virtual Iron® includes a tutorial that opens when you first connect to VI-Center. (See Connecting to the VI-Center.) The tutorial provides a high-level look at the product, with instructions on how to configure and start a virtual server.

The tutorial takes about 10 minutes and provides an introduction to the design of the management framework and the controls that make up the client interface. You can open or close the tutorial at any time by clicking the **Show Tutorial** check box on the **Help** pulldown (see Figure 14).

Figure 14. Open the Tutorial



VI-CENTER OVERVIEW

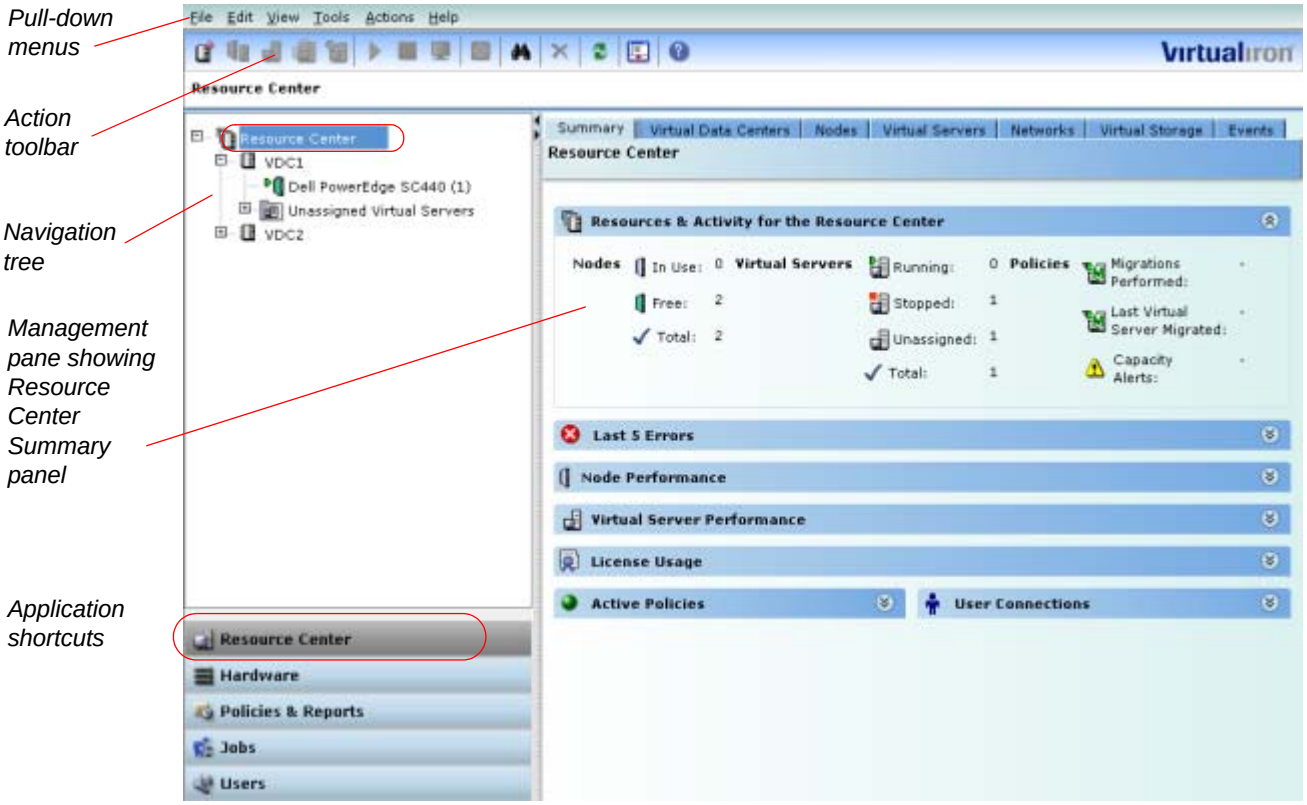
Once you install and configure Virtual Iron®, you have a *virtualization environment* in which to create and manage *virtual servers* on a set of *managed nodes*. Management for this environment is provided by Virtual Iron® VI-Center™, a transaction-based framework that also includes an integrated database and a web-based management user interface.

The VI-Center user interface provides a set of work areas, buttons, pull-down menus, and tabs for access to various functions and configuration screens. See Figure 15:

- **Pull-down menus**—File, Edit, View, Tools, Actions, and Help
- **Action toolbar**—Allows quick access to a group of task icons
- **Navigation tree**—Shows hierarchy of physical and virtual components. Click on a component to open its default Summary pane and related management panes.
- **Management pane**—Resource Center, Hardware, Policies & Reports, Jobs, and Users
- **Application Shortcuts**—Allows quick access to all management panes

The sections that follow describe each set of controls and their relationship to one another. Use the integrated tutorial to familiarize yourself with the product.

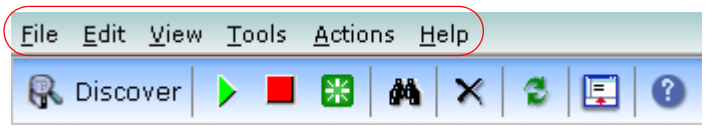
Figure 15. Overview of Client Design



USING THE PULL-DOWN MENUS

VI-Center contains a set of standard pull-down menus which are discussed briefly in the sections that follow.

Figure 16. Pull-down Menus

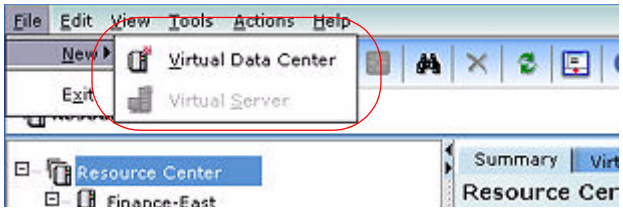


File Menu

The File menu options change depending on which application option you are using. **Exit** is the only available option when you are working in the Hardware, Policies & Reports, or Jobs panes.

- If you select **Resource Center**, use these File menu options to do the following:
  - **New—>Virtual Data Center**—Highlight **Resource Center** in the navigation tree to activate this option. Click to add a new virtual data center to the Resource Center.
  - **New—>Virtual Server**—Highlight a **node** in the navigation tree to activate this option. When you click to add a new virtual server to the node, the New Virtual Server Wizard appears.
- If you select **Users**, select **New User Accounts** to add users.
- For all application options, **Exit** exits VI-Center and closes the client user interface.

Figure 17. File Menu Options



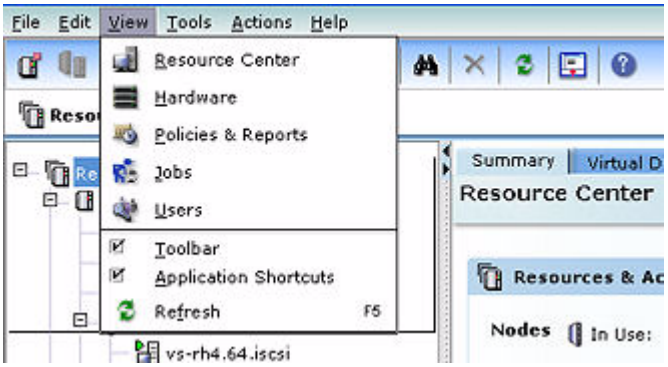
Edit Menu

Use the Edit menu to Delete objects from or Find objects in the database.

View Menu

Use the View menu to hide or show the Toolbar and Application Shortcut options, and to refresh screen data.

Figure 18. View Menu Options



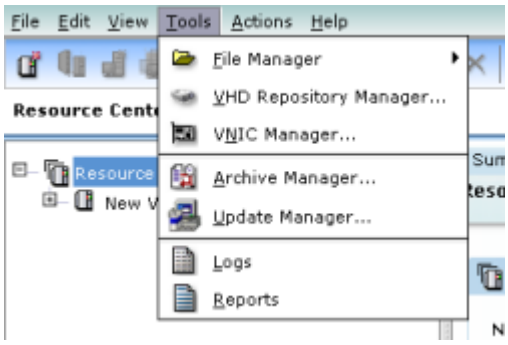
The first group of options in this menu open the same summary panes as the **Application Shortcuts**; use this menu to access the screens associated with the **Resource Center**, **Hardware**, **Policies & Reports**, **Jobs**, and **Users** options. Each of these options is discussed in Using the Application Shortcuts.

- Deselect **Application Shortcuts** to hide these options. When selected (checked) they appear below the navigation tree.
- Deselect **Toolbar** to hide the Toolbar icons. When selected (checked) they appear just below the pull-down menus.
- Click **Refresh** to update the client UI with the latest information from the VI-Center database.

Tools Menu

Use the Tools menu to manage your archives, import or export hard drive images, and configure software update notifications.

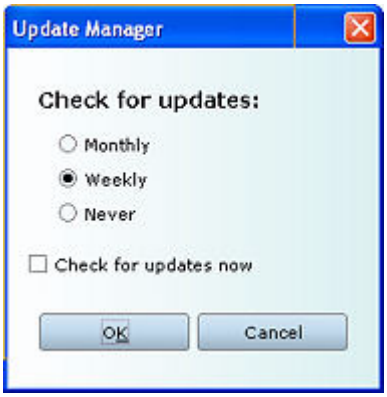
Figure 19. Tools Menu



- **File Manager**—Use the **Get a file** and **Put a file** options to move files to and from VI-Center. For example, you can move an iso file to the NBD (Network Block Device) directory on VI-Center, making this image available for booting by virtual servers.

Note: When performing put or get operations, proceed with caution. There is no warning if by moving a file you will overwrite a file in either the source or destination directory.

- **VHD Repository Manager**—Imports or exports a virtual hard drive image to or from the VI-Center VHD repository and your local computer. See VHD Repository.
- **NBD Repository Manager**—Sets the directory for network boot device ISO images.
- **VNIC Manager**—Creates virtual NICs for virtual servers. You must have at least one VNIC to create a virtual server. See Creating a Virtual NIC.
- **Archive Manager**—Moves all jobs and associated events that are older than a specified date to a location in the VI-Center database. See Configuring the Archive Manager.
- **Update Manager**—VI-Center checks, according to a period you specify, whether there is a new software version available for download. If there is, you are notified via email. Allows monthly, weekly, or immediate notification of Virtual Iron software updates.



- **Logs**—Provides access to various node logs such as backup, system, DHCP and TFTP logs which can be useful to Virtual Iron® customer support.
- **Reports**—Provides access to an index of all reports stored in the database. See Reports for information on generating reports.

Actions Menu

The Actions menu options change, depending on which of the application views you select from the View menu or the Applications Shortcuts, located below the navigation tree.

Note that the Action Toolbar icons also change according to the Application Shortcuts view you are working in to correspond with the Actions menu.

RESOURCE CENTER

Use the Actions menu to start, stop, and restart virtual servers, and open a console. Other operations include cloning virtual servers and performing snapshots. See Creating and Configuring Virtual Servers for information and procedures.

HARDWARE

In the Hardware view, use the Actions menu to start, stop, and restart virtual servers, discover hardware, and rescan SAN Ports. See Creating and Configuring Virtual Servers, and Configuring Storage.

POLICIES & REPORTS

In the Policies & Reports view, use the Tools menu to start and stop policies. For an overview of the Policies & Reports view, see Policies and Reports in this chapter. For detailed information and procedures, refer to the Policies and Reports chapter.

JOBS

In the Jobs view, use the Tools menu to abort an operation in progress. For a detailed description of the Jobs view, see About the Jobs Framework.

Help Menu

The Help menu contains links to Virtual Iron documentation, technical support, and licensing information.

- **VI-Center Help**—Select this option or press the **F1** key to open Virtual Iron Online Help, the electronic version of the *Virtual Iron System Administrator Guide*.
- **Show Tutorial**—The *Virtual Iron Tutorial* takes you through the steps for setting up a virtual server. Check or uncheck the box in the menu to open or close the tutorial.

- **Virtual Iron Home Page**—This option is a link to Virtual Iron's website. Of particular interest is the **Services and Support** option, which contains links to the following:
  - Product documentation
  - A searchable knowledge base
  - Compatibility and requirements lists
  - Other support resources, such as upgrading and conversion procedures and access to Virtual Iron forums and blogs
  - Professional services
- **Technical Support**—This option provides a login window for email correspondence with technical support personnel.
- **About**—This option opens the About VI-Center window which contains tabs for viewing the current software version, licensed and unlicensed features on your system, and an end-user license agreement. Information concerning licensed features is described in more detail in the next section.

Accessing Version and License Information

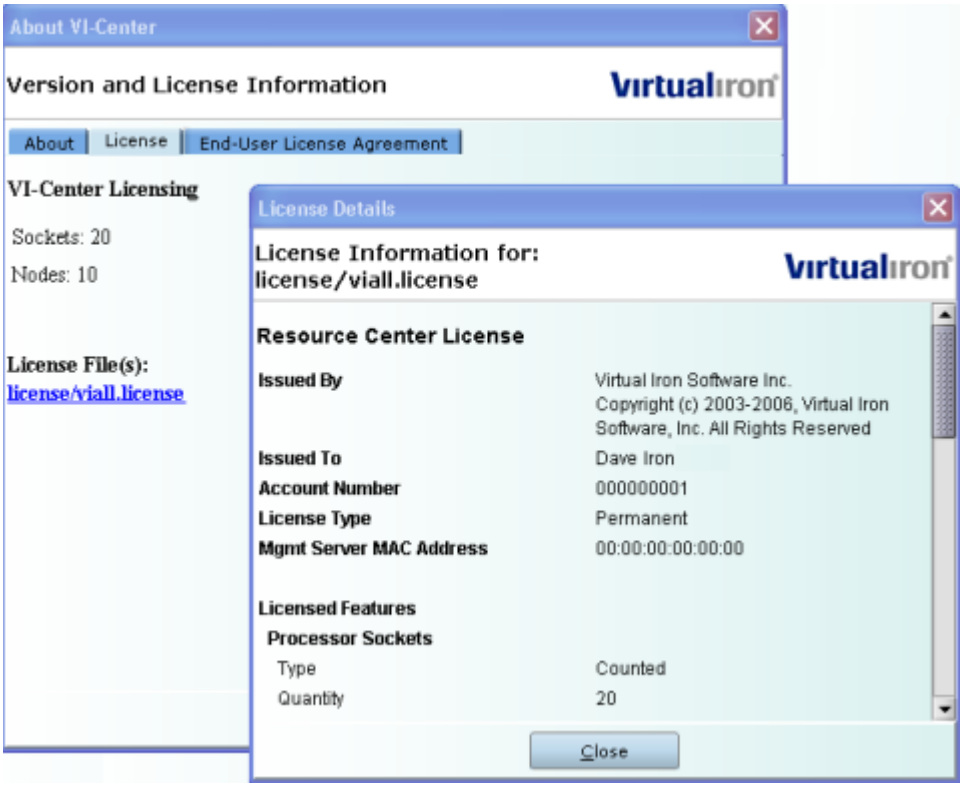
Each Virtual Iron® license supports a specific number of sockets that may contain a single-core or multi-core CPU. As of release 4.4, there are no limits on the number of MAC addresses allowed per license. There is a new tool in the Tools menu that allows you to generate as many VNICs as you require.

DETERMINING WHAT YOUR LICENSE SUPPORTS

To determine which Virtual Iron software version you are running click the **Help > About**.

To check which features you are currently running, and the number of supported sockets, select the **License** tab or click an individual license file link for detailed information about the license as shown in Figure 20.

Figure 20. Virtual Iron Management Server Licensed Features Window



The Virtual Iron Management Server window displays information pertaining to your system, including your account number, the number of sockets in use, the management server's MAC address, and the features you are currently licensed, or not licensed, to use.

Scroll down to see a list of all virtual network adapters and virtual host bus adapters.

Note: In this context, each *socket* houses a processor: a single chip that contains one or more cores. Each *core* consists of one or more execution units, and a set of shared execution resources (such as cache and I/O).

To obtain additional features, contact your Virtual Iron representative.

ADDING A NEW LICENSE

Step 1. Obtain a new license from your Virtual Iron representative.

Step 2. Copy the license file to the license directory.

The default directory for Windows:

`Program Files/VirtualIron/VirtualizationManager/license`

The default directory for Linux:

`opt/VirtualIron/VirtualizationManager/license`

Step 3. Restart the Management Server.

USING THE APPLICATION SHORTCUTS

The Application Toolbar buttons define the functional areas for operations performed in the Virtual Iron® framework.

Resource Center

Click **Resource Center** from the Application options to manage virtual data centers (VDCs), managed nodes, and virtual servers. It is in the Resource Center that you create VDCs, assign managed nodes to VDCs, and then create and configure virtual servers on the nodes. Resource Center is the top-level object in the navigation tree. A sample of the tree is shown in Figure 21.

RESOURCE CENTER TABS

The default Summary tab in the Resource Center management pane presents a high-level view of configured resources, as well as migration and capacity information. The remaining tabs mirror the hierarchy shown in the navigation tree.

Click these tabs to perform configuration tasks and obtain detailed information on VDCs, nodes, and virtual servers. Click the **Events** tab for activity information on all the objects in the Resource Center. See Figure 21.

Figure 21. Resource Center Tabs

Hardware

Click **Hardware** for information on *managed nodes* and their components, and to configure these components.

Figure 22 shows a sample display of the Hardware view with one of the nodes selected.

Figure 22. Hardware View, Ethernet Port Selected

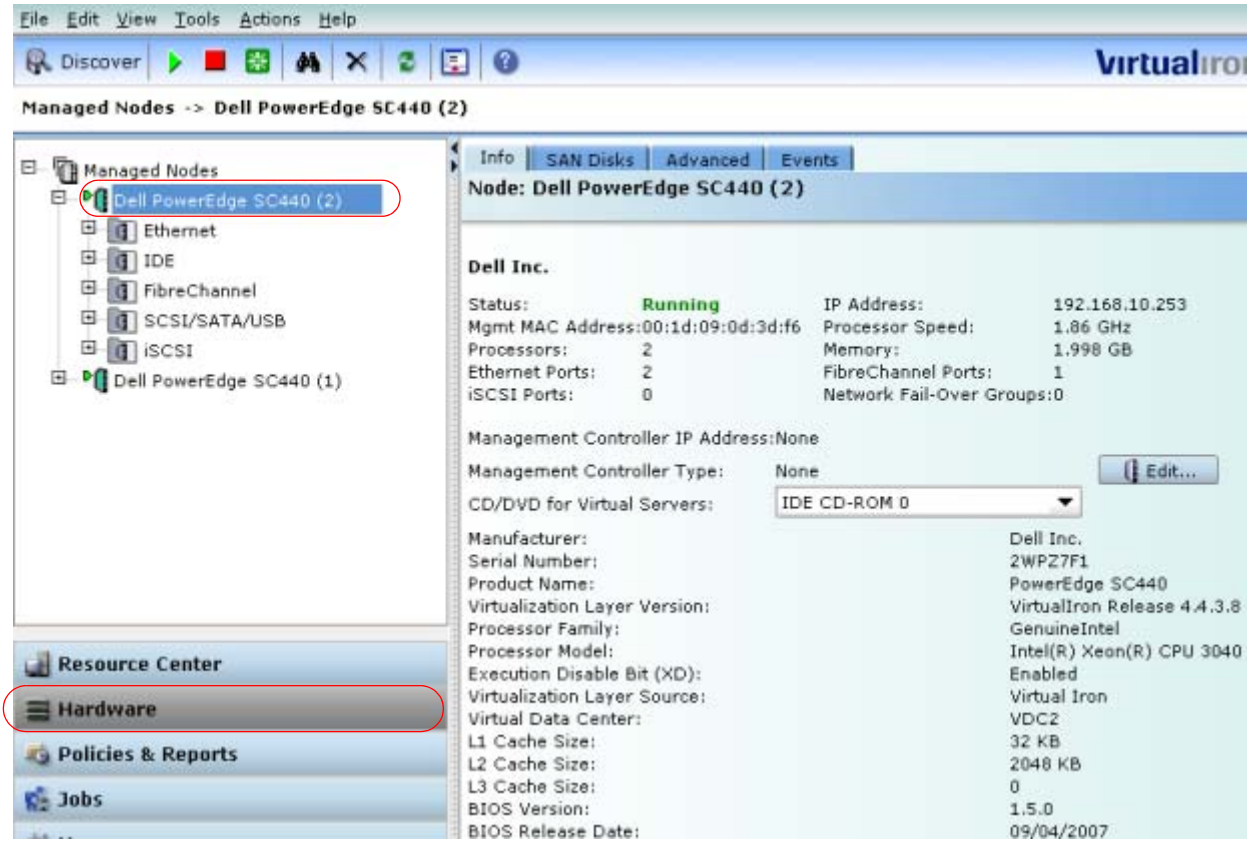
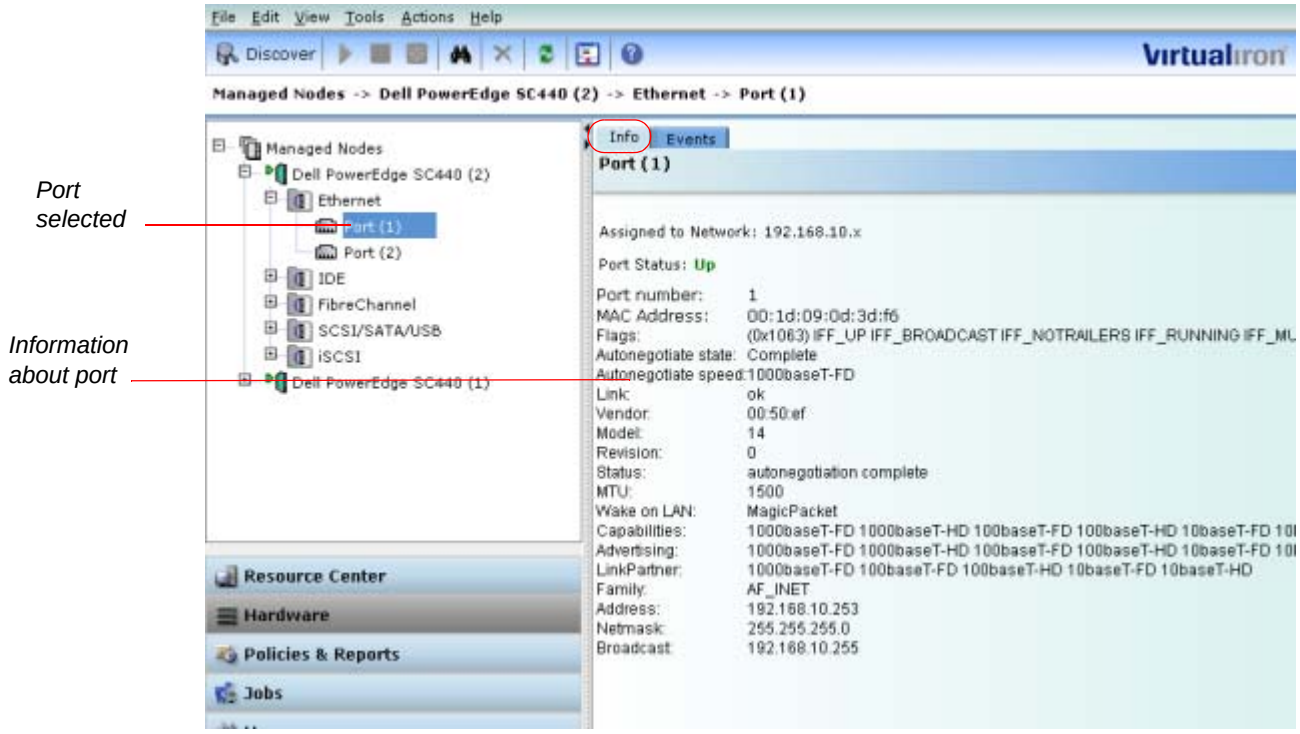


Figure 23 shows a sample display of the Hardware view with four nodes. Each of these nodes has an Ethernet card, CD ROM drive, and a Fibre Channel card. In this case, Dell 440 node, Ethernet port 2 is selected. Information on the card is displayed in the **Info** pane.

Figure 23. Hardware View, Ethernet Port Selected



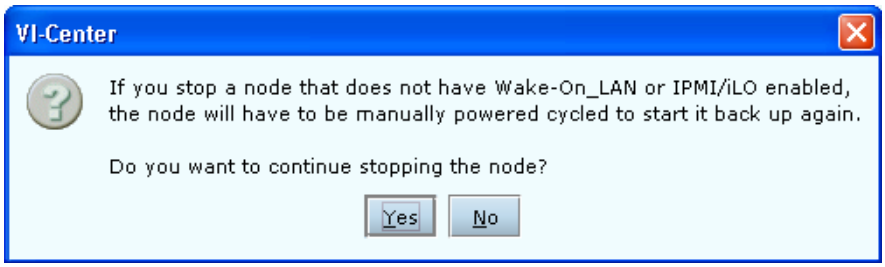
STOPPING A NODE

Step 1. Click **Hardware** tab.

Step 2. Select the node you want to stop.

Step 3. Click the **Stop** button.

A warning dialog appears.



Step 4. If you are sure the node is configured to start via Wake-on-LAN or IPMI, click **Yes**.

STARTING A NODE

Step 1. Click **Hardware** tab.

Step 2. Select the node you want to start.

Step 3. Click the **Start** button.

Policies and Reports

When you click **Policies and Reports** in the Application toolbar, options for User Policies, Reports, and System Policies are listed in the navigation tree. The Policies and Reports pane shows which policies are configured and scheduled. Note the Policy Key in the title bar, which indicates status.

Select from the options to configure policies that affect virtual servers in the environment or to generate reports according to criteria you specify. Note that for some reports you may choose either HTML or CSV (comma separated values) for the output format.

USER POLICIES

Configure these policies to alert a user of specific events, configure criteria for rebooting selected nodes, or scheduling backups.

- **EmailNotifier**—Set up email notification for specified users whenever a specified node, virtual server, or virtual data center experiences a specified event category.
- **RebootDataCenter**—Use this option to set reboot rules for all data centers or each data center.
- **SystemBackup**—Use this option to set the location for a backed-up VI-Center database, and the number of backups to retain.

REPORTS

- **EventReport**—Use the tabs associated with this option to set the frequency, date range, and event type to be reported: Informational, Warning, or Error.
- **JobReport**—Use the Summary pane to set the frequency or date range for a report that shows all jobs performed during that period.
- **NodeReport**—In the Summary pane, specify report criteria for all nodes or specific nodes in the virtual data center. In addition, you can apply these criteria to all or a selected virtual data center, and whether the report output is applied to groups, volumes, or virtual disks.
- **VirtualDisksReport**—You may select various combinations of specific types and states of virtual disks. You may choose to limit output to groups, volumes, or virtual disks.
- **VirtualServerReport**—You may select various combinations of criteria for virtual servers from all or a specific virtual data center.

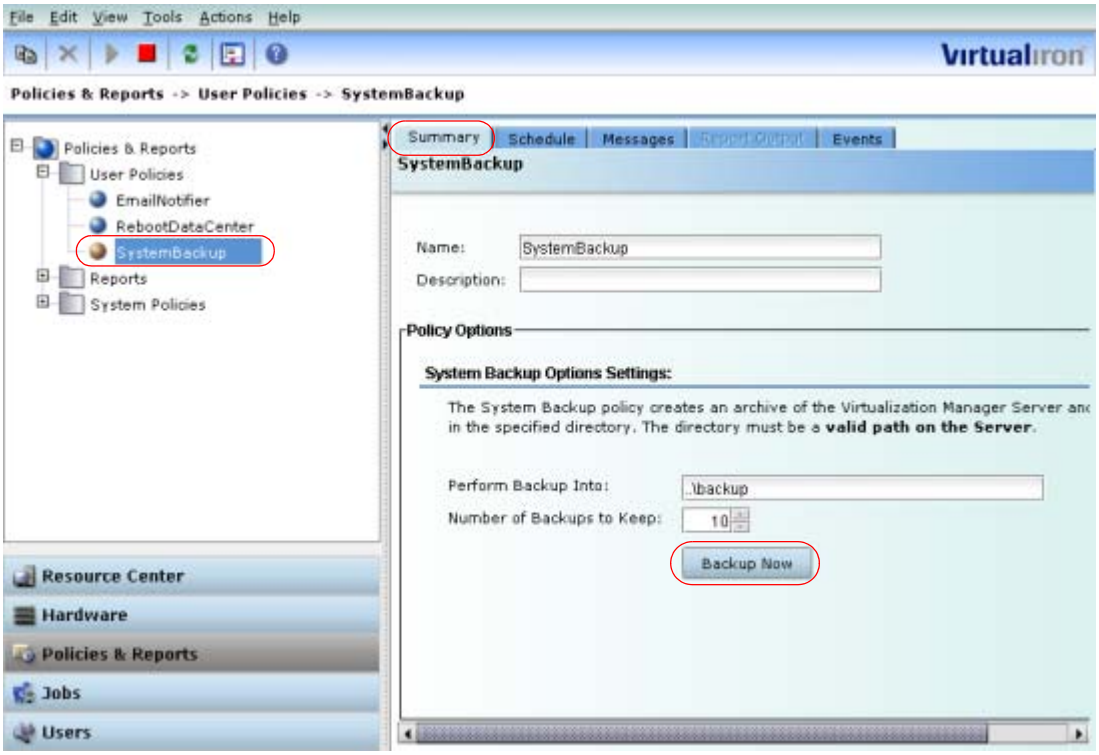
SYSTEM POLICIES

System policies apply to the environment as a whole.

- **AutoRecovery**—Provides high availability for virtual servers by automatically moving them to a new physical server if their managed node fails.
- **LiveCapacity®**—Optimizes virtual server use across a shared pool of resources. It automatically moves running virtual servers to a new physical server in a VDC if any of the servers exceed a specified CPU threshold for a fixed period of time.

Figure 24 shows a sample of the Policies and Reports area. See Policies and Reports for more information and procedures.

Figure 24. Policies and Reports View



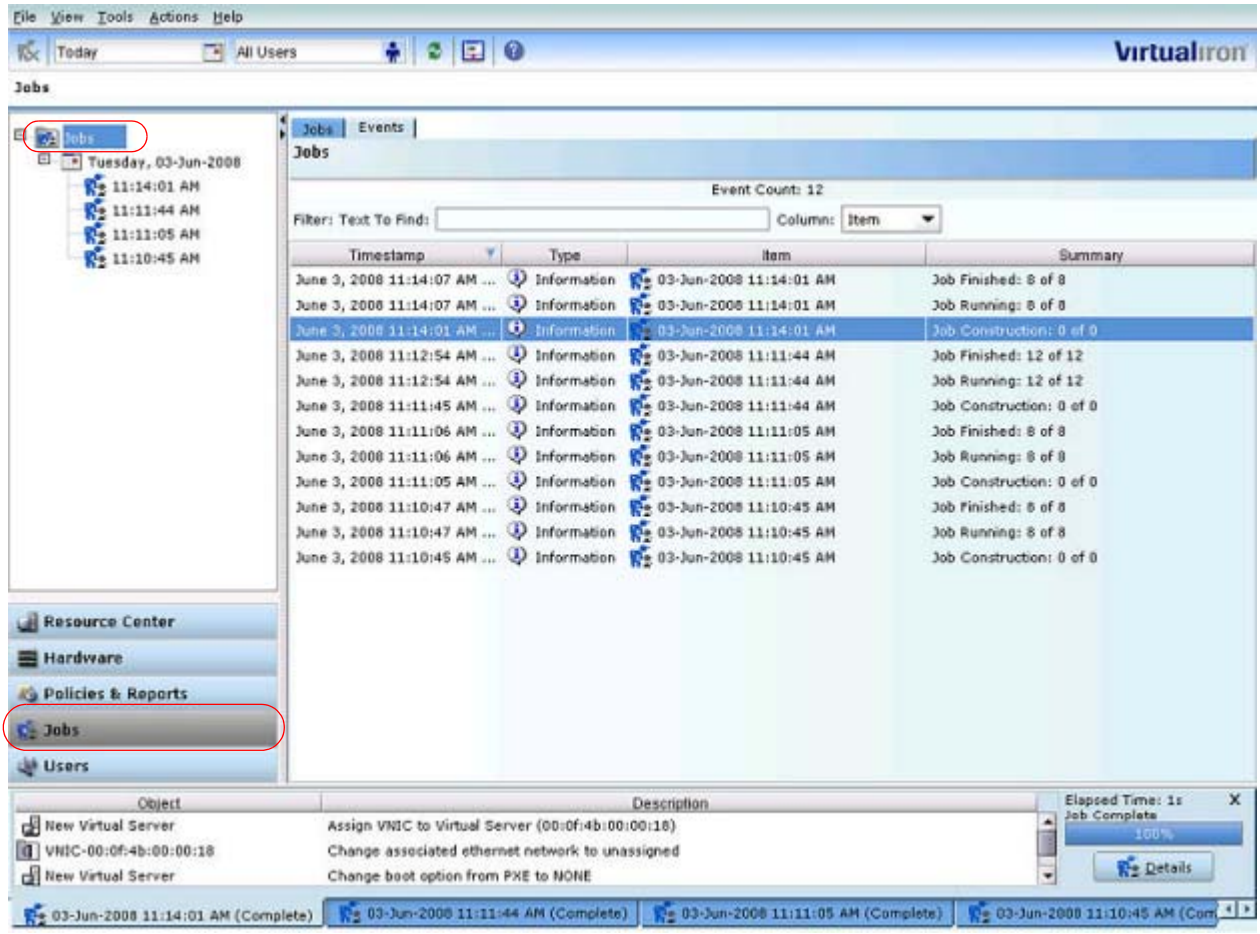
Jobs

Click **Jobs** in the Application toolbar for information on current and past tasks that have been completed in the environment. A job is a set of one or more operations made within the environment that have been entered to the Virtual Iron® database. Examples of operations include:

- Adding or deleting a user
- Adding, renaming, or deleting a VDC or VS
- Reconfiguring a VS (for example, increasing or decreasing allocated memory, adding processors)
- Discovering physical resources
- Adding, changing, or deleting policies

A sample of the Jobs view is shown in Figure 25.

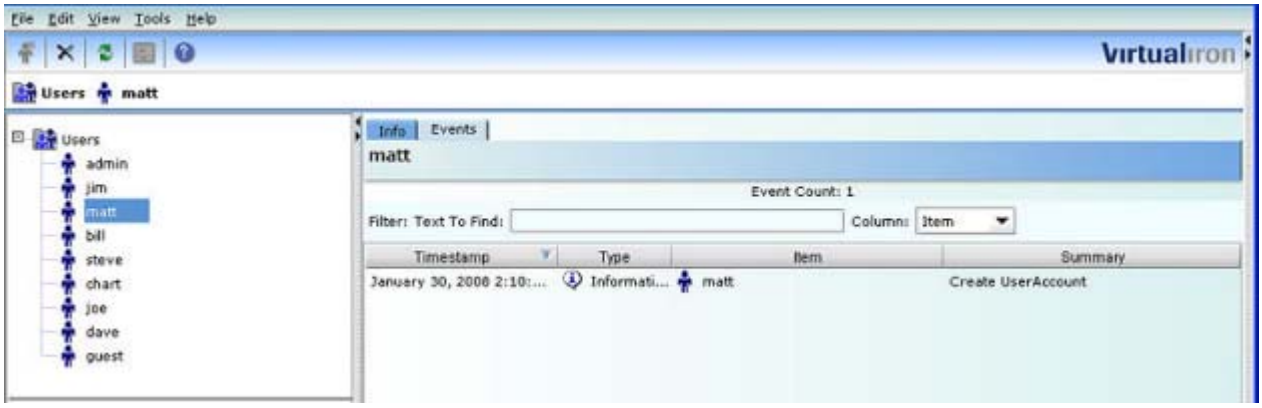
Figure 25. Jobs View



Users

Click the **Users** button in the Application toolbar to create and manage Virtual Iron® user accounts. Each user account has a unique name and password.

Figure 26. Users, Events View



USING THE NAVIGATION TREE

The navigation tree shows the relationship between managed objects within the virtualization environment. These objects are both physical and virtual, and include managed nodes (and node components), virtual data centers, and virtual servers created with the software.

The content of the navigation tree changes, depending on the button you click in the Application toolbar.

A sample of the navigation tree for **Resource Center** is shown in Figure 27. This view shows the relationships between Virtual Data Centers (**VDC**), managed nodes, and the virtual servers (**VS**) hosted by those nodes. In this example, **VDC** *Finance East* contains nodes, named *Dell 440*, *Dell 380*, *Dell 430*, and *Supermicro*.

Figure 27. Navigation Tree, Resource Center View

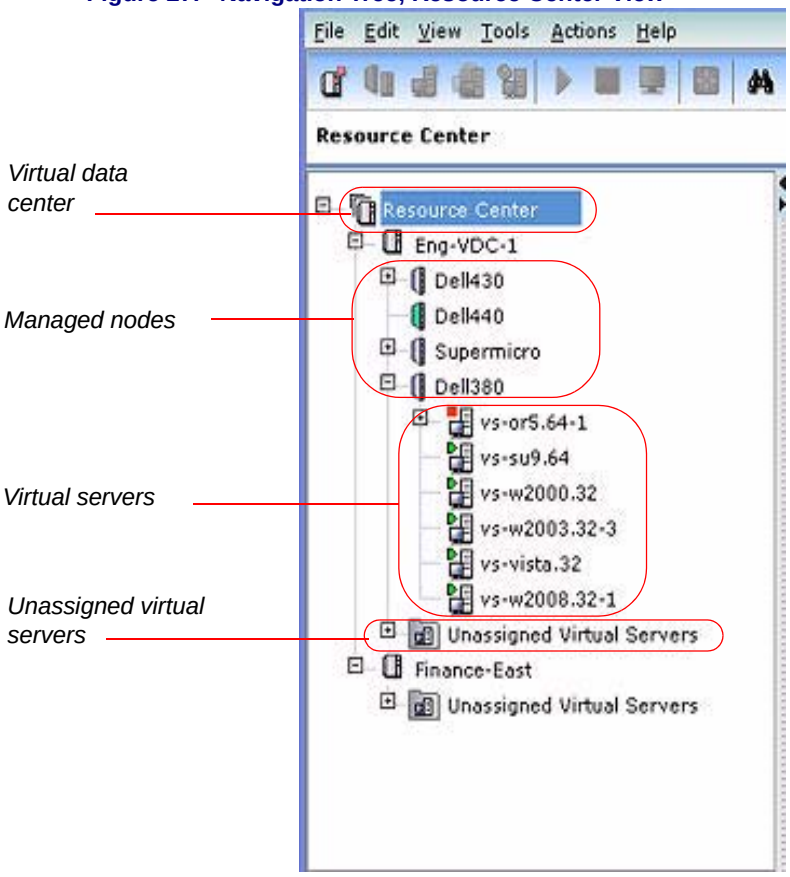
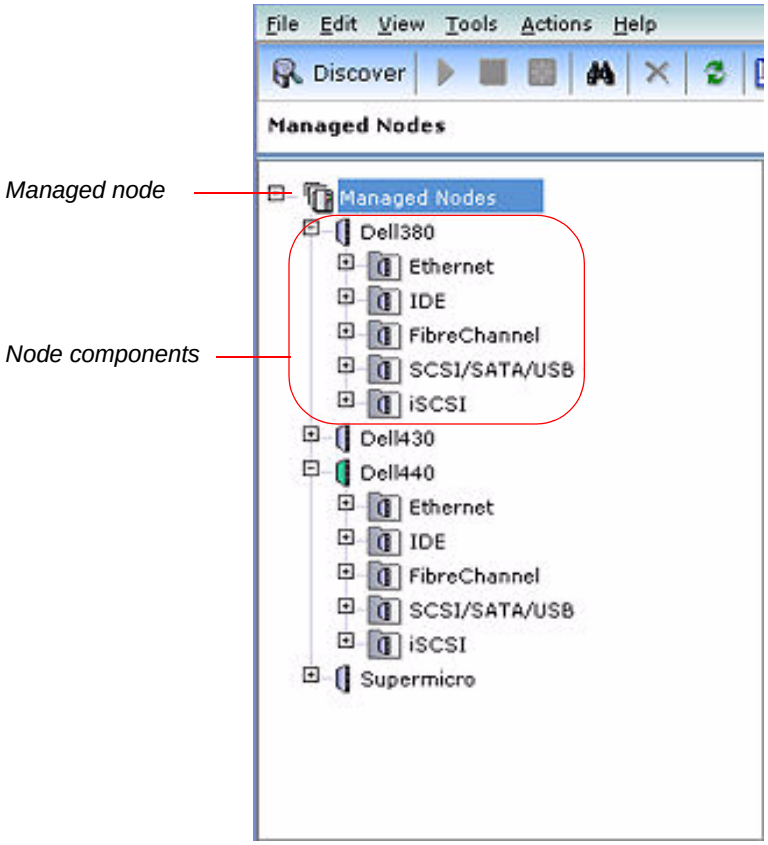


Figure 28 shows a sample navigation tree as it might appear in the **Hardware** view. This view exposes the components of each managed node.

Figure 28. Navigation Tree, Hardware View



USING THE ACTION TOOLBAR

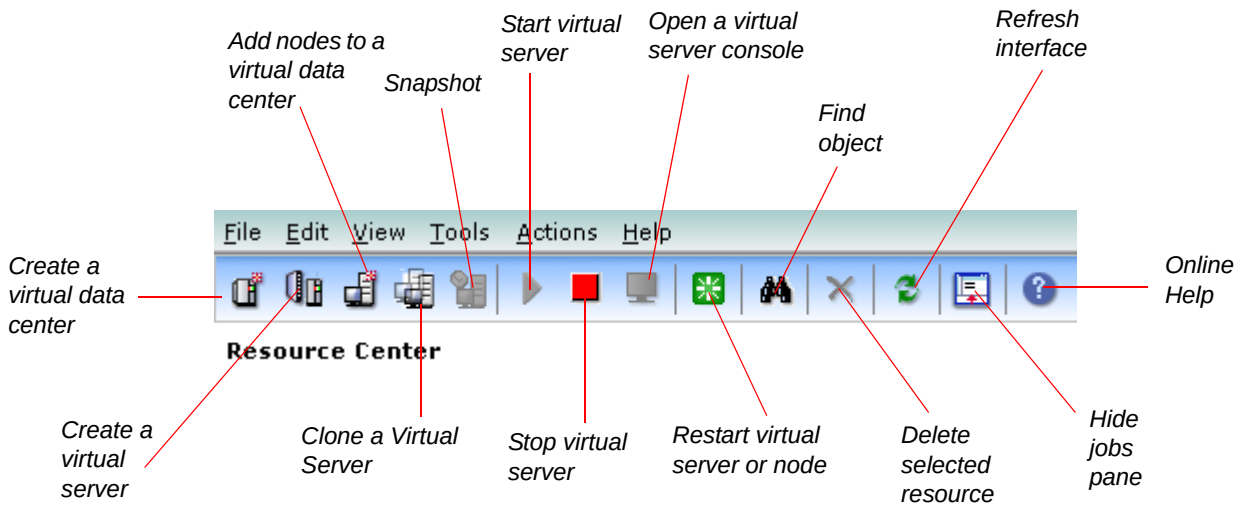
The Action Toolbar is positioned just below the pull-down menus. The icons in the Action Toolbar are arranged to support the work-flow required to the perform tasks associated with a particular application.

The pull-down menus and Action Toolbar are used together to perform specific actions in the virtualization environment. Depending on the operation, the options in the **Actions** menu and the buttons in Action toolbar change. For example, if you select **Resource Center** from **View** menu or **Application Shortcut**s, the Action Toolbar appears as shown in Figure 29. In this case, you would click the buttons in the toolbar to create objects in the virtualization environment:

- Create a virtual data center
- Add a node to a virtual data center
- Create a virtual server
- Clone a virtual server
- Get a snapshot of a virtual server
- Start a virtual server
- Create a virtual server console
- Find an object in the environment

See Figure 29.

Figure 29. Action Toolbar Icons, Resource Center View



ABOUT THE JOBS FRAMEWORK

VI-Center uses a Job operations framework that supports a flexible approach to the reconfiguration of physical and virtual objects.

Managing in a Multi-User Environment

VI-Center is designed for use in an environment in which a number of users may have access to the same objects. VI-Center maintains an accurate and consistent view of the virtualization environment while users perform separate and simultaneous jobs.

Each configuration change is a *job*—a transaction performed by a single user. The steps that follow describe how resources are locked and released at the start and conclusion of each job.

WHAT'S IN A JOB?

A job is a configuration change that affects one or more physical or virtual objects. Examples of user operations that can be included in a job are:

- Renaming a virtual data center or other object
- Adding or deleting a virtual data center
- Adding VNICs to a virtual server
- Moving a Virtual Server from one VDC to another
- Deleting a virtual server
- Changing the minimum and maximum values for a virtual server's memory and/or CPUs

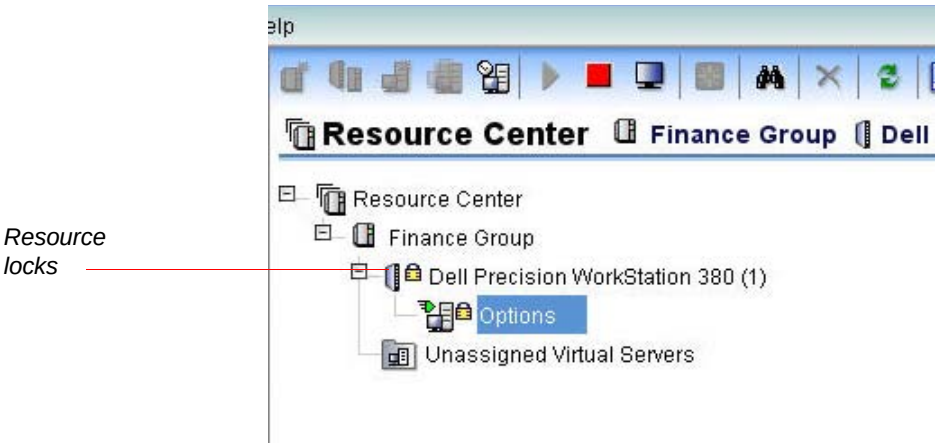
Jobs and Resource Locking

A single job can contain one or many individual operations. When a job is in progress, a yellow lock appears to the left of the resources included in the job.

Objects involved in a job are locked to all other users in the Virtualization environment until the job is completed or cancelled. Only a user with the same permission level on the object can unlock it. This assures that a consistent and accurate view is maintained for all users. See Figure 30.

The state of locked objects cannot be known until the locks are cleared. The state of the virtualization environment is always accurately reflected by the state of objects that are *not* locked.

Figure 30. Management UI, Showing Resource Locks



LOCKS AND MULTIPLE USER

A number of different users may perform jobs simultaneously, provided they are performed on different objects. For example, suppose User A has created *Finance-One* virtual data center and begins a job by moving nodes into another virtual data center. At the same time, User B modifies the resources of *Commodities* virtual data center. Assuming each user is working at the VI-Center™ UI (rather than via an API), each would have a separate job pane for his jobs, and would see the other's objects (as well as his own) as locked. The objects remain locked until the jobs are completed.

Prior to completing a job, a lock can be cleared in two ways:

- By logging out the user who initiated the lock. This action can be performed by the user, or by the virtualization environment administrator.
- By direct action of the virtualization environment administrator.

As a job completes, its progress is shown in the Jobs progress pane. All locks are cleared when a job completes.

JOB FAILURE AND ROLLBACK

Job operations are validated by the VI-Center as they are added to the Job tab. *The failure of any operation cancels the entire job and all other operations it specifies.* The state of the virtualization environment is rolled back to what it had been prior to the start of the job. All locks in the operation are released.

JOBS AND EVENTS

When a job operation fails, one or more events may be generated and displayed on the VI-Center™ UI. Events are flagged with yellow icons in the navigation tree. See Job Failure and Rollback.

To get information on failed events, click **Events** in the application toolbar. This displays the VI-Center™ event log.

JOB STATES

While a Job is in progress, the job tab can have any of the states defined in Table 1.

Table 1. Jobs Tab States

	Meaning
In Progress	A Job is running.
Complete	The Job has completed.
Failed	The Job has Failed. The virtualization environment has been rolled-back to its previous state and all locks have been released.
Aborting	The Job has been Aborted via console Abort command. The virtualization environment has been rolled-back to its previous state and all locks have been released.

PERFORMING JOB OPERATIONS

The sections that follow explain how to perform job operations within the virtualization environment™.

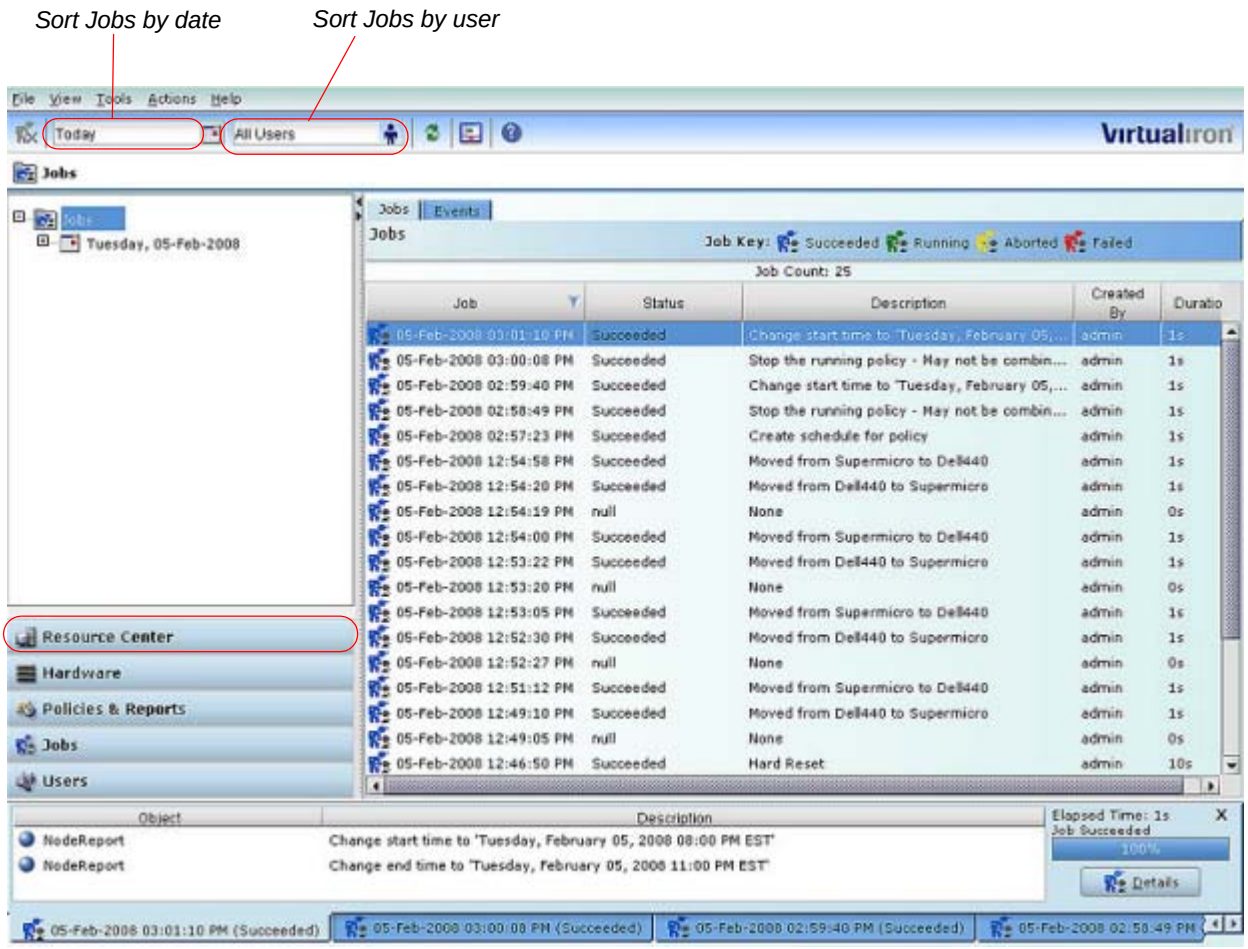
- About the Jobs View
- Starting a Job
- Aborting Jobs
- Determining the Cause of Job Failure
- Closing Job Tabs

About the Jobs View

The Jobs view provides comprehensive information on all completed, queued (pending), and in-progress jobs in the virtualization environment. The information is compiled in a time-stamped list. Jobs can be sorted and viewed by date or by user.

The jobs view is primarily used to get a global view on jobs, to evaluate information on jobs completed or aborted in the past, or for Administrative users, to cancel a job in progress. Figure 31 shows the jobs view.

Figure 31. Jobs View



Starting a Job

A job begins when you make any change within the virtualization environment. Each change you make appears in the Job Operations tab as a discrete operation. Job operations can be comparatively minor actions, such as renaming a virtual server. Operations may also have a wider scope, such as the creation of a new virtual data center or virtual server, or the movement of a node from one virtual data center to another.

As an example, these actions include:

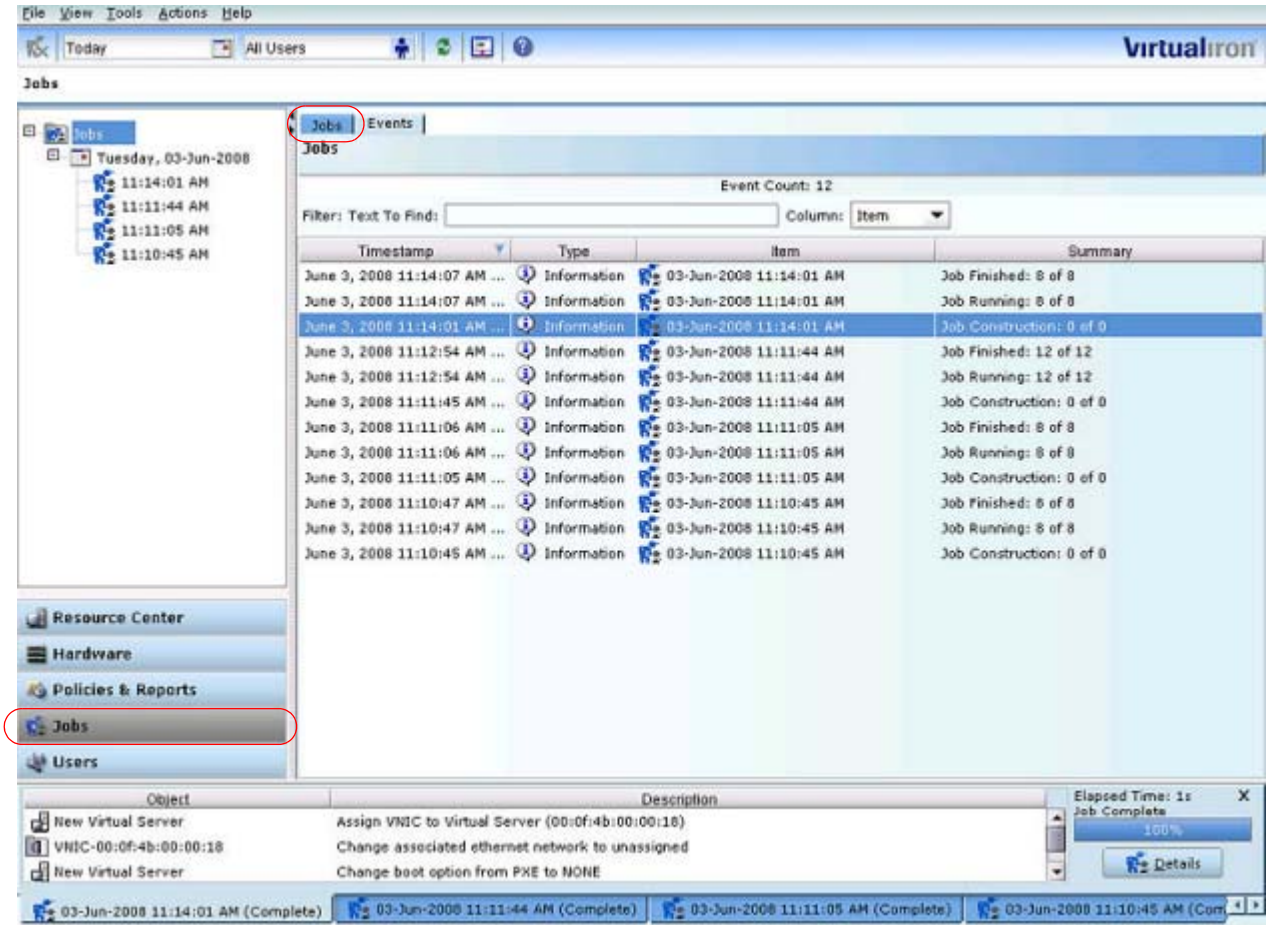
- Creating virtual data centers
- Creating and renaming virtual servers
- Starting or stopping virtual servers
- Changing virtual server processor or memory settings, or boot parameters

Performing any of these actions changes the configuration of the virtualization environment. This starts a *Job*, and opens a Job Operations tab at the bottom

of the management pane to show the job's progress. See Figure 32.

Note that if you click Details, the Jobs view shown in Figure 32 appears.

Figure 32. Job Operations Tab Containing an Operations Queue



Note that the nature of each operation is captured in the Description field. The Object field shows the object under management within a numbered operation. These objects are locked until the job completes, or the operation itself is cancelled. Objects are unlocked when a job completes or when a job is aborted. Until an object is unlocked, it cannot be managed by any other user in the virtualization environment.

Aborting Jobs

Before a job completes, the **Abort** button appears below the Job Progress status bar. If you want to cancel a job before it is completed, the VI-Center™ displays a warning message. Click **Yes** to continue with the Abort operation, or **No** to allow the job to run to completion.

If you abort a job, all operations queued in Job Progress roll back to the pre-job state. Note that some job operations such as renaming an object, complete quickly. Others, such as adjusting the memory used by a virtual server, take longer.

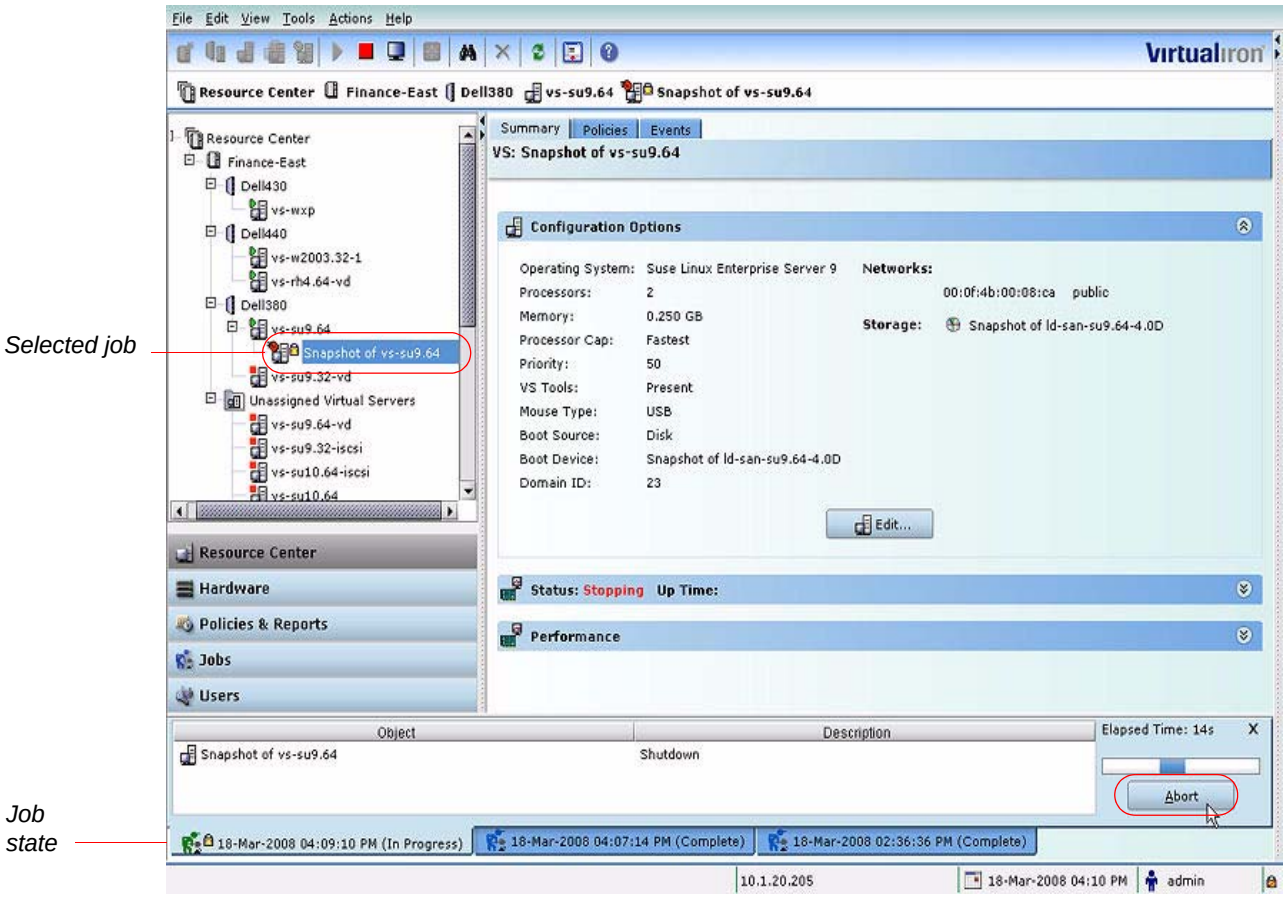
ABORTING A JOB IN THE JOBS VIEW

If a job is running or fails to complete, an Admin user can abort the job from the Jobs view.

Locate the job in the navigation tree.

Select the job and click **Abort**.

Figure 33. Aborting an Under Construction Job



Determining the Cause of Job Failure

If a job succeeds, all the operations associated with it are implemented in the virtualization environment. A Job Succeeded message appears in the Job Progress area.

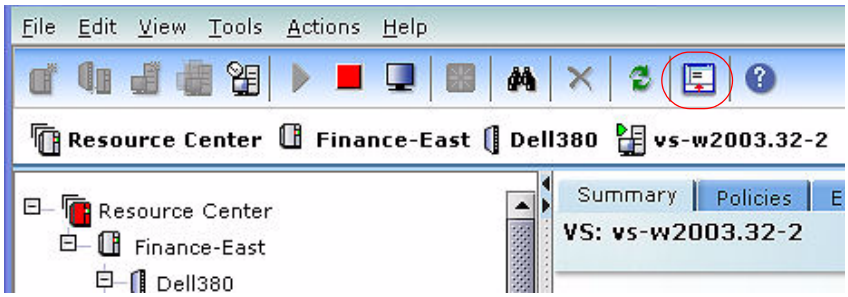
If the job fails, the state of the virtualization environment returns to its pre-job state. A job failure presents **Error** and **Details** buttons on the tab. Click **Details** to see high-level information on all operations in the job. Click **Error** to open a pop-up containing information on the specific operation that failed within the Job.

Closing Job Tabs

When you create a job, the Job Progress area remains on-screen. To clear it, press the F5 key, or click the Job control icon shown in Figure 34.

Figure 34. Job Control Icon

Hide or Show Jobs



4

CONFIGURING NETWORKS

MAPPING PHYSICAL PORTS TO LOGICAL NETWORKS

Before configuring networks, you will map all available ports to the set of logical Ethernet networks created within VI-Center. This involves the following tasks:

- Defining a name or alias for each network. The name should be a recognizable name that has to do with the network's use.
- Logically connecting all physical NIC ports on each node in the Resource Center to the networks you want them to use.

Defining Networks in a Virtualized Environment

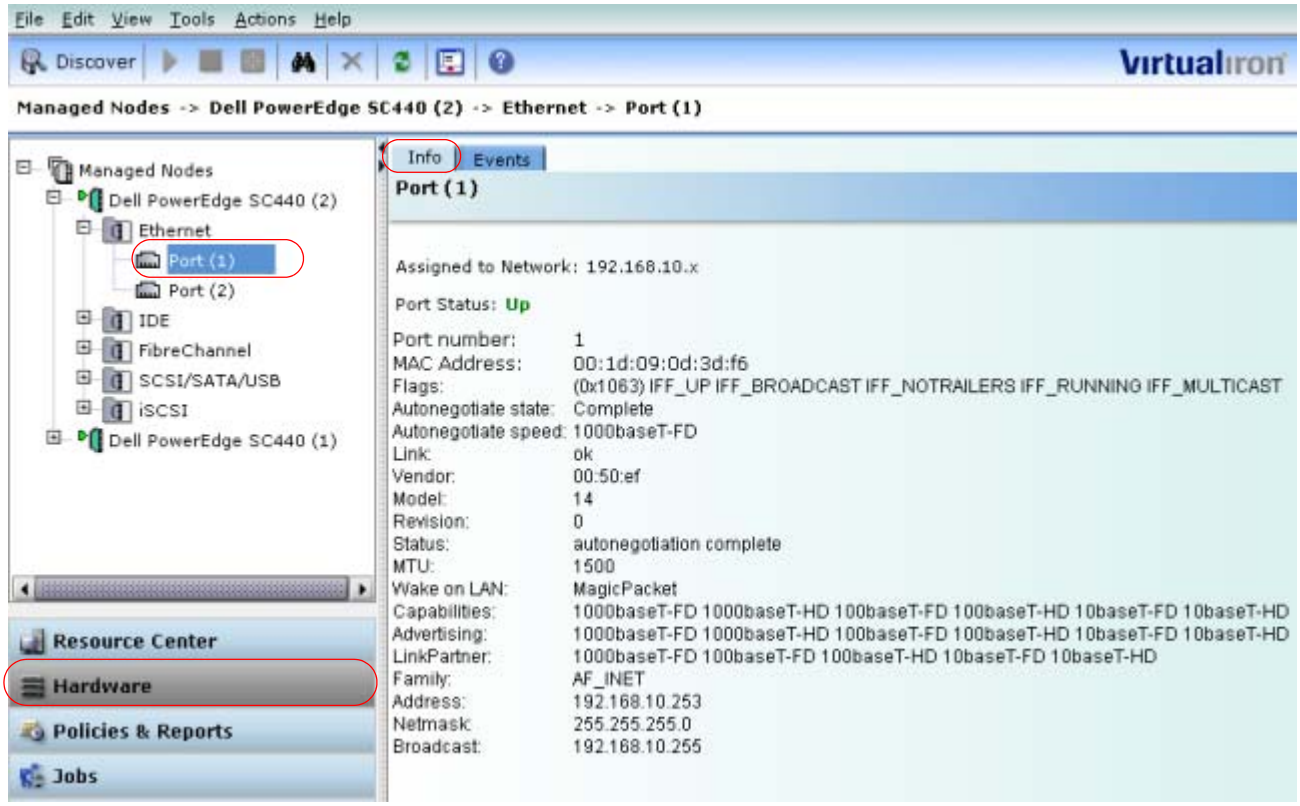
When nodes boot in the Virtual Iron® framework, information about the components of each node is displayed on VI-Center. Each managed node is shown on the VI-Center user interface, along with its Ethernet cards and ports.

Step 1. Connect a port to a network: Plug a managed node into a physical network you want it to use.

Step 2. Click **Hardware** in **Applications Shortcuts**, or select **Hardware** from the **View** menu.

Step 3. In VI-Center, expand the navigation tree: Click on a node until you see **Port (1) to (x)** listed. Click the listed ports to check their status and specifications. See Figure 35.

Figure 35. Port Information Example

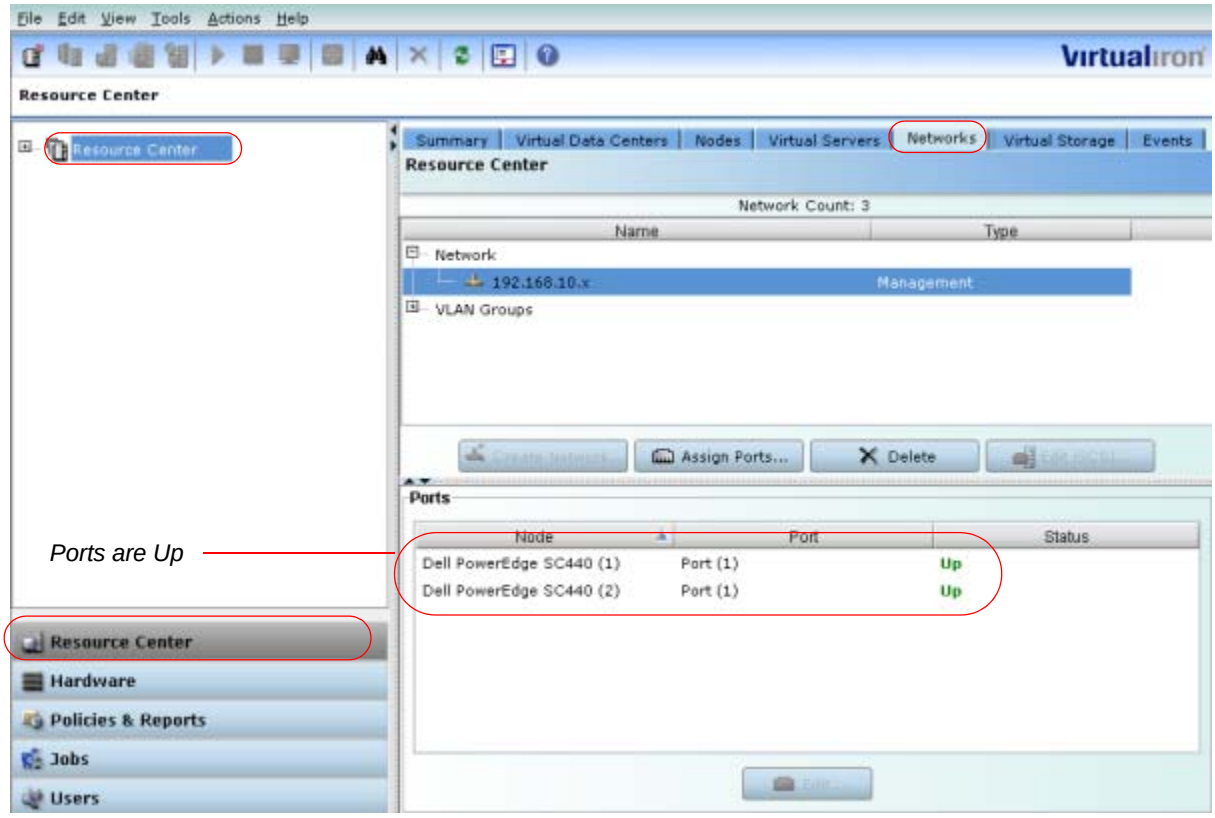


Step 4. Click the **Resource Center** application shortcut.

Step 5. In the navigation tree, click the node and select the **Networks** tab.

Step 6. Select a network in the **Network** tree diagram. The port you connected appears in the bottom of the Networks window with a status of ***Up***, as shown in Figure 36.

Figure 36. Ethernet card and port information



CONFIGURING NETWORKS

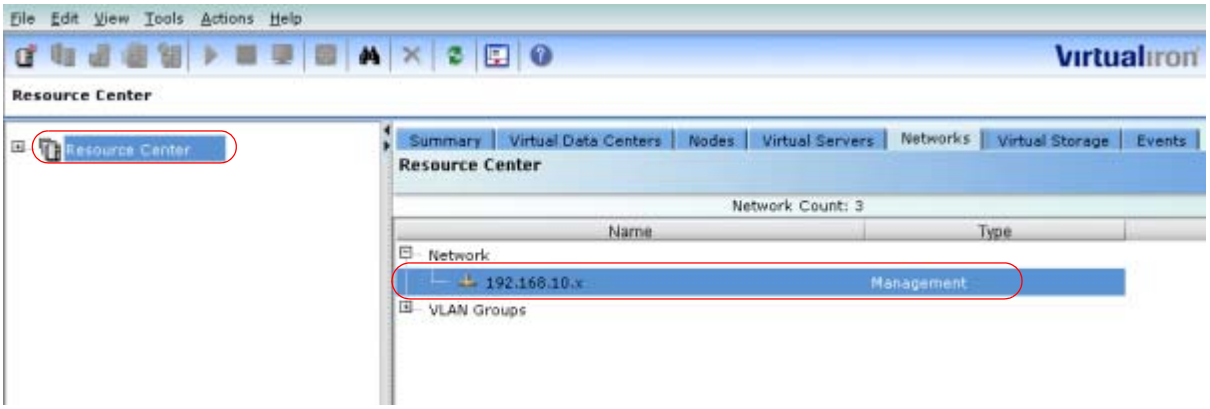
This section describes how to configure Ethernet and iSCSI networks, and how to configure Ethernet ports to support multiple VLANs. It contains the following procedures.

- Configuring Ethernet Networks
- Configuring iSCSI Connectivity
- Configuring VLANs
- Creating a Failover Network

Default Management Network, Extended Enterprise Edition

Virtual Iron Extended Enterprise Edition (XEE) requires that you manage system nodes over a dedicated Ethernet network instead of a public network. The dedicated management network is detected and displayed for you. By default, the name of this network is its Class C IP address. The type of this network is **Management.** See example in Figure 37**.**

Figure 37. Initial Network, Configuration - Extended Enterprise Edition



Configuring Ethernet Networks

To configure Ethernet networks, proceed as follows.

Step 1. Click **Resource Center** in **Applications Shortcuts**.

Step 2. Select **Resource Center** in the navigation tree, and the **Networks** tab.

Step 3. Click the **Create Network** button as shown in Figure 38.

Step 4. In the Create Network Wizard window, enter the network name and click **Next**.

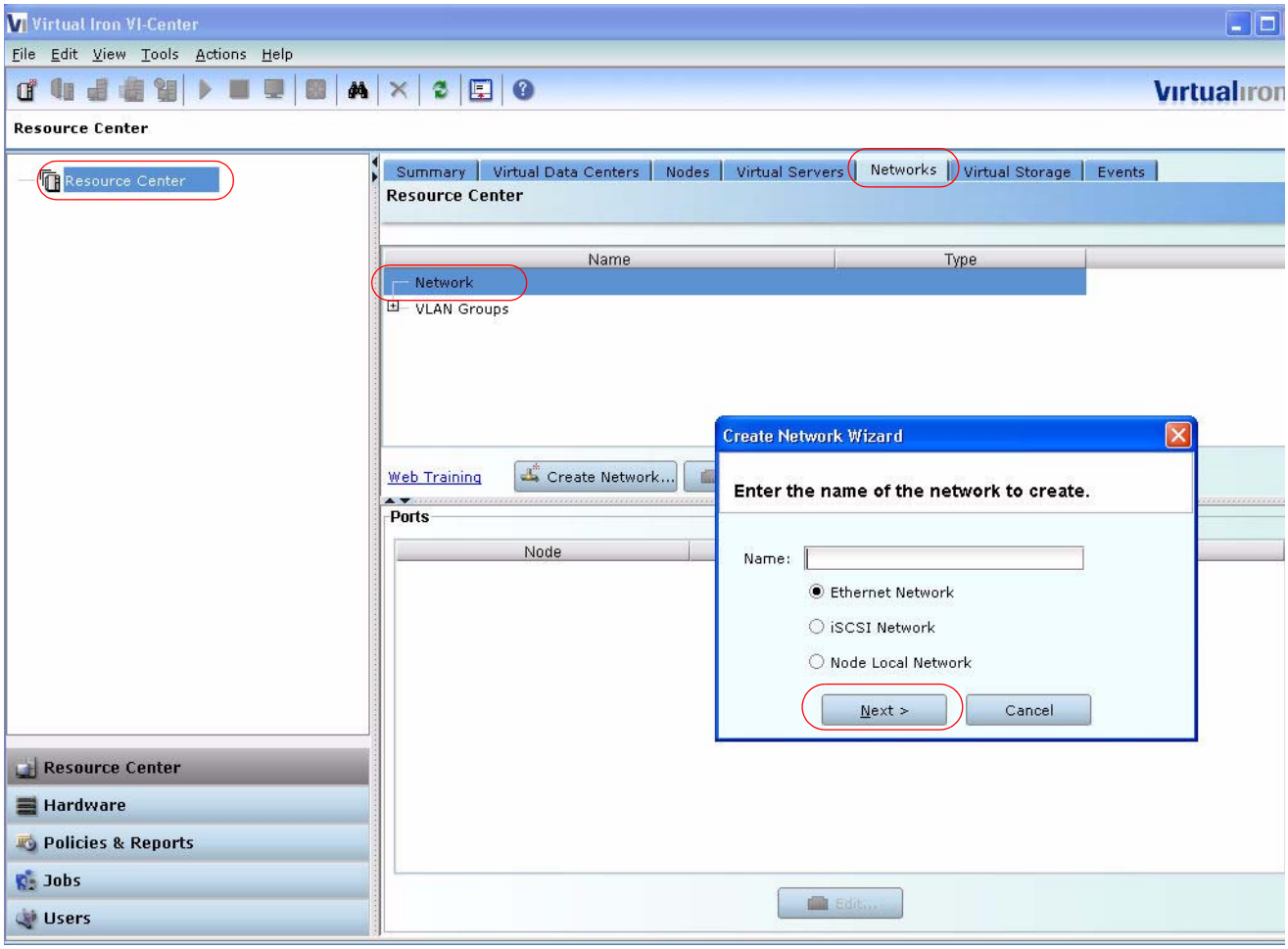
The symbolic names you choose should relate to the uses of the network. This step adds these logical names to the VI-Center database.

Step 5. Select one of the following:

- Ethernet Network
- iSCSI Network—If you select iSCSI Network, see Configuring iSCSI Connectivity for more information.
- Node Local Network—Allows Virtual Servers on a single node to communicate without using a NIC. See Node Local Networks.

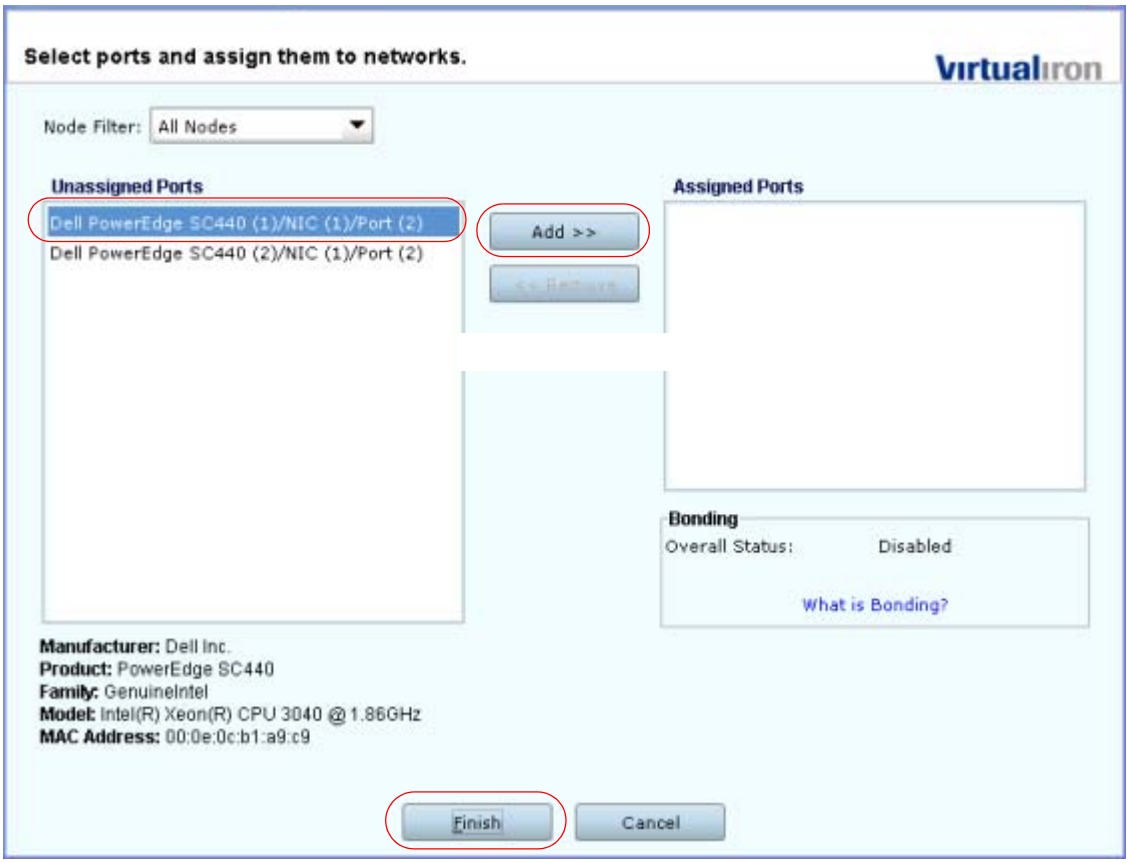
Step 6. Click **Next**.

Figure 38. Adding Ethernet Network Names



Step 7. VI-Center displays the window shown in Figure 39. Select the unassigned port and click **Add** to assign the node you just connected to the symbolic Ethernet name chosen for that network. Select the network name from the pull-down.

Figure 39. Associate a physical card/port with a symbolic network name

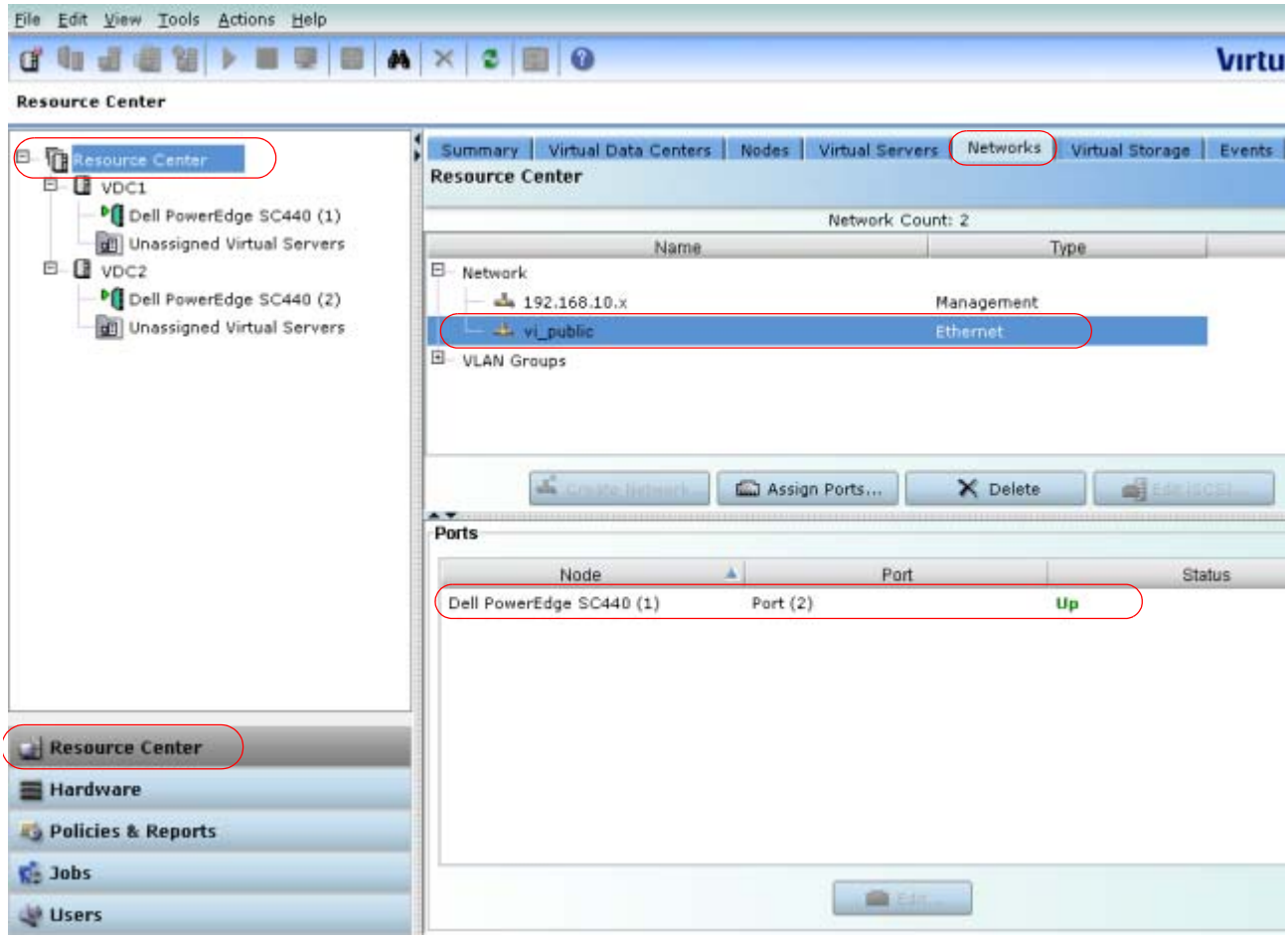


Step 8. Repeat this procedure for each card/port, until you have assigned each physical port to one of the symbolic names chosen for your public networks. Click **Finish**.

The Ethernet network you have created appears in the Network tab (Figure 40). Its type is Ethernet. Note that the port you have assigned to the network appears in the **Port** area.

To create a failover network, refer to Creating a Failover Network.

Figure 40. Configured Ethernet Network and Associated Port



Configuring iSCSI Connectivity

Internet SCSI (iSCSI) is an IP-based storage networking standard that allows connection to data storage facilities over local and wide area networks and the internet. Though it runs at lower bandwidth than Fibre Channel networks, iSCSI performs the same basic function as Fibre Channel. However, iSCSI has distinct advantages. Since it runs over Ethernet, it does not require an HBA or other dedicated FC device. You can have up to two iSCSI networks per node.

ISCSI CONFIGURATION GUIDELINES

Follow these guidelines when configuring switches from iSCSI networks:

- Make sure that the iSCSI storage server is on the same subnet as the network you are connecting from.
- Do not mix iSCSI traffic with other LAN traffic. Use VLANs if necessary to isolate the iSCSI network on a switch.
- Use managed 1 GB switches.

- Set all target, initiator and inter-switch ports to 1 GB full duplex (auto-negotiation OFF/Disabled).
- Set flow control to ON on target, initiator, and inter-switch ports.
- When interconnecting switches, make sure you have sufficient bandwidth connections between switches. Use fiber interconnections or Link Aggregated Groups to provide adequate bandwidth.
- In the case of Cisco switches, enable the spanning-Tree PortFast option, for other vendors a similar option may be available, if not disabling spanning-tree is recommended.

Note: Virtual Iron® recommends that your iSCSI networks are on a dedicated network that is not accessible to virtual servers. This assures the security of the storage traffic and better performance.

Virtual Iron® supports iSCSI connections between managed nodes and SAN resources.

CONFIGURING AN ISCSI NETWORK AND ADDING ISCSI PORTS

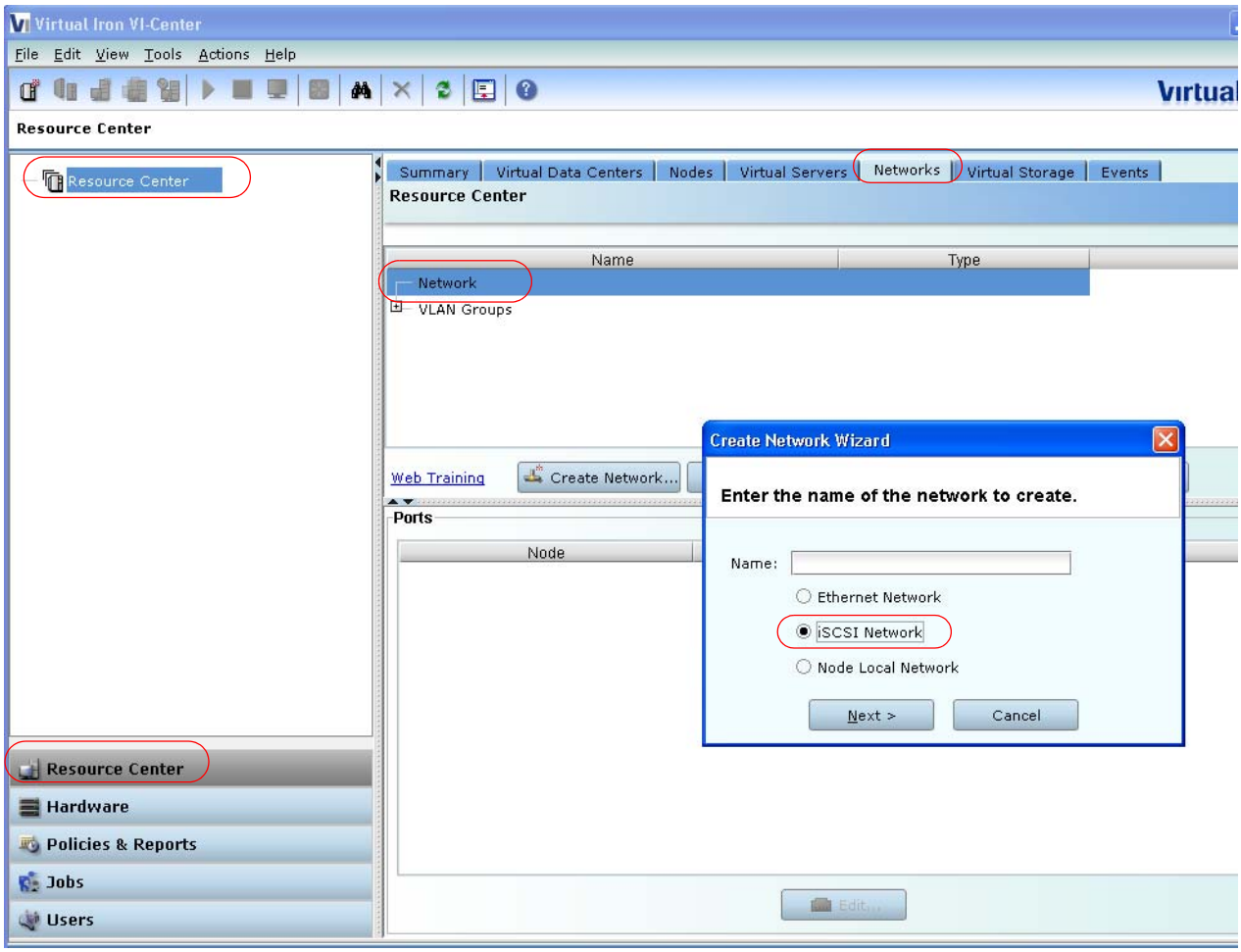
Step 1. Click **Resource Center** in **Applications Shortcuts**.

Step 2. Select **Resource Center** in the navigation tree, and the **Networks** tab.

Step 3. Click **Create Network** as shown in Figure 41.

Step 4. The Create Network Wizard appears. Enter a name for the network, check **iSCSI Network,** and click **Next>>**.

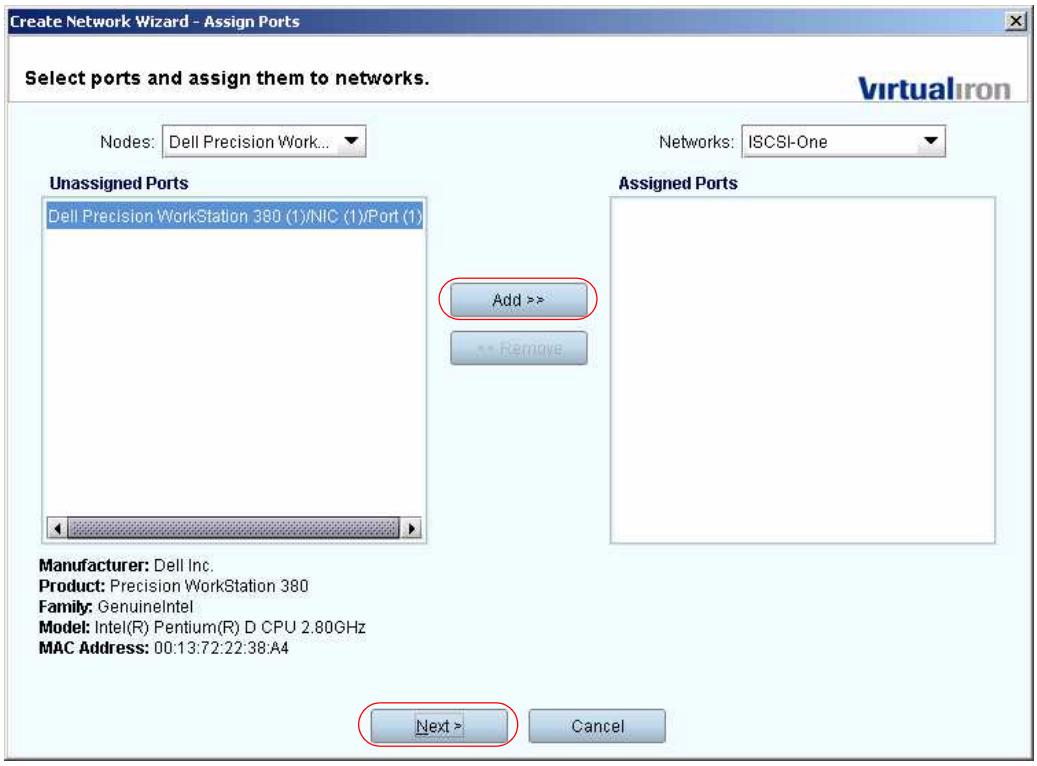
Figure 41. Configuring iSCSI Connections



Step 5. The **Create Network Wizard-Assign Ports** window shown in Figure 42 appears. Select a node and network from the pulldown menus.

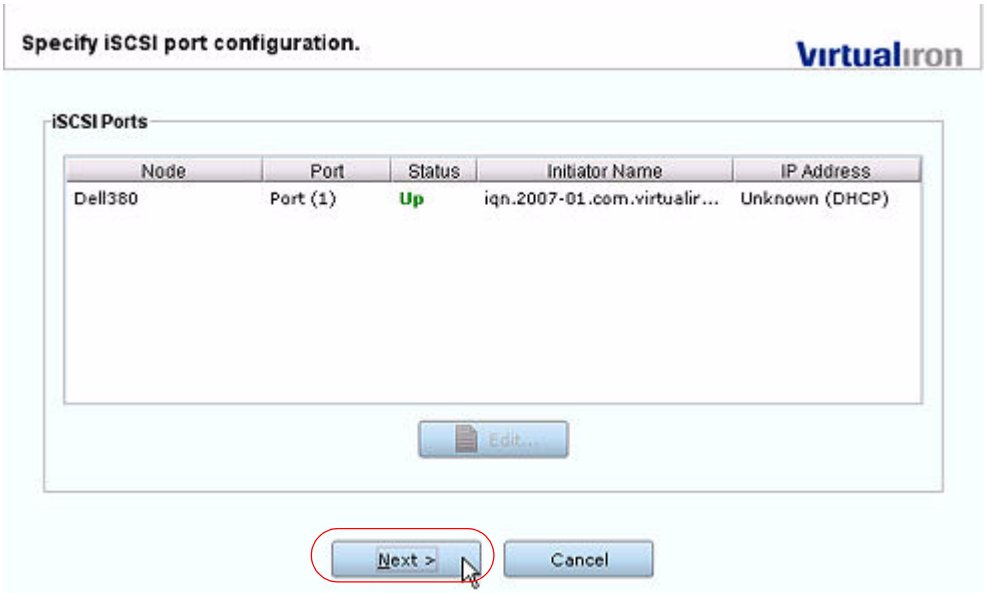
Step 6. To assign ports to the iSCSI connection, select a port in the **Unassigned Ports** pane and click **Add**. The port moves to the **Assigned Ports** pane on the right. Click **Next** when you have finished assigning ports.

Figure 42. Assigning Ports to iSCSI Connections



Step 7. In the iSCSI Port Configuration window, click **Next**.

Figure 43. Assigning Ports to iSCSI Connections



Step 8. in the iSCSI Servers window, select an MTU value. Note that 9000 represents Jumbo frames. Click **Add** and **Finish**.

Refer to Configuring and Managing Storage to complete iSCSI configuration.

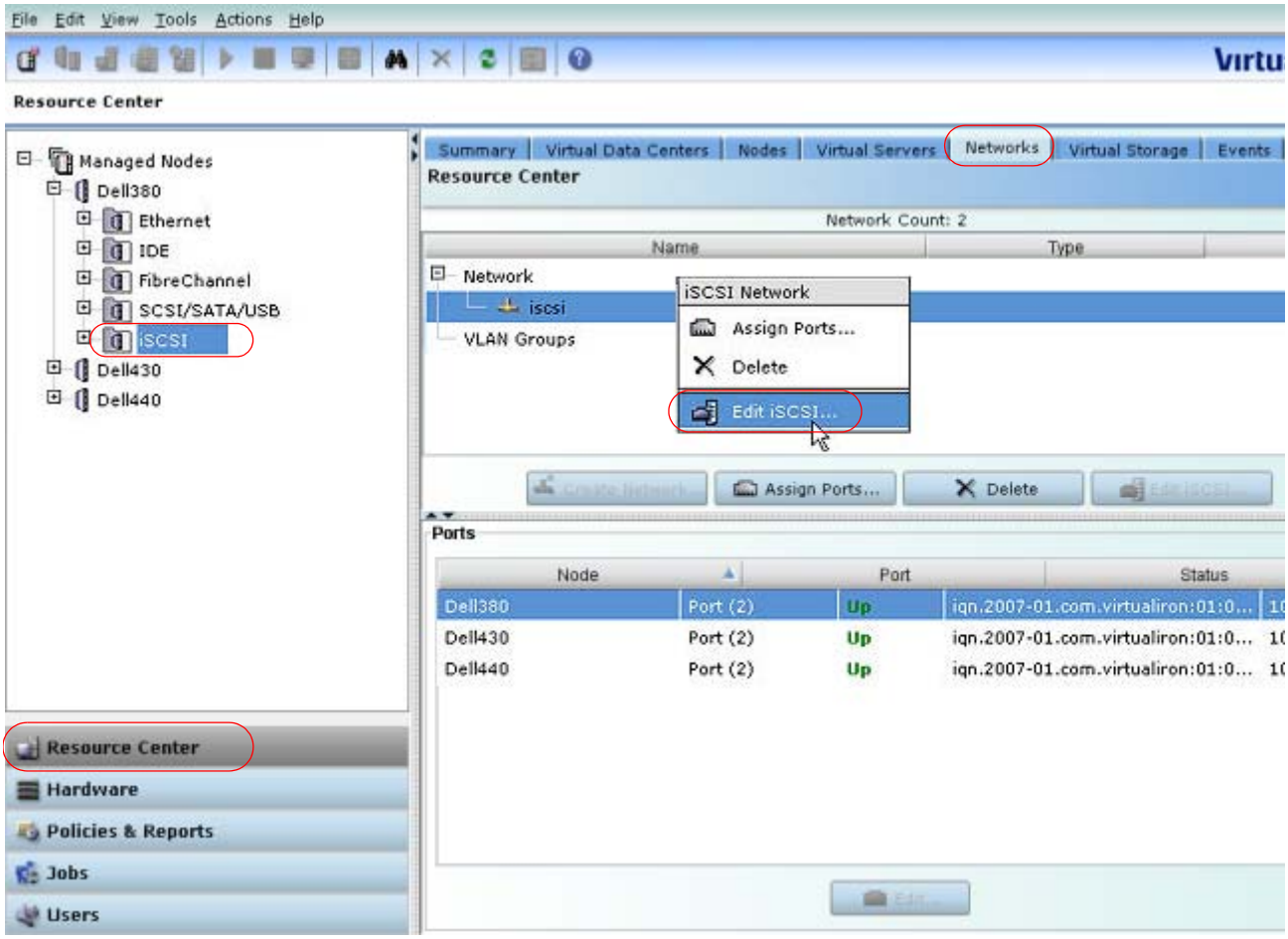
Editing iSCSI Port Configuration

Step 1. To change iSCSI port information, in the **Resource Center** view, select the iSCSI port from the navigation tree.

Step 2. Click the **Networks** tab and select the **iSCSI** icon. See Figure 44.

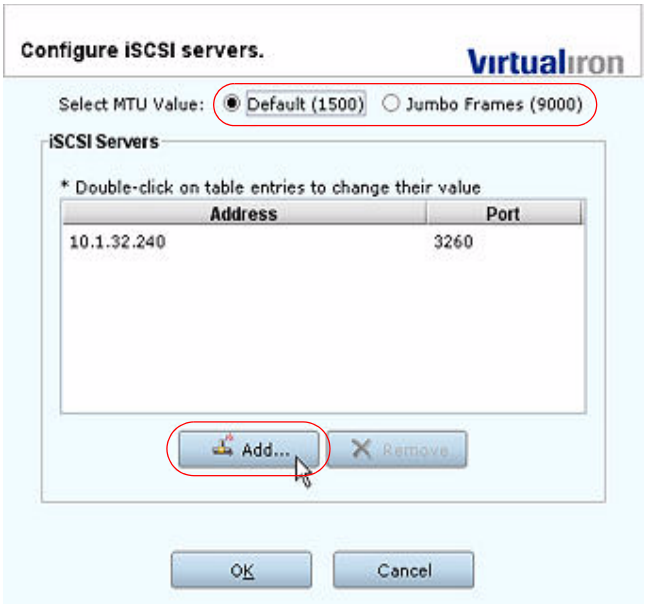
Step 3. Right click and select **Edit iSCSI**.

Figure 44. Editing iSCSI Port Information



Step 4. The **Edit iSCSI Servers** window appears as shown in Figure 45.

Figure 45. Adding iSCSI Port Information

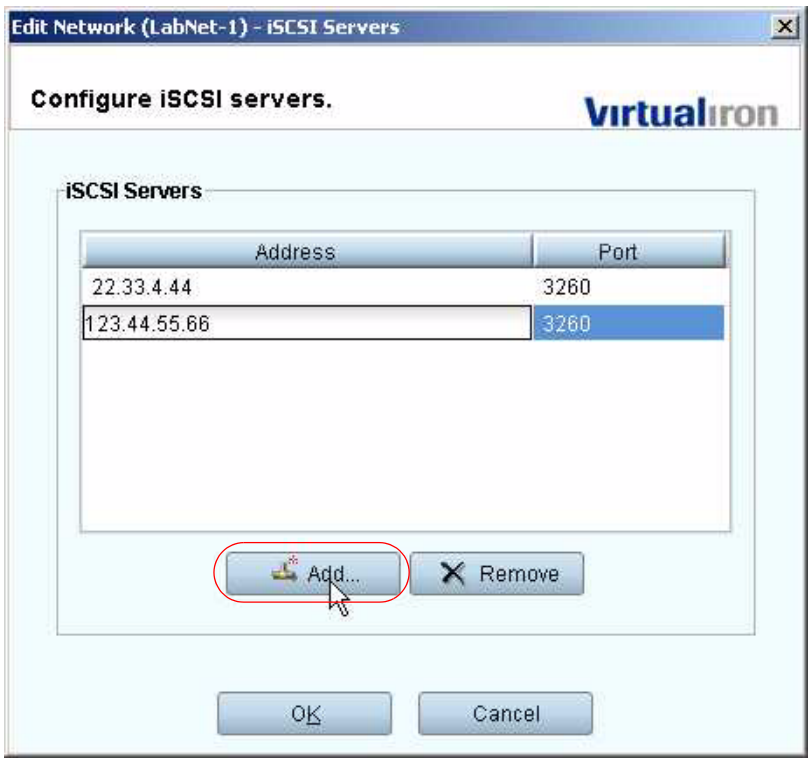


By default, DHCP is used to configure the IP address of the iSCSI port. An initiator name is provided by VI-Center. You can use this window to assign a new initiator name, and/or a static IP address and mask. To do so, click **Add**.

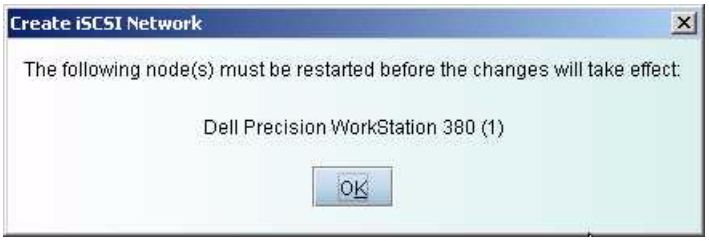
Step 5. Select an **MTU Value**. After making all changes, click **OK** to accept the changes and close the window.

Step 6. Use the window that appears next to add the IP addresses of the iSCSI servers reachable on this connection. See Figure 46. Add an alternative connection port for iSCSI servers as needed. Click **Add** to add a new connection, and key in the IP address. Click **OK** when finished.

Figure 46. Adding iSCSI Server Information



Step 7. The system displays the following message, indicating that you need to reboot the node that owns the iSCSI port you have configured:



In addition, this node is placed in a warning state, indicated by a yellow icon.

After rebooting the node, the iSCSI configuration is complete.

TO TEST ISCSI CONNECTIVITY

Step 1. To test iSCSI connectivity, in the **Resource Center** view, click the node in the navigation tree.

Step 2. Select the **Networks** tab.

Step 3. Select the iSCSI attribute and click the **Test Connectivity** button.

Configuring VLANs

Virtual Iron supports multiple Virtual LANs (VLANs) on the same port. Each VLAN is essentially an independent logical network operating with other VLANs over the same physical connection.

Configuring VLANs involves creating one or more VLAN Groups, each of which can house multiple VLANs. Each VLAN is assigned a distinct VLAN identification. The VLAN ID is used by an attached VLAN switch to segregate traffic among the different VLANs operating on the same link. Once a VLAN is configured, it functions exactly like a separate physical connection.

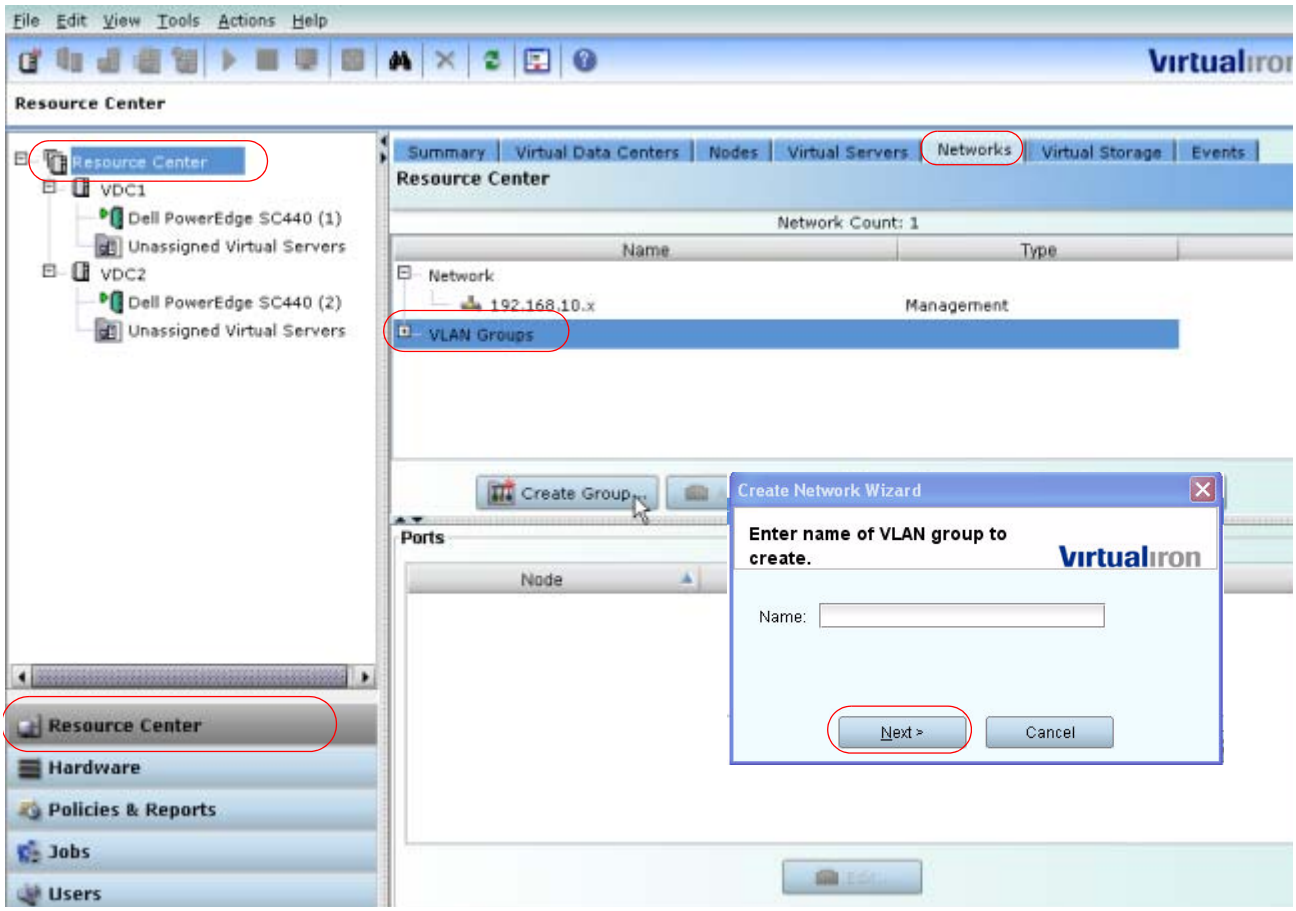
It is important to coordinate VLAN configuration with the administrator of attached VLAN switches, so that appropriate VLAN IDs are assigned to the VLANs you configure.

Step 1. In the **Resource Center** view, select the **Networks** tab.

Step 2. Select **VLAN Groups** in the navigation tree. Click **Create Group...** from the pop-up menu as shown in Figure 47.

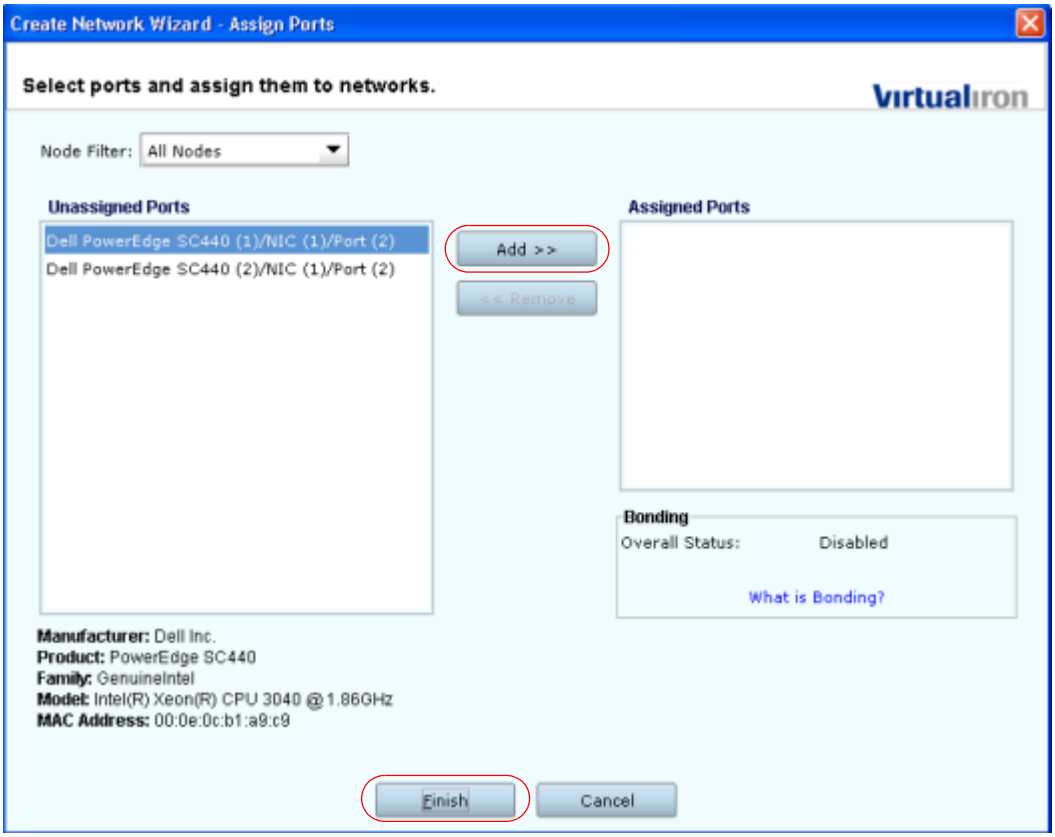
Step 3. Enter a name for the VLAN Group in the **Create Network Wizard** and click **Next>>**.

Figure 47. Configuring VLAN Groups



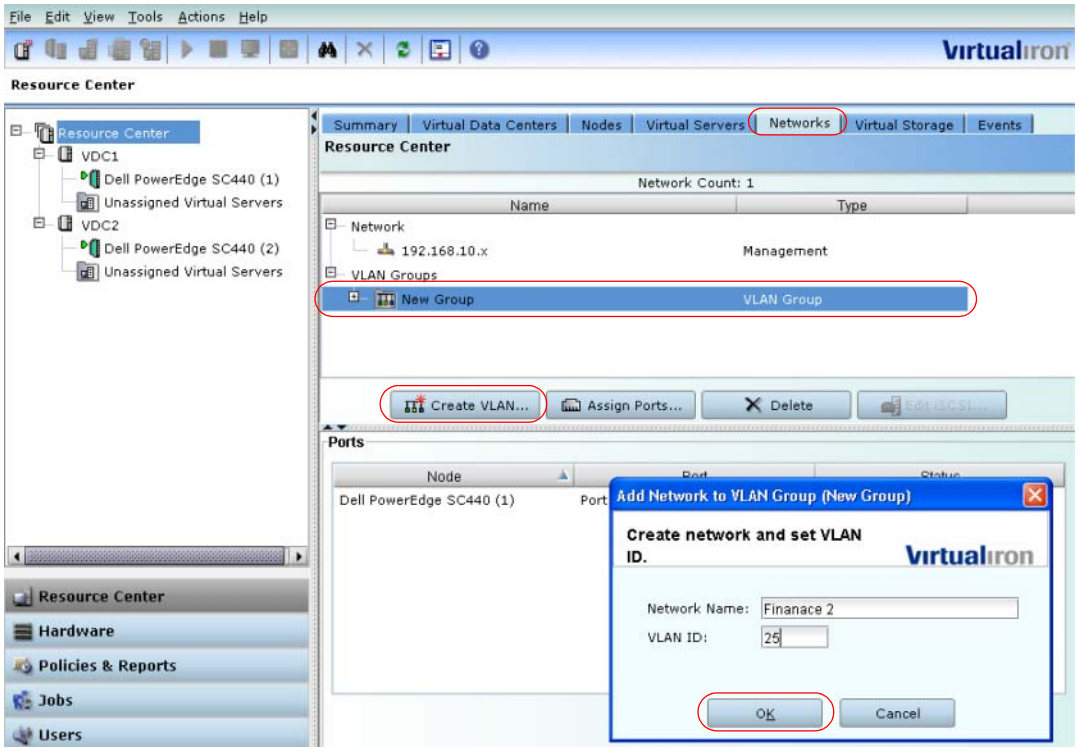
Step 4. The **Assign Ports** window shown in Figure 48 appears. To assign a port to the VLAN Group, select the port in the **Unassigned Ports** pane. Then click **Add>>**. The port moves to the **Assigned Ports** pane on the right. Click **Finish**.

Figure 48. Assigning Ports to a VLAN Group



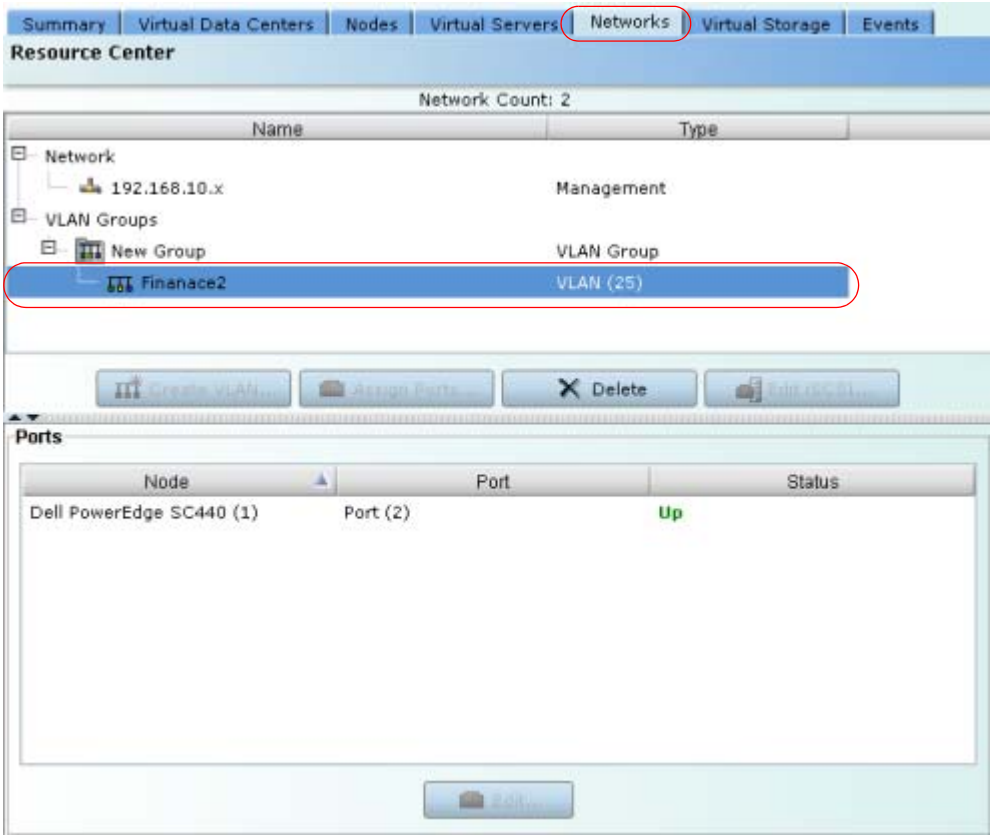
Step 5. In the **Managed Nodes** window, select the VLAN group you have created and choose **Create VLAN** from the pop-up window as shown in Figure 49. Add the name of the VLAN connection, and a VLAN ID. VLAN IDs must be in the range of 2 to 4095. Click **OK**.

Figure 49. Create VLAN



Step 6. The VLAN Group and VLAN you have created appear in the network window as shown in Figure 50. Repeat this process to add additional VLANs as required.

Figure 50. VLAN Created



Node Local Networks

A Node Local Network is an isolated host-only network. Virtual machines connected to this network cannot be migrated (because the network is only on the one host). You will also need to think about how to assign IP addresses ... either put a DHCP server on the network or assign static IP addresses. A reason you may want to use a node local network is to isolate virtual machines from external networks.

CREATING A FAILOVER NETWORK

To protect your network in the event of a failure, you can bond any two physical ports in the same node so that they represent a single logical interface. The two ports show the same hardware MAC address.

You can configure network failover bonds for:

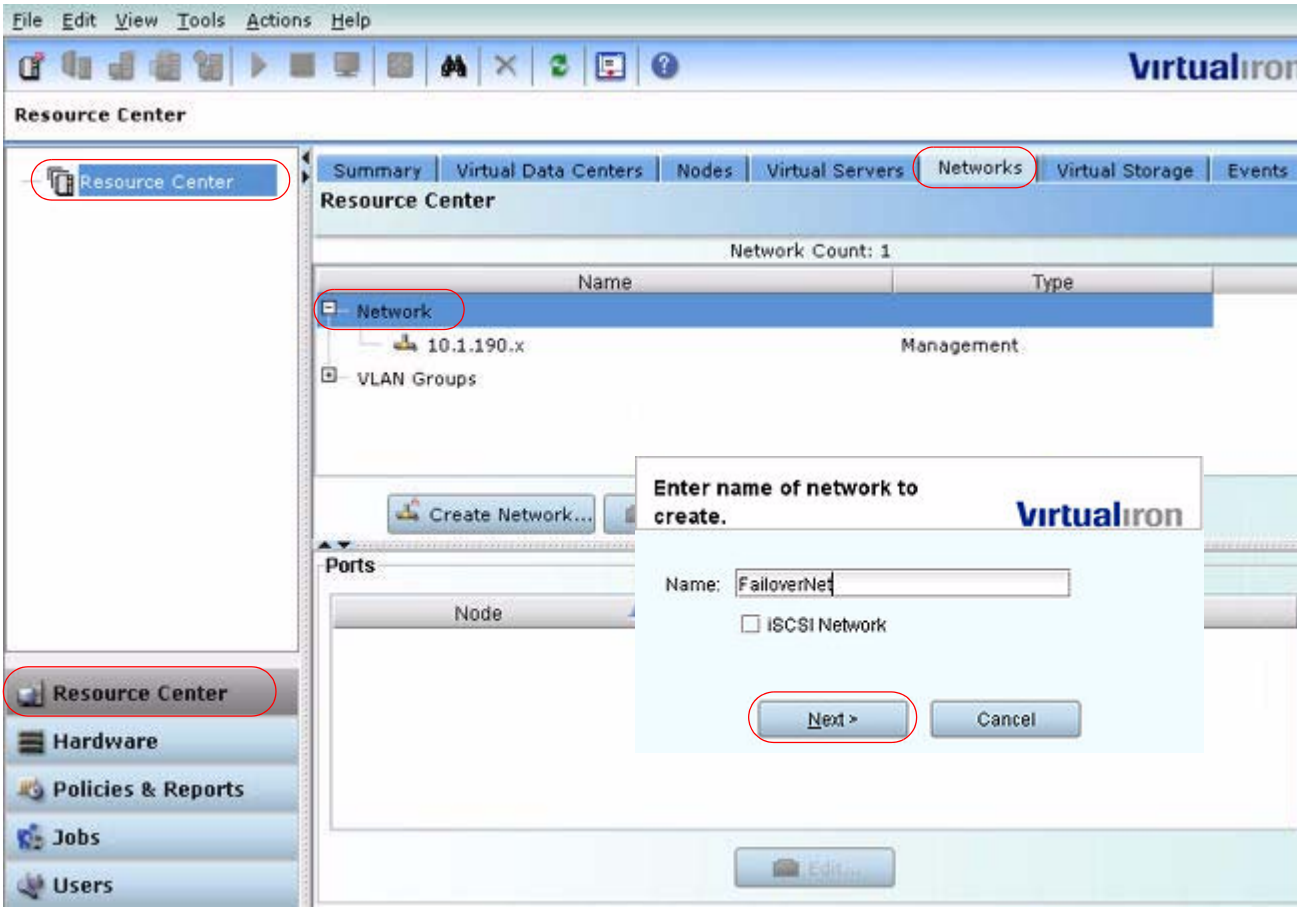
- Ethernet networks
- VLAN networks
- iSCSI Networks

Step 1. In the **Resource Center** view, select the **Networks** tab. See Figure

51.

Step 2. Click **Create Network**, or right-click and select **Create Network**.

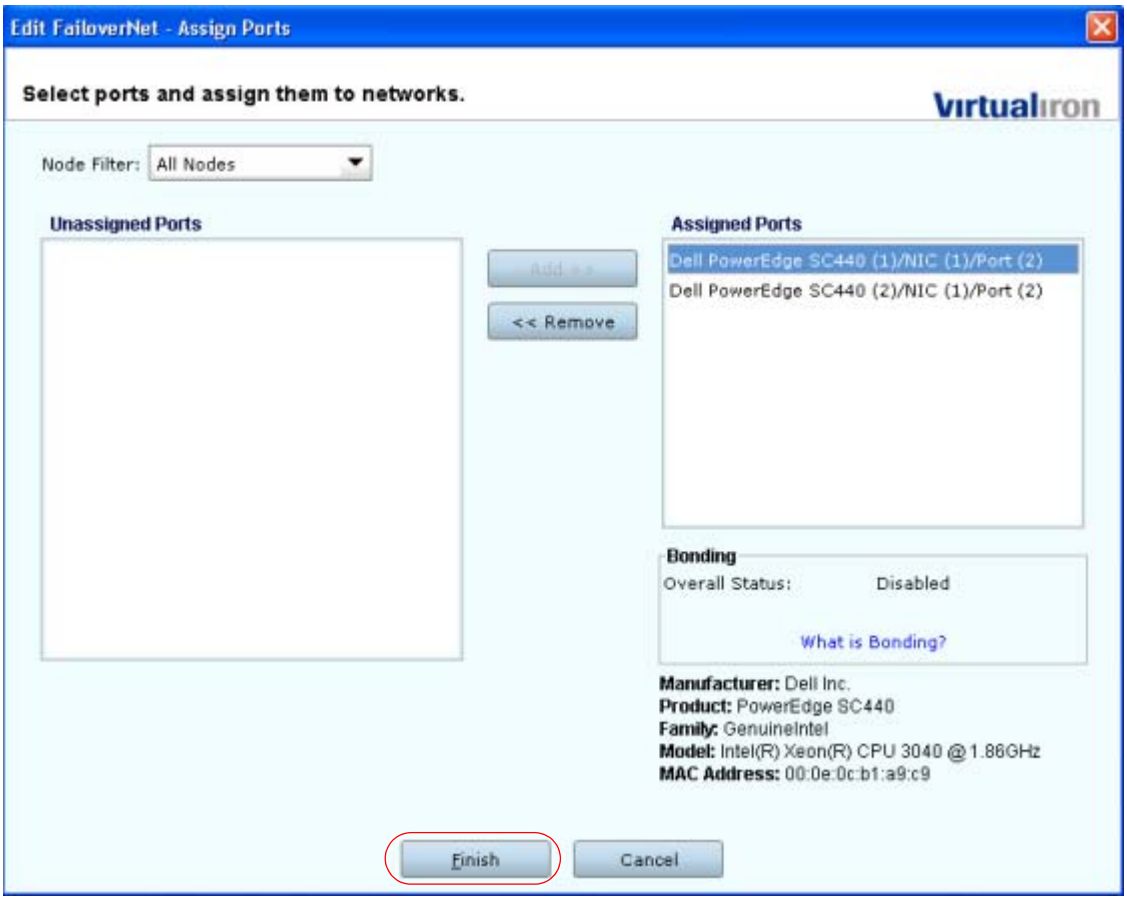
Figure 51. Create Network Selections



Step 3. In the pop-up window, enter a name for the failover network.

Step 4. Select the ports you want to bond for failover from the Unassigned Ports list. Click **Add**. Note that once you have assigned the ports, information related to the bonded ports appears at the bottom of the Assigned Ports list. See Figure 52.

Figure 52. Assign Bonded Failover Ports



Step 5. Click **Finish** to bond the two ports.

Step 6. Add your network to your virtual server. See Configuring Ethernet Networks.

5

CONFIGURING AND MANAGING STORAGE

STORAGE MODELS

The design decision you make regarding how virtual servers access storage could affect the success of your server virtualization deployment and/or your investment in storage infrastructure and practices.

When creating a virtual server, the data center manager creates a new virtual hard disk for each new virtual server. The manager allocates a certain amount of storage capacity and maps the virtual server to that disk storage.

Comparison of Virtual and Physical Storage

There are two primary models for how a virtual server accesses its storage—*virtual* or logical storage access, and *physical* storage access (i.e., raw).

- The virtual storage access model uses a logical volume manager to provide access to storage and to create and manage virtual machine images.
- The physical storage access model allows a virtual machine to map directly to storage in the same way that a physical server maps storage.

The design decision of virtual versus physical storage access will depend on the use cases for server virtualization as well as the desire to leverage existing investments in storage infrastructure and practices.

VIRTUAL STORAGE ACCESS MODEL

Since data center managers often create multiple virtual servers—typically with relatively small virtual hard disks—server virtualization vendors developed the ability to create virtual disks and disk groups from iSCSI and Fibre Channel LUNs. This is particularly useful in application development and test environments, where virtual machines are created for specific testing purposes and are often deleted once the test is complete. For these purposes, a virtual storage access model where the administrator creates, modifies and deletes virtual hard disks on the fly, is best.

The drawback of a virtual storage access model is that it introduces a new layer of abstraction. Storage management applications can be affected as the mapping of virtual disks to physical LUNs is abstracted to another level.

PHYSICAL STORAGE ACCESS MODEL

In a physical storage access model, a virtual machine's virtual disk is mapped directly to the raw iSCSI or Fibre Channel LUN in the same way that a physical server is mapped to a LUN. A main advantage to this model is the ability to maintain investments in storage management solutions and disciplines. Since the virtual machine is interfacing with the storage directly, all existing storage management solutions such as snapshots, replication, and resource management, work seamlessly.

CONFIGURING STORAGE

Virtual Servers (VSs) can be configured to access two types of disks:

- **Logical disks**—High-performance disks that can be assigned to one or more virtual servers. The size can be smaller than the underlying physical disk. Supported on Fibre Channel, iSCSI, and local storage.
- **Raw SAN disks**—High performance. One or more virtual servers use one entire physical LUN.

Note: For best performance, Virtual Iron recommends that all storage be in logical disks.

Note: A single LUN can not use the both Fibre Channel and iSCSI.

The following table summarizes the functional differences between these disk types.

	Logical	Raw
Shareable between VSs	X	X
High-performance	X	X
Supported on iSCSI SAN	X	X
Supported on Fibre Channel SAN	X	X
Supported on local storage	X	--
Ability to subdivide physical disk	X	--
Cloning capability	X	--
Dynamic VHD file import	X	--
Fixed VHD file import	X	--
Export capability	X	--

Advantages of Managed Storage

VI-Center presents a unified framework for controlling local or SAN disks that are accessible to managed nodes and their VSs. In this framework, you create one or more *disk groups* (DGs), and subdivide them into one or more *logical disks*. Logical disks have additional utility in that they can be copied (cloned) and exported for use by other virtual servers. Neither of these capabilities is available in the management of raw SAN disks.

Overlaying a storage framework on available physical storage has distinct advantages. All physical LUNs can be administered from VI-Center. Following initial information exchange with the SAN administrator, the VI-Center administrator can use this framework to configure and manage logical disks on the SAN.

DISCOVERY AND MANAGEMENT OF PHYSICAL DISKS

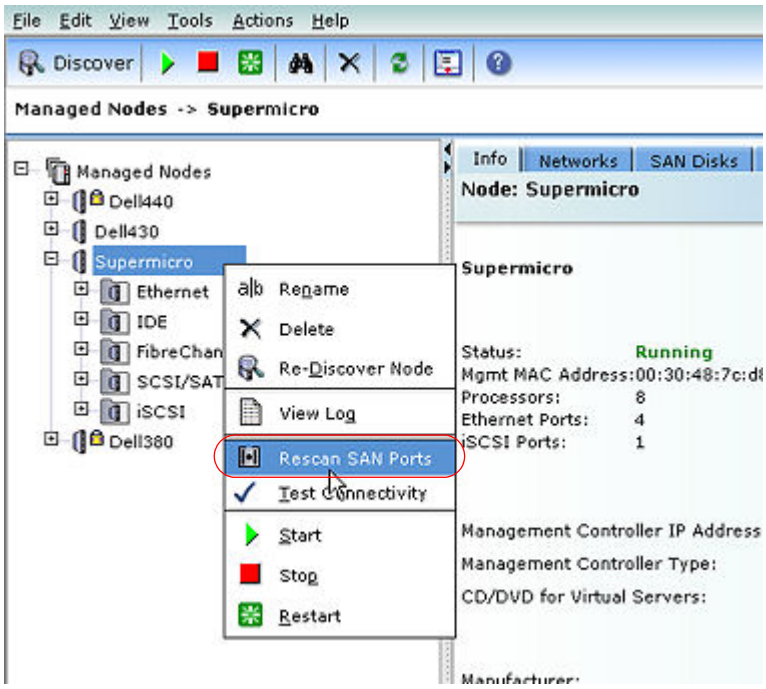
Virtual Iron supports three types of physical disks:

- Fibre Channel SAN disks
- iSCSI SAN disks
- SATA, SAS, or parallel SCSI node-local disks

Local IDE drives are not supported.

All physical disks are automatically discovered during the node boot process. If you reconfigure LUNs while a node is running, before adding them to the system, perform a Rescan to update the management server: In VI-Center's **Hardware** view, right-click the managed node and select **Rescan SAN Ports** from the menu. This step assures synchronization between the management server and your environment. See Figure 53.

Figure 53. Rescan SAN Ports



To access physical SAN resources, the managed node hosting it requires a host bus adapter (HBA) or network interface card (NIC). Each HBA has a unique WWNN or iqn, which you need to provide to your SAN or iSCSI administrator. The administrator makes specific LUNs visible to managed nodes in the Virtual Iron® framework.

Once this information has been configured in your SAN infrastructure, SAN targets and LUNS become visible to the managed nodes programmed to access them.

Storage Multipath

This version provides experimental and partial support for iSCSI multi-path, focusing on multiple storage controllers.

SAN multipath has been tested for Fibre Channel HBA and array cable pulls and disabled switch ports. Please see

http://www.virtualiron.com/products/servers.cfm

for the list of supported arrays.

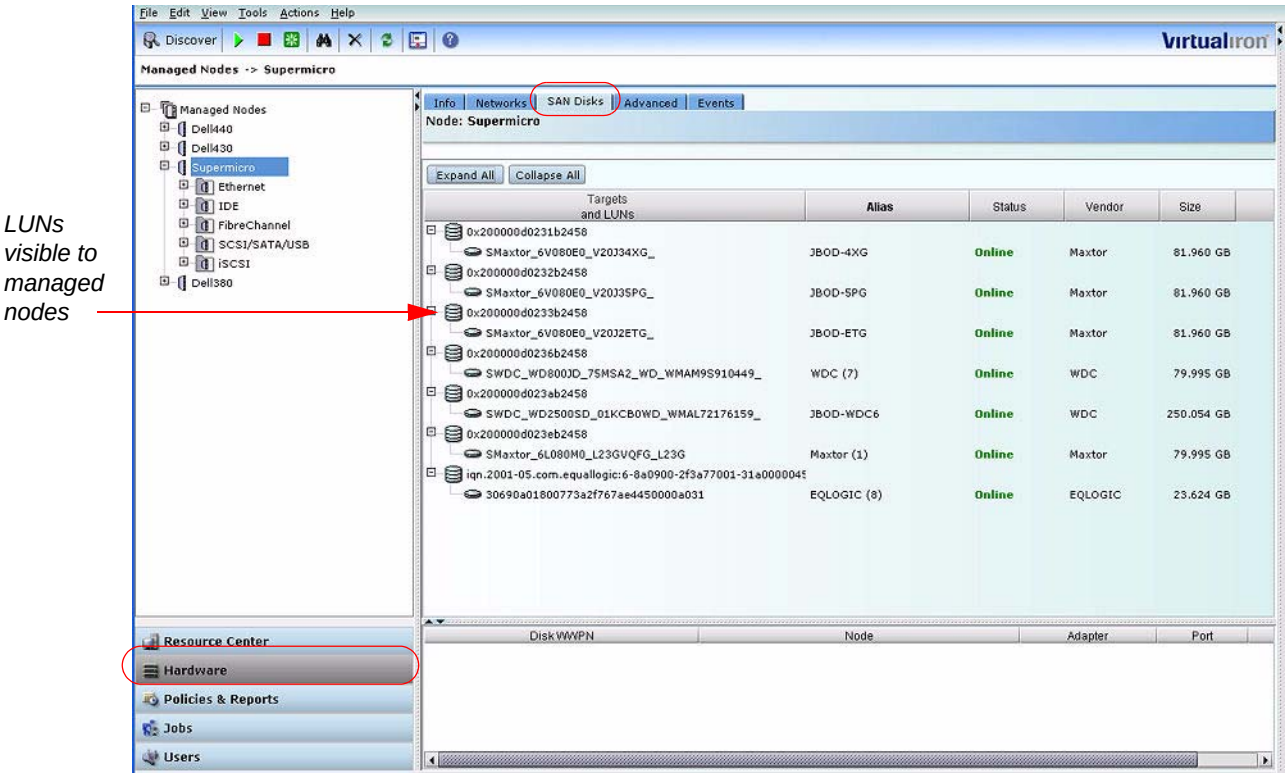
Viewing LUNs Accessible to all Managed Nodes

Step 1. Click the **Hardware** shortcut**.**

Step 2. Select a node in the navigation tree.

Step 3. Select the **SAN Disks** tab. A sample view is shown in Figure 54.

Figure 54. LUNS available to All Managed Nodes



LUNs and Aliases

VI-Center allows you to assign an alias to each LUN. Examples of aliases are “Windows 2003 + SQL Server” or “SAP data.”

To assign an alias to a LUN, in the **Hardware** view,

Step 1. Select the node.

Step 2. Select the **SAN Disks** tab.

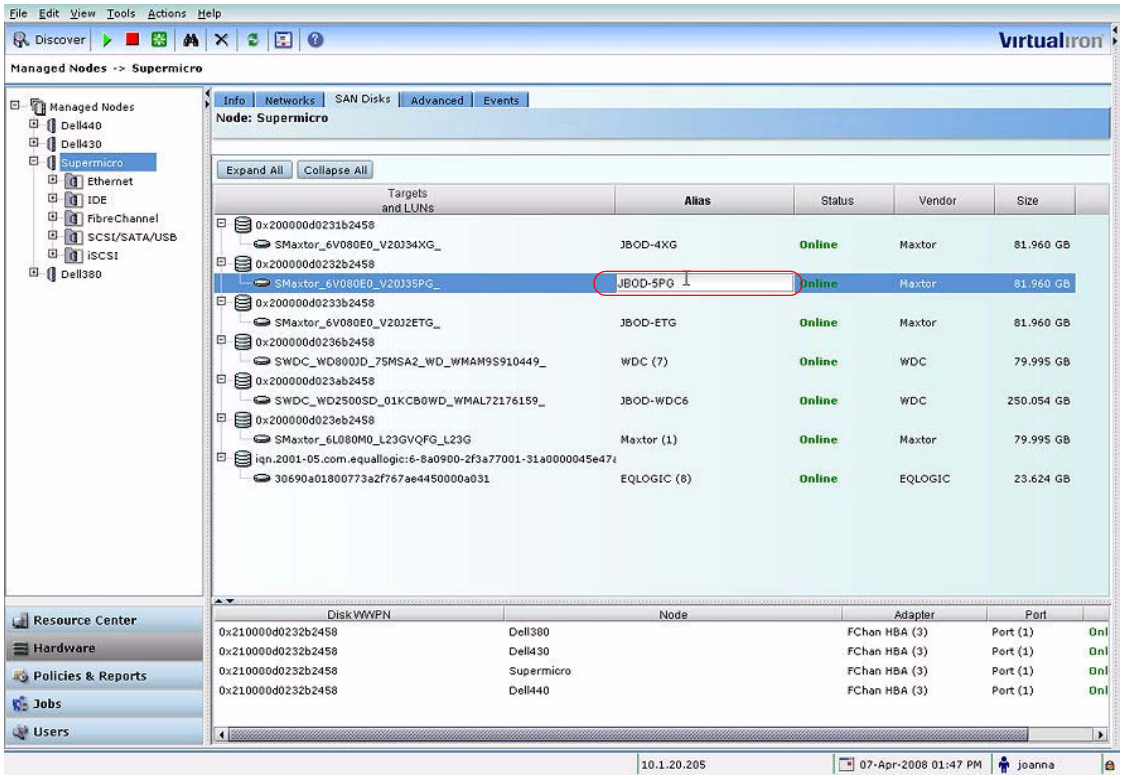
Step 3. Select the LUN and double-click its designation in the **Alias** column.

Step 4. Enter the alias in the field. An example is shown in Figure 55.

Note the WWPN (WorldWide Port Name) information that at the bottom of the window. This is the unique serial number assigned to each Fibre Channel adapter that identifies that network port from all others.

Figure 55. Alias assigned to a LUN

Alias assigned to a LUN

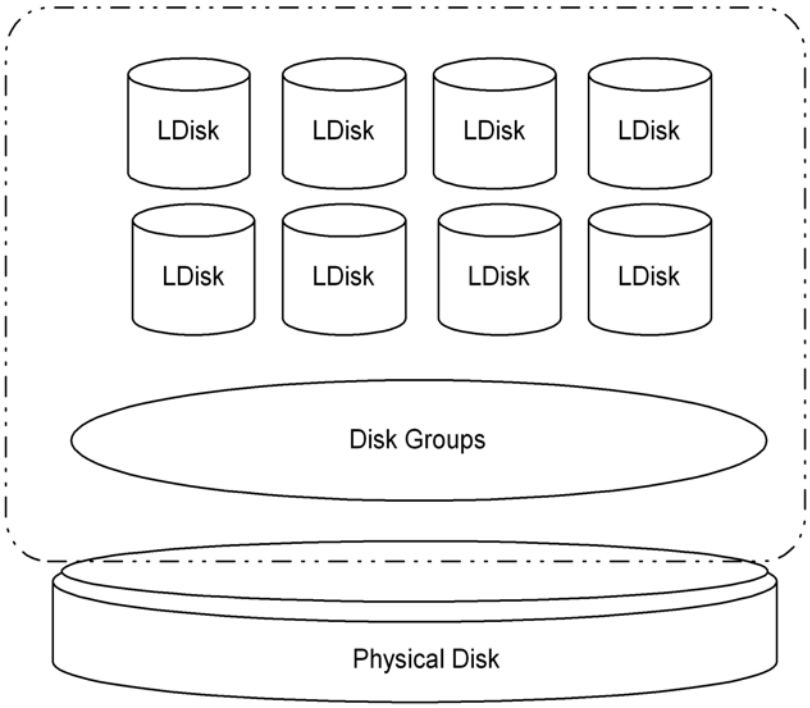


CONFIGURING LOGICAL DISKS

The Virtual Iron VI-Center supports the creation and assignment of logical disks on local drives or SANs. Before you configure logical disks, read the following section to understand how logical disks are organized within *disk groups* (DGs).

The illustration in Figure 56 shows the relationships between physical disks, DGs, and logical disks.

Figure 56. Virtual Iron® SAN Storage Management



Disk Groups and Logical Disks

Each disk group is essentially a storage container. Disk groups consist of one or more SANs or local disks. Virtual Iron® enables you to make use of the storage contained in a DG by subdividing it into one or more logical disks. The process for creating logical disks on a local drive is the same as for creating them on a SAN.

Logical disks can be copied (or cloned) for use by other VSs, and they can also by administratively exported or imported from a directory within VI-Center.

Once you create logical disks, they are visible to all VSs hosted on the VDC.

Creating Disk Groups

Follow this procedure to create disk groups. After you create the disk groups, you can assign them to virtual servers, as described later in this procedure.

Step 1. Begin by creating and assigning nodes to a Virtual Data Center as described in Creating Virtual Data Centers.

Step 2. To create a disk group, in the **Resource Center** view:

A. Select the VDC in the navigation tree.

B. Select the **Virtual Storage** tab.

C. Select either **Local Disks** or **SAN Disks.**

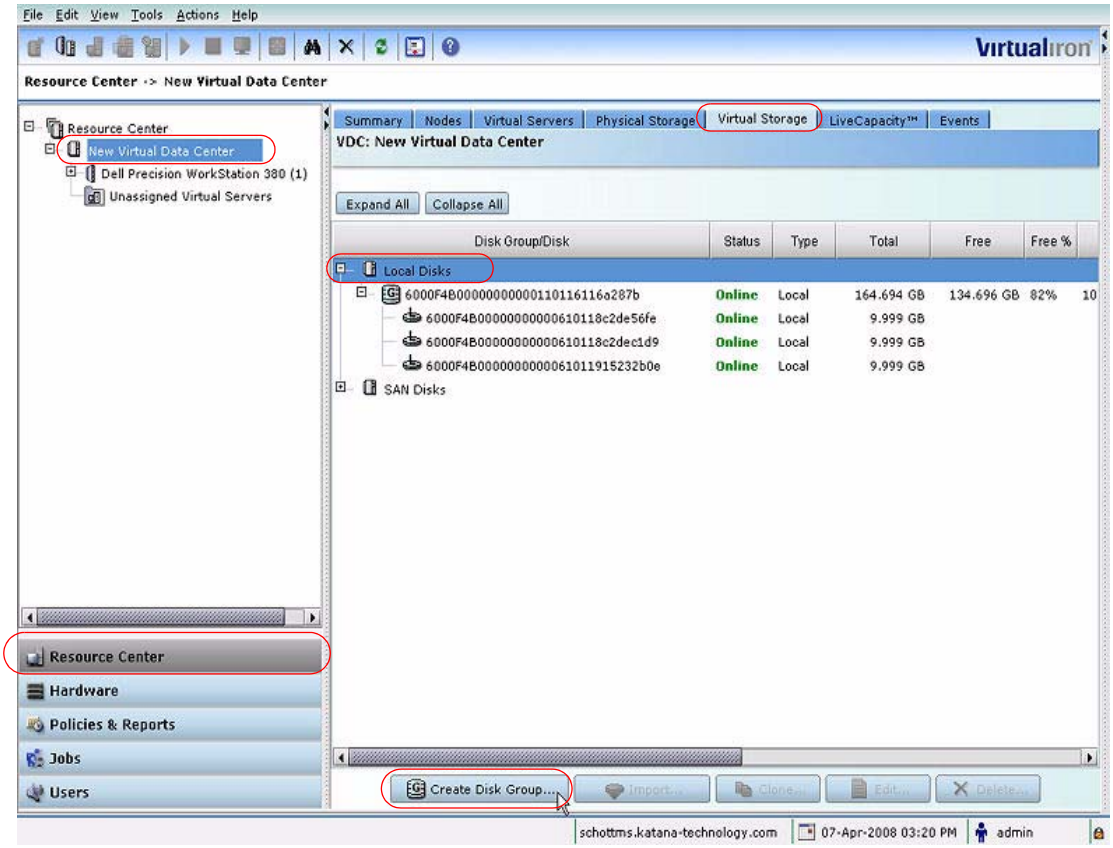
D. In Figure 57, a local disk has been selected. Click **Create Disk Group...**

Figure 57. Create Disk Group

VDC selected

Local disks selected

Create Disk Group



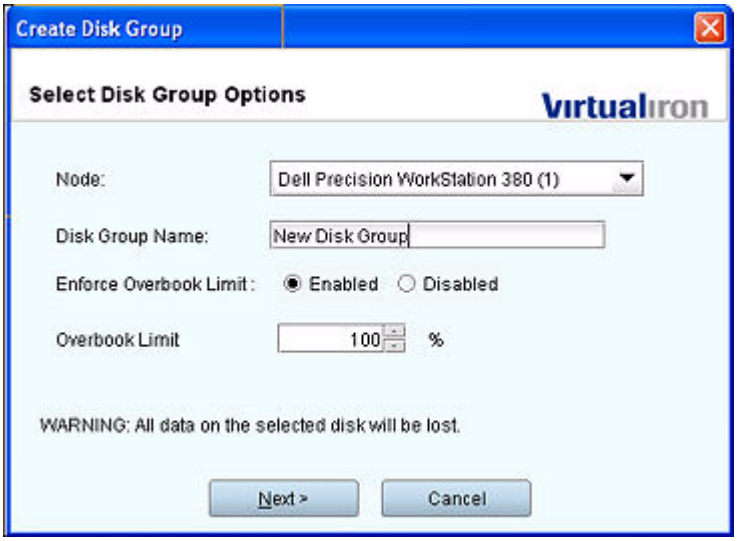
Step 3. The Disk Group Wizard appears (Figure 58) with all nodes in the VDC listed in the Nodes pulldown.

The DG Name **New Disk Group** is assigned to the group by default. Enter a name for the disk group.

Leave the default values for **Enforce Overbook Limit** (Enabled) and **Overbook Limit** (100%). These fields are related to the Snapshot feature. See Snapshots and Overbooking for detailed information.

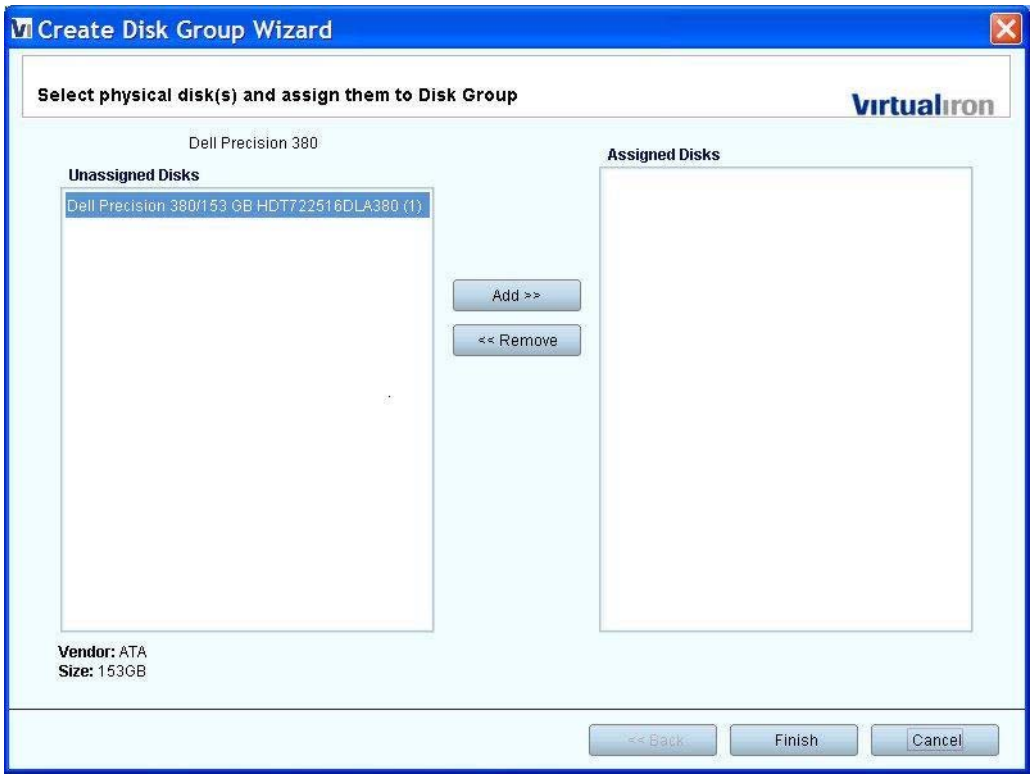
Step 4. Click **Next>>** to continue.

Figure 58. Begin DG Wizard



Step 5. Each DG must be mapped to a physical disk. In the next window (see Figure 59), choose the disk on which to place the disk group. In Virtual Iron®, each physical disk can be allocated to one and only one disk group. You can add disks to the disk group at creation time, or dynamically when the disk group is in operation, if you need additional storage space.

Figure 59. Assigning a Disk to the DG

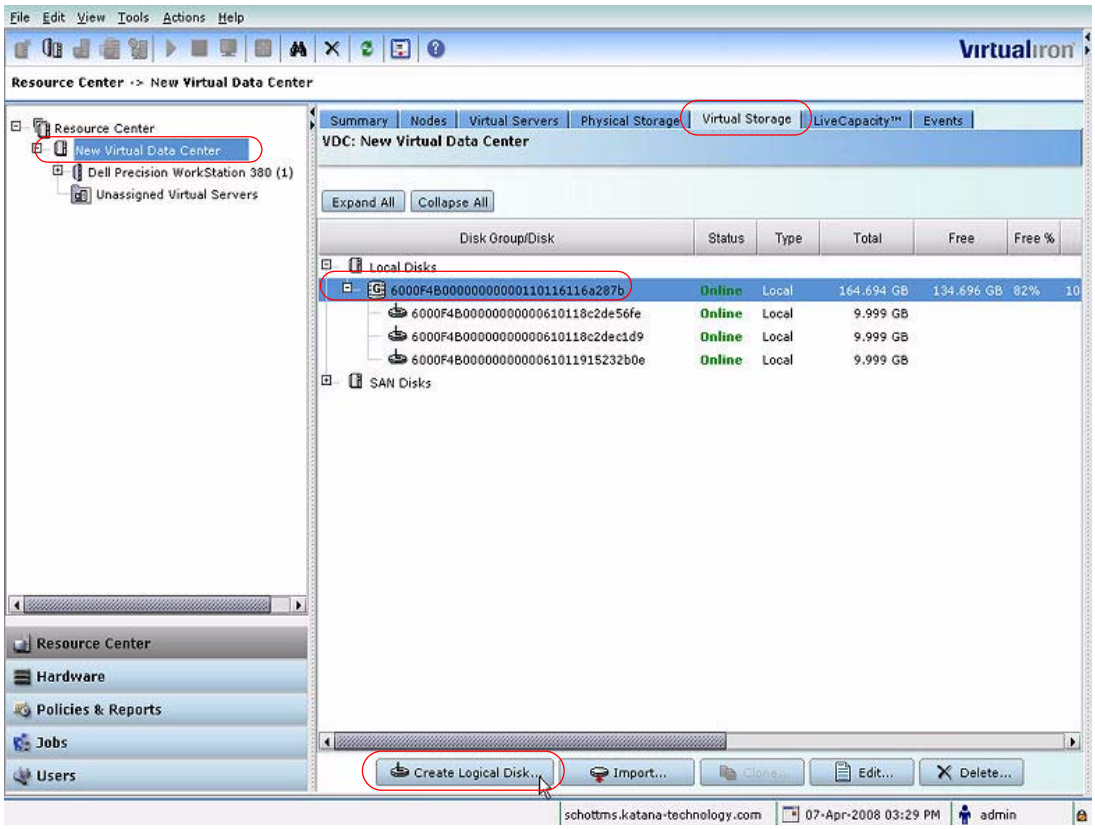


To assign a disk to the DG, select the disk in the Unassigned Disks pane. Then click **Add>>** and **Finish**. The new DG appears in the window as shown in Figure 59.

Creating Logical Disks

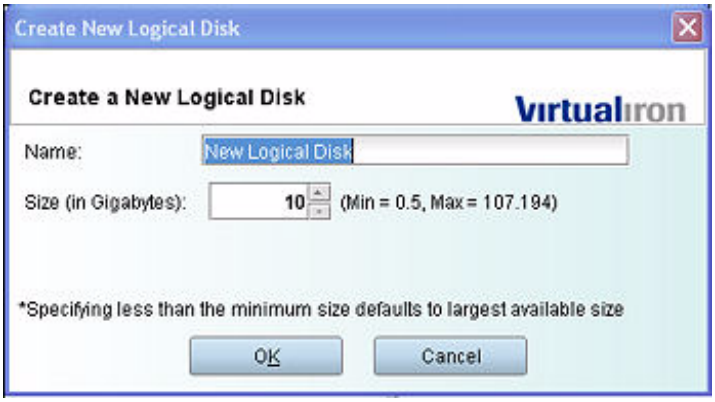
Step 1. Select a disk group as shown in Figure 60.

Figure 60. Select Disk Group



Step 2. Click **Create Logical Disk** (see Figure 61). The window shown in Figure 61 appears.

Figure 61. Create a New Logical Disk



Step 3. Assign a name to the logical disk, and a size in GB. By default, the name assigned by VI-Center is New Logical Disk.

Step 4. Click **OK**. The new logical disk is added to the tree in the Logical Disks tab.

Creating iSCSI LUN Groups

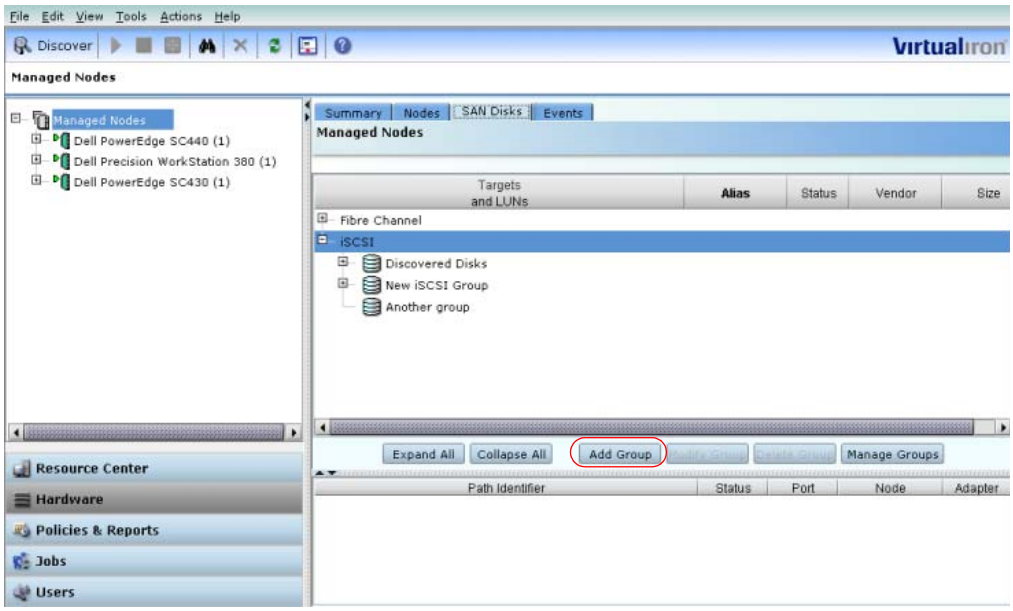
If you have a lengthy list of iSCSI LUNs, you can group iSCSI LUNs in any logical grouping you want.

Step 1. Click **Hardware**.

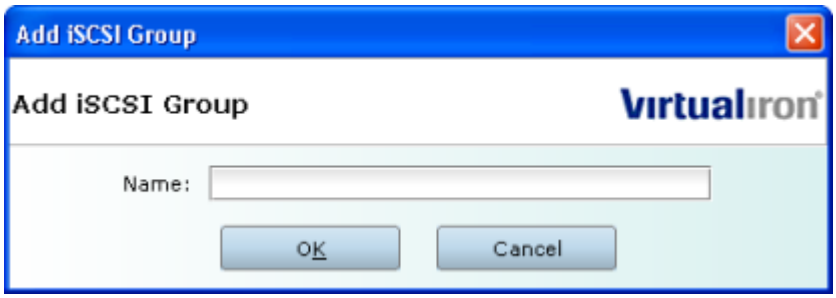
Step 2. Click the **SAN Disks** tab.

Step 3. Select **iSCSI**.

Step 4. Click the **Add Group** button.

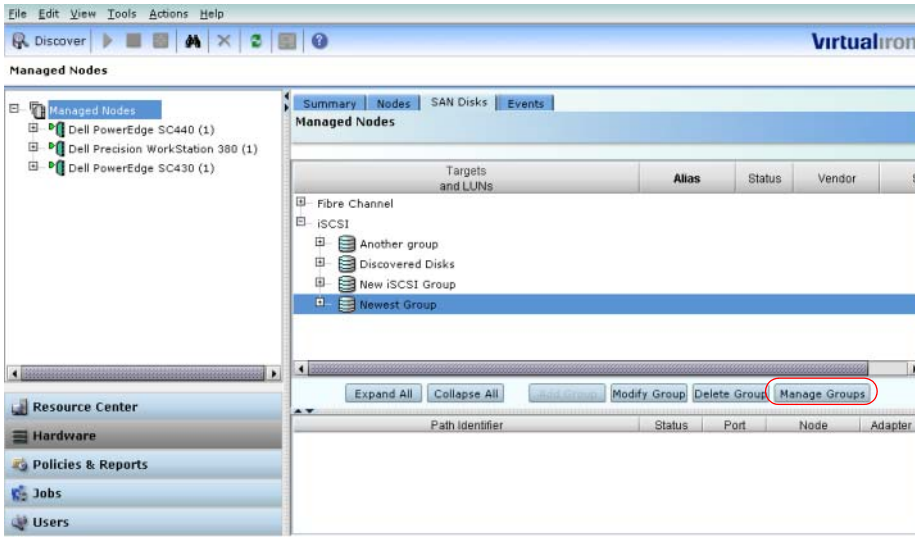


Step 5. The **Add iSCSI LUN Group** dialog appears. Enter a name for the new iSCSI group and click **OK**.

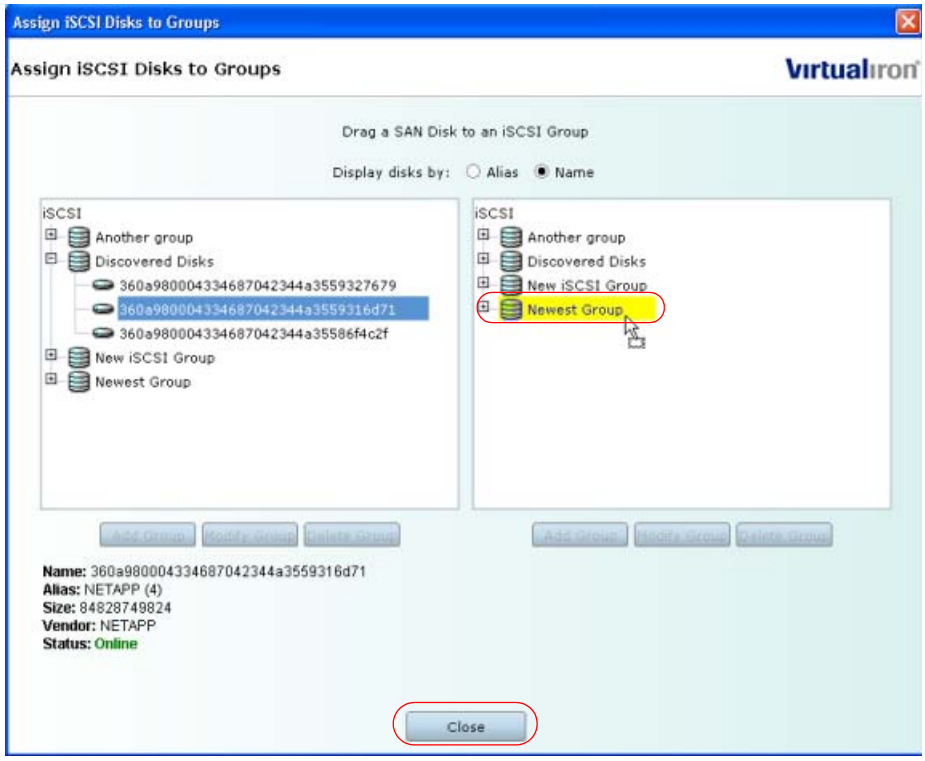


Step 6. Select the new iSCSI group.

Step 7. Click the **Managed Groups** button.



Step 8. In the **Assign iSCSI Disks to Groups** dialog appears, select disk or hold down the Ctrl key to select multiple disks, and drag and drop the selected disks on top of the new iSCSI group you just created.



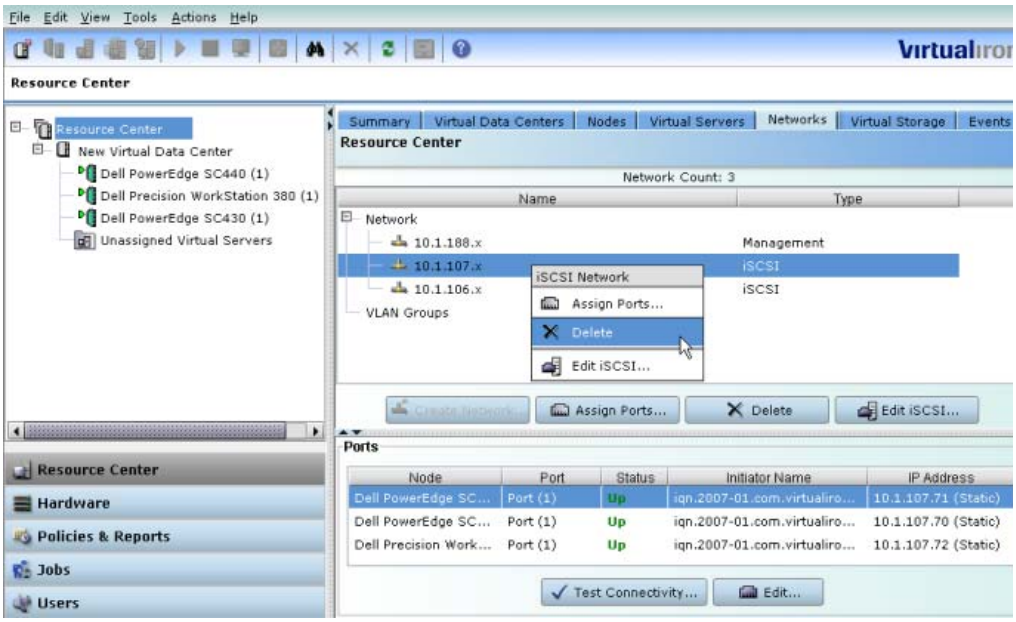
Step 9. Click **Close**.

Deleting iSCSI Networks

Step 1. Click **Resource Center**.

Step 2. Click **Networks**.

Step 3. Right-click on the iSCSI network you want to delete.



Step 4. Click **Delete** in the menu that appears.

EXPORTING AND IMPORTING

Use the export and import functions to move VHD files on the VI-Center from and to the disk groups in your data center. This is also useful if you want to move a logical disk to a new disk group in a different VDC.

There are two types of VHD files, each of which is stored differently in the data center:

- **Dynamic**—As data is written to the dynamic disk, the file grows as large as the maximum size that was specified when it was created. Unused space is not included in the image, reducing the size of the dynamic disk file. If you import a dynamic VHD, the file is imported to a virtual disk.
- **Fixed**—A fixed-size hard drive is one in which space is allocated when the VHD is created. The size of the disk does not change when data is added or deleted. If you import a fixed VHD, the files are imported to a logical disk.

Commonly used VHD files on the VI-Center may be made available to multiple users. Use the import and export functions to move VHD files to the VI-Center for use in virtual servers.

Exporting A Logical disk

To export a logical disk using Virtual Iron® Extended Enterprise Edition, proceed as follows:

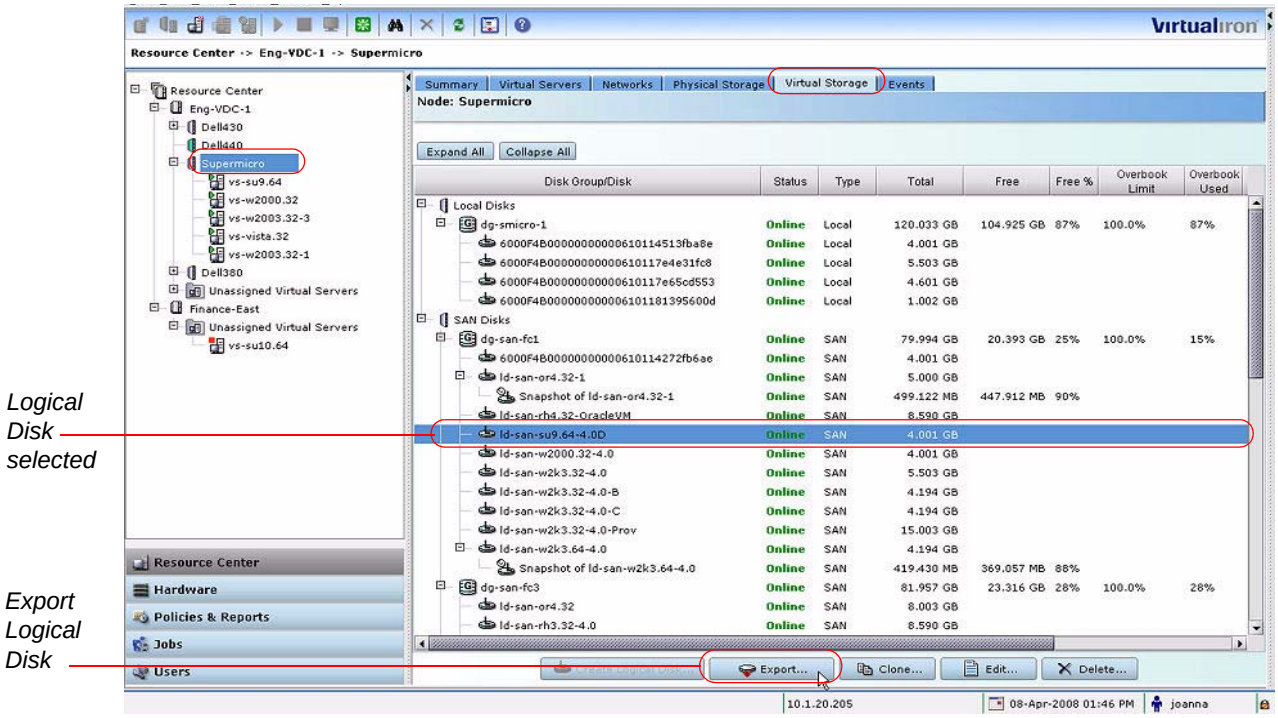
Step 1. In the Resource Center view, select the node in the navigation pane containing the logical disk to be exported. See Figure 62.

Step 2. Click the **Virtual Storage** tab and expand the list of Local and SAN disks.

Step 3. Select the logical disk in the pane.

Step 4. Click **Export**.

Figure 62. Exporting a Logical Disk

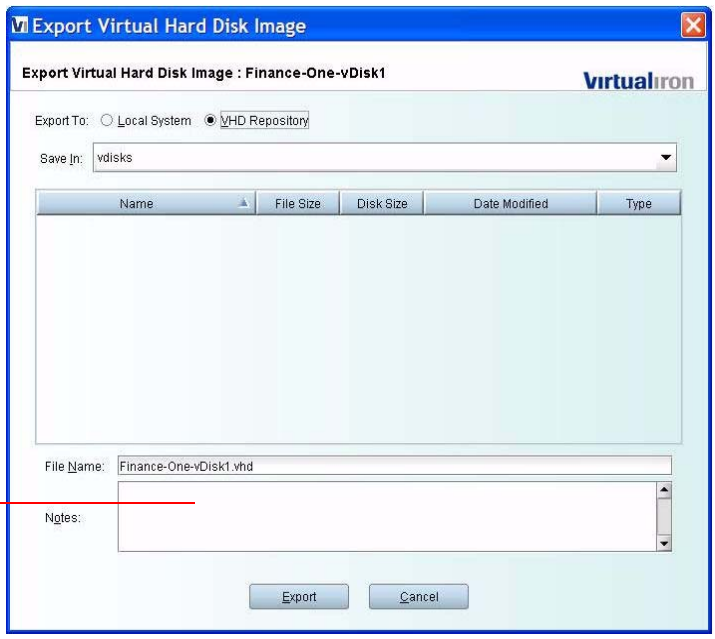


Step 5. VI-Center displays the **Export Virtual Hard Disk Image** window shown in Figure 63. The window shows the contents of the logical disk directory on VI-Center. You may enter notes on the content of the Logical Disk in the Notes pane.

Click **Export** to complete the operation.

Figure 63. Contents of Logical Disk Directory

Add optional notes on the exported Logical Disk



Importing a virtual disk

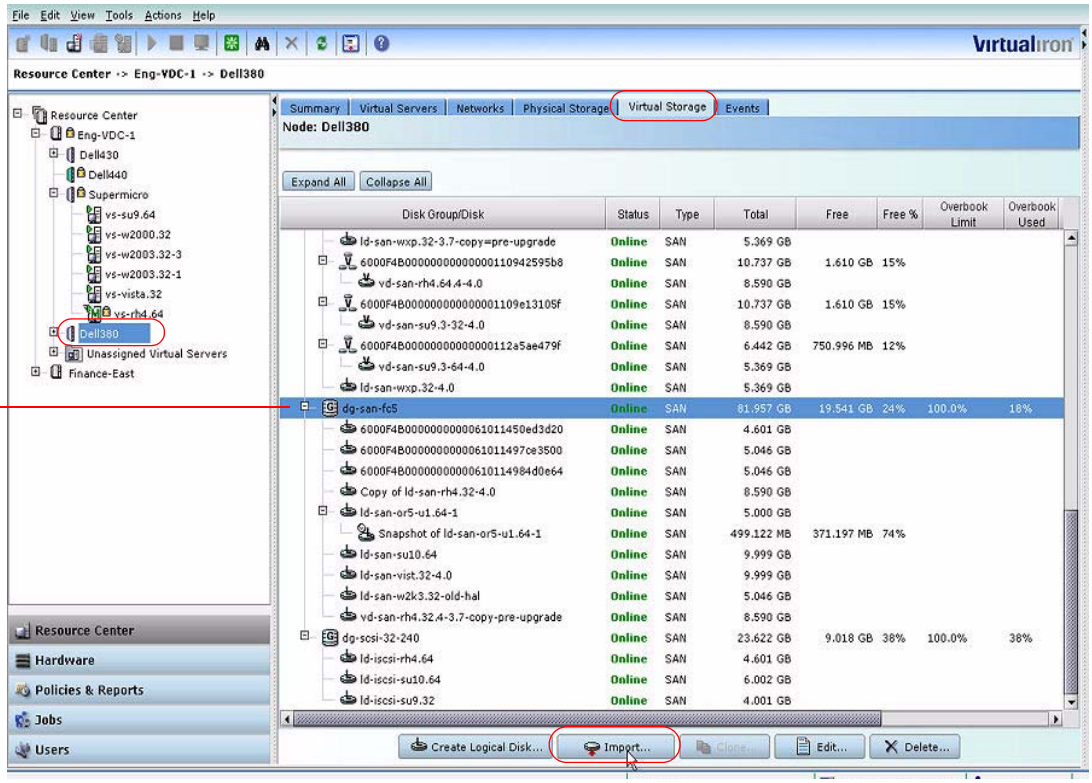
Step 1. In the Resource Center view, select the node in the navigation pane containing the logical disk to be imported. See Figure 64.

Step 2. Click the **Virtual Storage** tab and expand the list of Local and SAN disks.

Step 3. Select the disk group in the pane.

Step 4. Click **Import**.

Figure 64. Importing a Logical Disk



Logical Disk selected for import

Step 5. VI-Center displays the **Import Virtual Hard Disk** window shown in Figure 64. The window shows the contents of the logical disk directory on the VI-Center.

Choose the logical disk you want to import, then click **Import** to complete the operation.

CLONING DISKS

Virtual Iron® allows you to clone (copy) logical disks and their associated content to any other disk group under management. Note that logical disks can only be cloned when they are not in use by a virtual server.

Virtual disks may be cloned to logical disks or other virtual disks.

	To:
Logical Disk—Fixed	Logical Disk—Fixed
Virtual Disk—Dynamic	Logical Disk—Fixed or Virtual Disk—Dynamic
Virtual Disk—Fixed	Logical Disk—Fixed

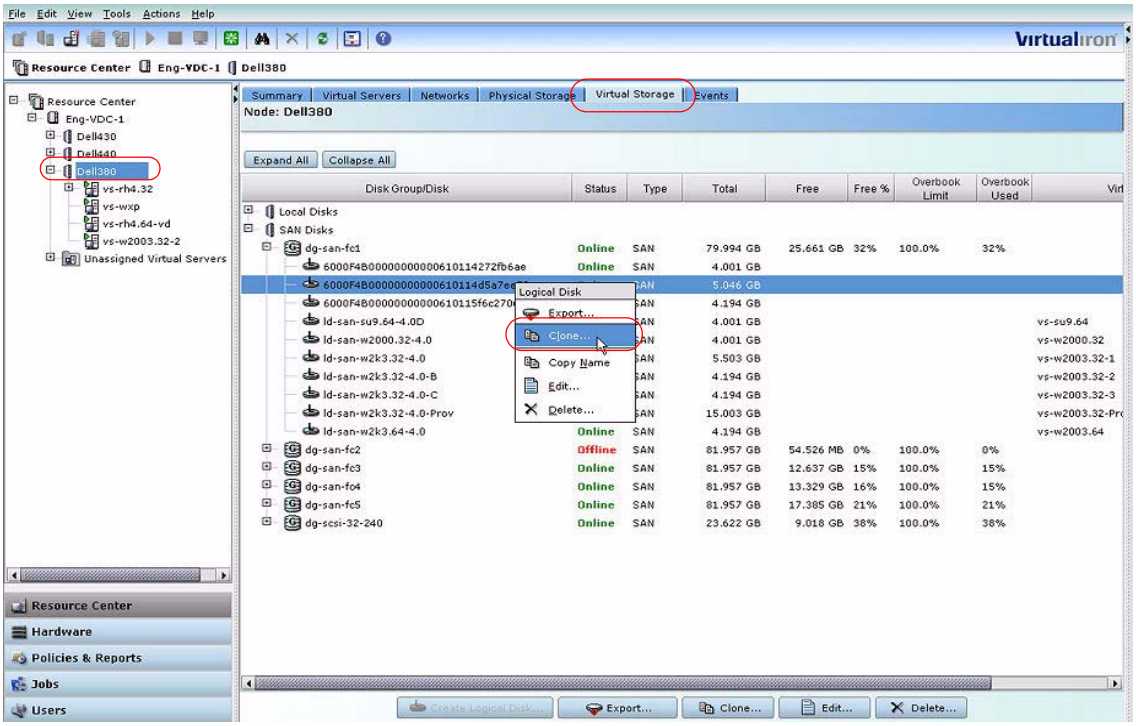
Cloning Logical Disks

Step 1. In the **Resource Center** view, select the node in the navigation pane that contains the virtual server you want to clone. See Figure 66.

Step 2. Click the **Virtual Storage** tab and expand the navigation tree.

Step 3. Select the logical disk to clone. Right click and select **Clone** from the menu, or click **Clone** at the bottom of the window.

Figure 65. Cloning a Logical Disk



In the **Clone Logical Disk** dialog box, type a name for the logical disk, and use the pull-down menu to choose a volume for the cloned disk's parent. Click **OK**. The cloned logical disk is created on the disk group you specified.

Note that VI-Center only presents volumes eligible to support the disk you are cloning. If a disk you are cloning has .5GB, only volumes with at least this much space are presented on the pull-down menu.

The cloning operation may take several minutes. The progress bar that appears is updated every 10-15 seconds.

Figure 66. Cloning a Virtual Server

Choose parent volume

VHD REPOSITORY

For Virtual Iron XEE, the Virtual Hard Disk (VHD) image is a complete copy of a virtual computer's operating system and its applications. You may import or export a VHD image to or from the VI-Center VHD repository and your local computer. Note that when you change the directory used as the VHD repository of the VHD files, you change it for all users.

VHD File Naming Conventions

Exporting to a repository results in a VHD image file from which you can create virtual disks. You can't import directly from a local computer to a VHD repository.

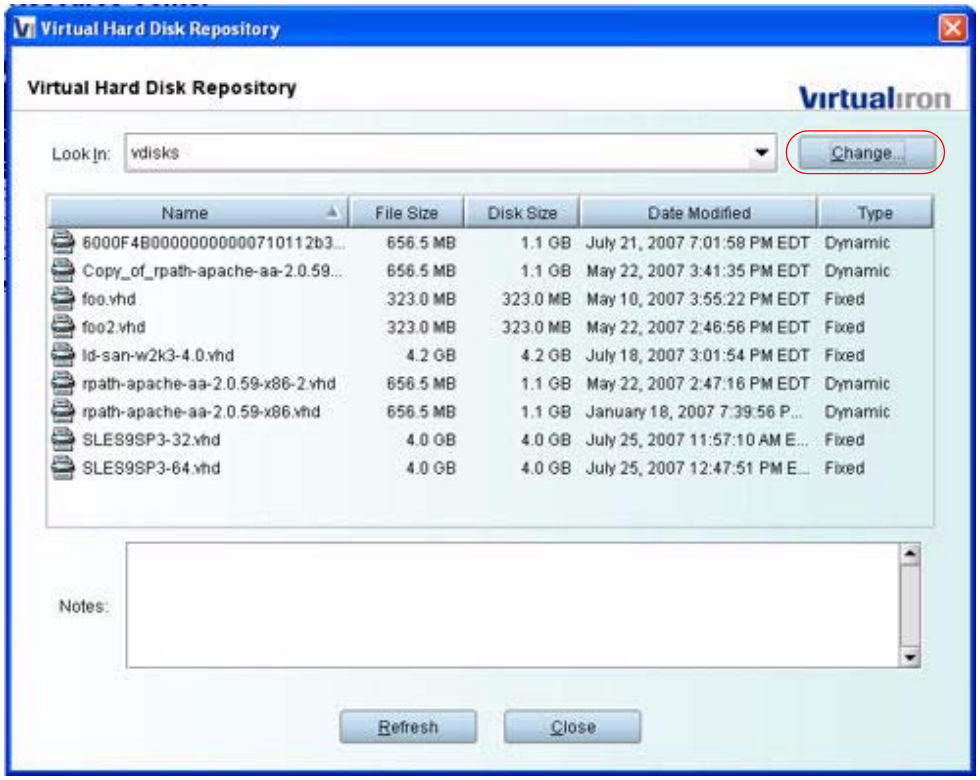
Importing from a repository allows you to save a VHD image file that has been added to the VHD repository from a managed node, into a repository's virtual disk.

Exporting or Importing VHD Image Files

Note that if you change VHD directories to a local computer, you can change it back to the default Vdisks Directory.

Step 1. In the VI-Center **Tools** menu, select **VHD Repository**. The following screen appears.

Figure 67. Virtual Hard Disk Repository Screen Showing VHD Image File

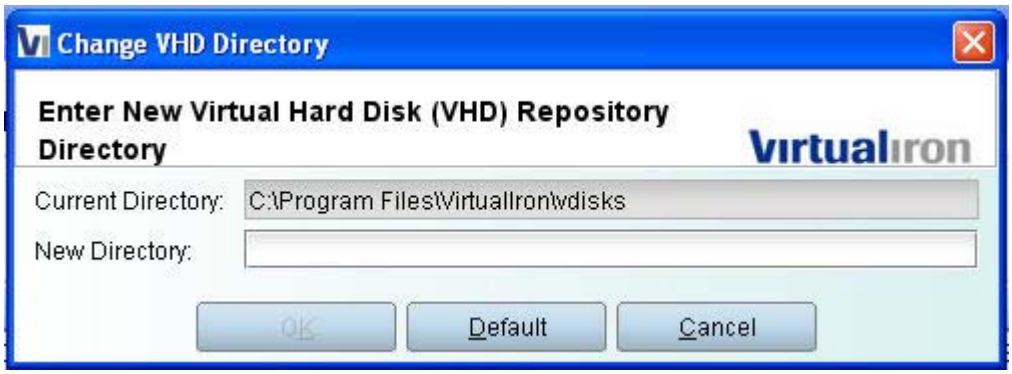


Step 2. Select a location from the pulldown menu.

Step 3. Click **Change**.

Step 4. The dialog box shown in Figure 68 appears. Click **Default**.

Figure 68. Change VHD Directory Dialog Box



Step 5. If you wish to set up a non-default VHD repository, refer to the following procedure.

Customizing Your VHD Repository

To set up a non-default VHD repository, do the following.

Step 1. Specify the VHD repository path by setting the local variable default, VHDRepositoryPath, in

etc/vdi.properties

to the directory you want to use as the VHD repository.

UNIX Linux—On Linux, the directory will be created if it doesn't already exist. For UNIX Linux management servers, UNIX Linux naming rules and directory separator characters apply. for example, to set the repository to the directory /opt/storage/vdisks:

start.arg.7 = /opt/storage/vdisks

Windows—On Windows, the directory must already exist and be shared. In addition, both Share and Directory permissions must be set to Everyone-Full Control. If an invalid directory is specified, or if the directory cannot be created, an error is logged, and the directory will remain set to the last valid directory set.

For local drives, the drive letter and a colon (c:) are followed by two “\” characters (\\) and NAS Storage\\VHD Repository. For example, to set the VHD repository to the directory NAS Storage\VHD Repository on the g: drive:

start.arg.7 = g:\\NAS Storage\\VHD Repository

For Windows management servers, windows-specific UNC syntax is required. This consists of four "\" characters (\\\\), followed by the server name (not the IP Address) and the path. Subdirectories in the path are specified with 2 "\" characters (\\). For example

start.arg.7 = *servername*\\NAS Storage\\VHD Repository

If you specify a directory for the VHD repository, the directory is created after you restart the VI-Center. If you specify an invalid directory, or if the directory can not be created, an error is logged and the directory remains set to the last valid directory.

Step 2. Restart the management server.

Note: Make sure that the account that runs the VI Management Server service has the appropriate permissions to read and write to the new directory or share.

NBD Repository

VI-Center allows you to set and edit your Network Boot Device (NBD) directory.

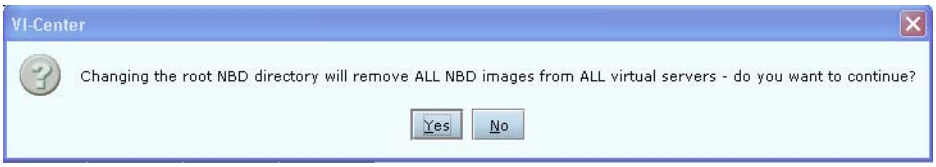
Setting the NBD Repository Manager

Use the following procedure to change the NBD directory.

Step 1. In VI-Center, select **Tools > NBD Repository Manager**.

Step 2. In he Network Block Device Repository window, click the **Change** button.

The following warning dialog appears.



Step 3. Click **Yes**.

Step 4. In the Change NBD Source Directory window, enter the new directory path you want to use. If you want to set your NBD directory to a network drive, you can't set the service to run as a "Local Service." The service should run on behalf of a user with network permissions.

Important Note: Microsoft Windows will not allow a process running as a service to access network drives using the format 'z:\nbd'. To access network drives, you will need to use the format '\\machine name\directory' or '\\IP Address\directory'.

Note: Shutting down the Management Server brings down the NBD and any Virtual Servers assigned to the NBD. Before restarting the Management Server, shut down all nodes with Virtual Servers attached to the NBD.

SNAPSHOTS AND DISK SPACE USAGE

A snapshot disk contains data from a disk at a specific moment in time. Since snapshot disks are temporary, the system will minimize the physical memory disk space needed to maintain them. For example, after configuring a virtual server and confirming that it is operating correctly, you can take a snapshot of the virtual server and its disk to capture its current state. Then, if you want to test some changes that you think might adversely affect the virtual server, if an error occurs, you can use the virtual server or the snapshot to quickly recover. See Virtual Server Snapshots for additional information and detailed configuration procedures.

The advantages of using Snapshot are:

- The initial size of the snapshot is a small fraction of the size of the parent virtual server.
- A snapshot can be taken whether the virtual server is on or off. Volatile memory is saved in an image file.
- The snapshot captures the state of a logical disk. This data is linked to, but independent from, the parent logical disk, so it can be used by other virtual servers.
- Snapshots take a fraction of the time of needed to clone a disk. Cloning also creates an independent disk, but uses more space.

Snapshots Example

Since Snapshot disks are temporary, the system will minimize the physical memory needed to maintain them. When you initially create a snapshot, a 10% default size is used.

For example, if your virtual server has a disk of 10 GB, your snapshot of this disk will be allocated 1 GB. How can a 10 GB disk be copied into a 1 GB space and maintain all the data? Through a process of maintaining pointers to the original disk's contents, the system uses less space to capture the data.

If any data changes on the original disk, the original data in this example is moved onto the snapshot disk area and the 1 GB space is used. If there are many changes on the original disk and the 1 GB space begins to fill, the system automatically increases the size of the Snapshot disk. See Virtual Server Snapshots for policy configuration.

EDITING A SNAPSHOT

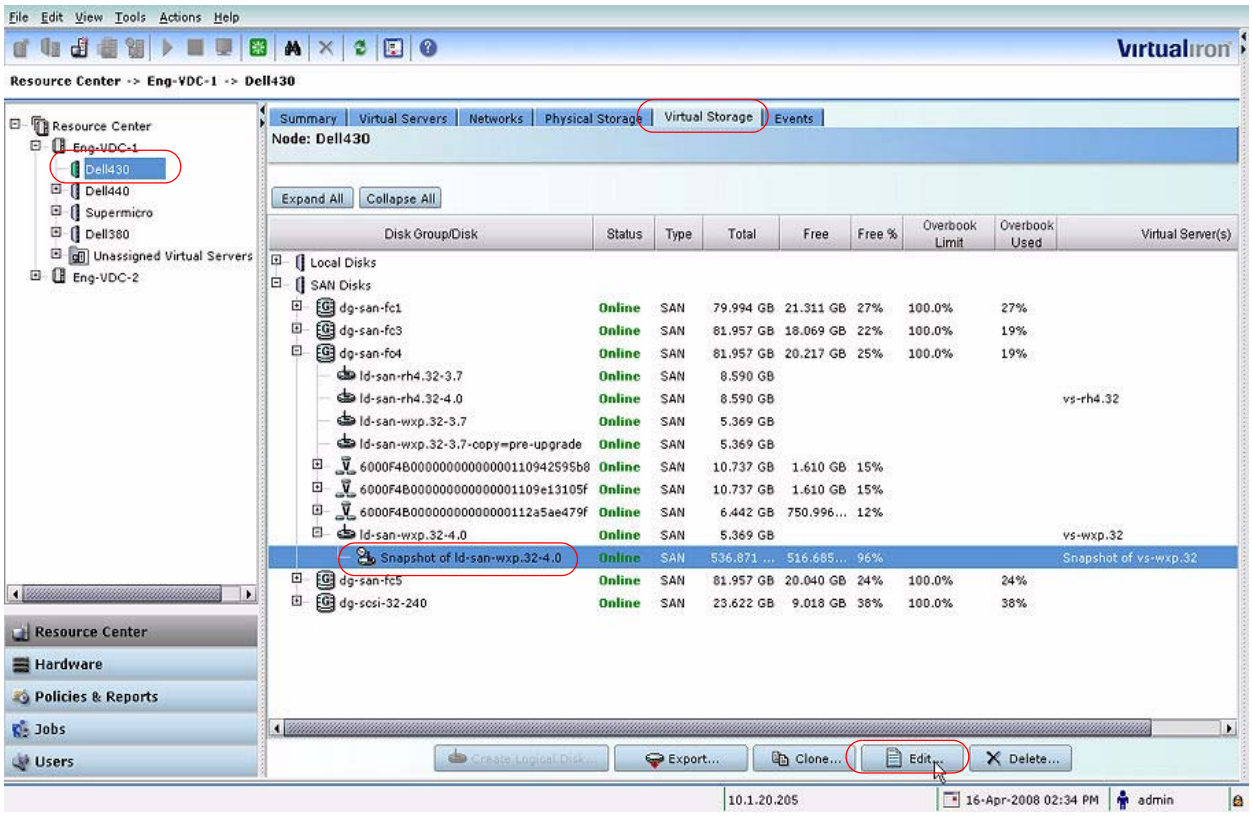
Step 1. In the Resource Center view, select the node in the navigation tree.

Step 2. Select the **Virtual Storage** tab.

Step 3. Expand the view and select the snapshot.

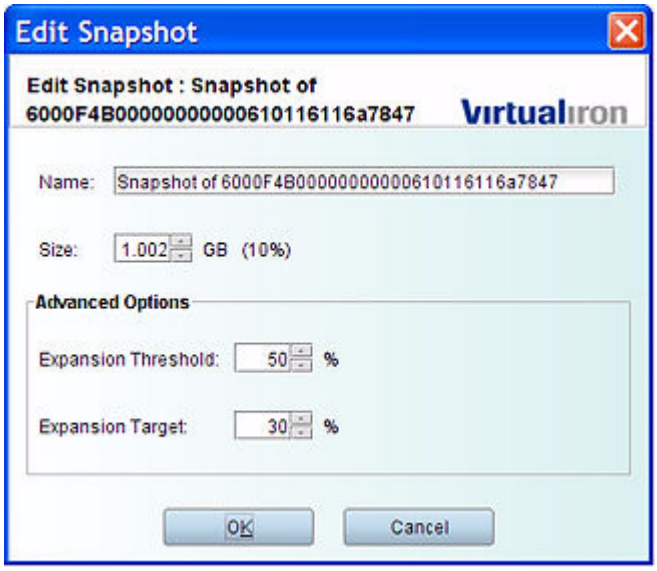
Step 4. Select the **Edit** button. See Figure 69.

Figure 69. Snapshot Entity in Virtual Storage



Step 5. The following dialog box is displayed.

Figure 70. Edit Snapshot Dialog Box



Step 6. Make your changes and click **OK**.

Notice that the size of the snapshot disk and the default threshold and target settings are shown. The system monitors the size of your snapshot disk.

When it gets to 50% full, the snapshot disk space grows until your current usage is at 30% of the space. In this example, once you have used about 500 MB of your 1 GB space, the snapshot will grow to be 1.5 GB, where 500 MB is about 30% of the 1.5 GB.

While you can think of the snapshot disk as an exact copy of your original disk, the Virtual Iron snapshot algorithm optimizes disk space usage to preserve as much disk space as possible.

Snapshots and Overbooking

When you take a snapshot of your logical disks, the system optimizes the space needed to maintain the snapshot data. However, the system also maintains expansion space for the snapshot to grow. Use the Overbooking value to specify the amount of space to use, and to allow the system to go over, or overbook, the specified expansion space.

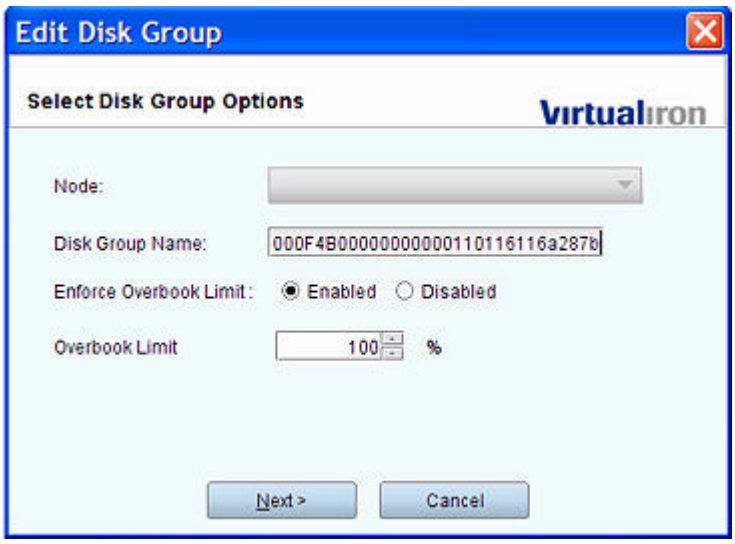
Here's an example: You have created a 100 GB disk group and then created the following disks for your virtual servers to use:

Table 2.

Logical Disk Size	Snapshot Size	Snapshot Expansion Size
20 GB	2 GB	18 GB
30 GB	3 GB	27 GB

At this point, your overbooking is **Enabled** and set to **100%**, the defaults for all disk groups. You can not create any more logical disks since you are currently using the 100 GB space: 20 + 30+ 2 + 3 +18 + 27 GB.

Figure 71. Setting Overbook Limit for Snapshots



Assuming that your snapshot disks will most likely not grow to consume their entire expansion size, you can adjust the overbooking value to take advantage of this. By changing the Overbook Limit to 150%, you can create another logical disk as shown:

Table 3.

Logical Disk Size	Snapshot Size	Snapshot Expansion Size
20 GB	2 GB	18 GB
30 GB	3 GB	27 GB
Additional logical disk		
25 GB	2.5 GB	22.5 GB

The 150% Overbook Limit allocates an additional 50 GB: 25 + 2.5 + 22.5 GB.

STORAGE MANAGEMENT

Storage management consists of the following:

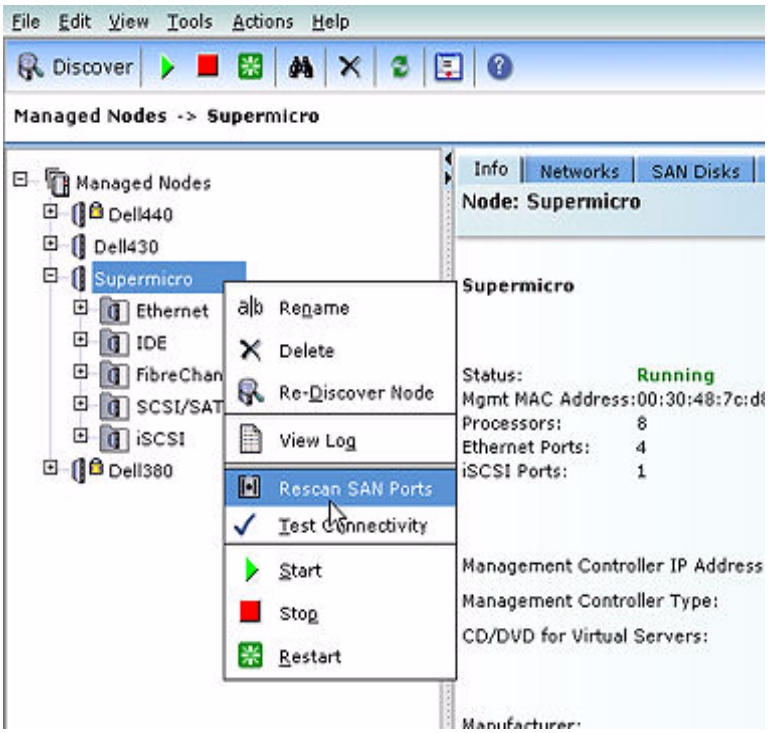
- Adding LUNs
- Resizing LUNs
- Removing LUNs

The storage management process is slightly different, depending on whether you are using raw or logical storage. There are capabilities in many storage servers that can improve storage utilization, such as thin provisioning. Consult your storage server documentation to see if this is right for you.

Adding LUNs

If you add LUNs to a storage controller, you do not need to reboot. In the **Hardware** view, simply run the **Rescan** command. See Figure 72.

Figure 72. Rescan SAN Ports



Resizing LUNs

Resize LUNs with caution! Please call Technical Support for assistance before resizing LUNs: 1-800-314-9872

Note the following in relation to resizing LUNs:

- LUNs should only be increased in size.
- LUNs that are part of a disk group cannot be resized.
- Only resize LUNs that are used raw.
- Before resizing a LUN, stop all virtual servers that are using that LUN.

Technical Support will supply a script and directions. Once you have completed the procedure, in the **Hardware** view, run the **Rescan** command on your LUNs to see the new LUN size. See Figure 72. Resizing a LUN requires a reboot of the node.

Reconfiguring SAN Storage

A SAN storage array should be reconfigured in this order:

Step 1. Delete any Logical Disks.

Step 2. Remove the LUN from any Disk Groups (if not raw disks).

Step 3. Remove the LUN from within the VI GUI.

Step 4. Delete the LUN mapping from the SAN array side.

Step 5. Create new LUN and mapping on the SAN array side.

Step 6. Rescan SAN ports.

Note: If you remove a LUN that is part of a disk group, your disk group will be invalid and must be deleted.

Before deleting a LUN, stop all virtual servers that are using that LUN (or the disk group that relies on that LUN).

Removing a LUN does not require you to restart the node.

Snapshotting LUNs

If you plan to use storage server features such as cloning and snapshots, use the raw storage model. Creating a snapshot of a LUN with logical disks causes duplicate entries to be created in VI-Center.

6

CREATING AND CONFIGURING VIRTUAL SERVERS

This chapter explains how to create and configure VDCs and virtual servers.

CREATING VIRTUAL DATA CENTERS

A virtual data center (VDC) is an administrative entity that consists of one or more managed nodes. Each VDC functions as a true data center—a group of nodes that have been segregated to meet specific business needs.

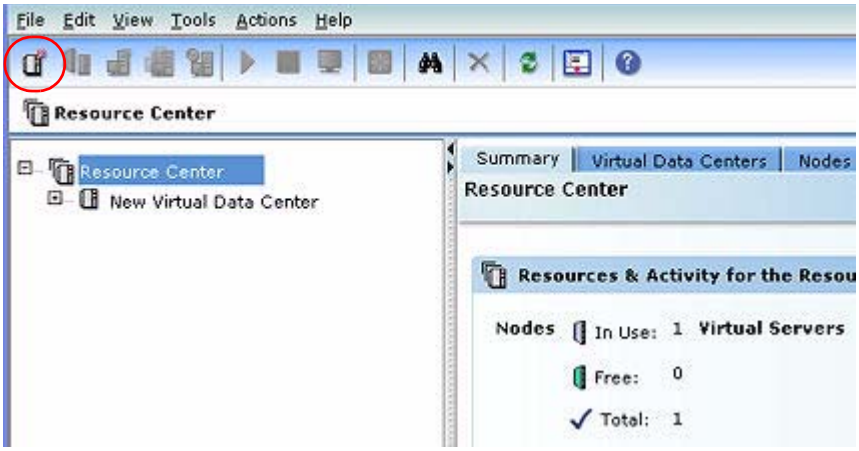
The hardware resources in each VDC are only available to the virtual servers hosted by them. In the same way, other VDCs function as a separate set of physical resources. The many VDCs into which you can separate all the nodes under management can be likened to the partitions into which a large computer might be divided.

VDCs are Containers for Virtual Servers

Before you create virtual servers, you need to create the VDC that will house them.

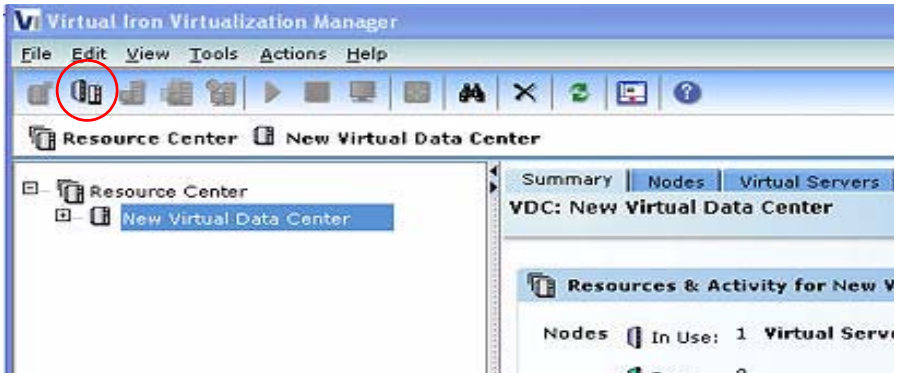
Step 1. In the **Resource Center** view, click the **Create New Virtual Data Center** icon as shown.

Figure 73. Creating a VDC



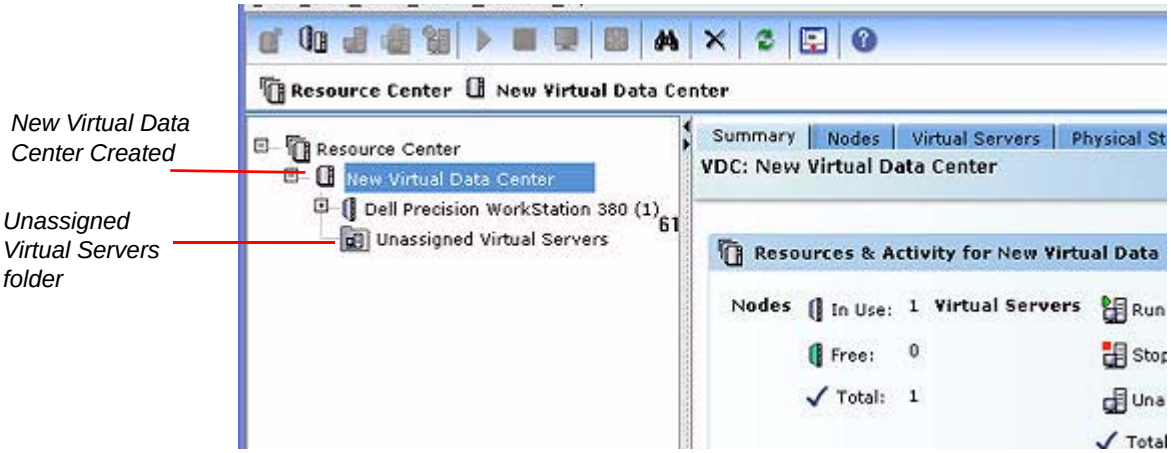
Step 2. The New Virtual Data Center appears in the navigation tree. While you perform this operation, yellow lock icons indicate that the object cannot be managed by other users.

Figure 74. VDC in Navigation Tree



Note that another folder called *Unassigned Virtual Servers* appears below the new virtual data center. This folder serves as storage area attached to a virtual data center. It is a place to move virtual servers that are shut down. It is also a staging area—a place to configure virtual servers for later deployment in the virtual data center. For more information, see VDCs and Unassigned Virtual Servers.

Figure 75. The Unassigned Virtual Servers Folder



ASSIGNING NODES TO VIRTUAL DATA CENTERS

Now that you have created a VDC, add at least one managed node to it.

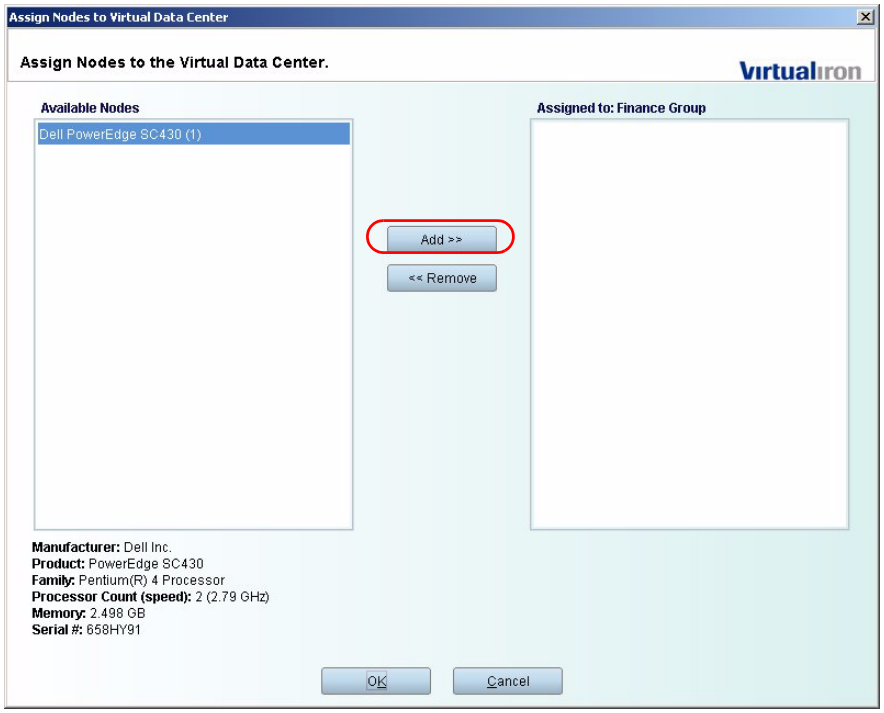
Step 1. To add nodes to the VDC, select its name in the navigation tree and click the **Assign Nodes** icon.

Figure 76. Assign Nodes Icon

Step 2. The **Assign Nodes** dialog opens with information about all nodes that have been discovered by the Virtual Iron® management server that are not assigned to another VDC. (See Creating Virtual Data Centers.)

To move the node to the VDC you have created, select the node and click **Add >>**. Then click **OK**.

Figure 77. Assigning Nodes to a VDC



The node moves from the Available Nodes to the Assigned Nodes pane. You can assign as many nodes as are available to a VDC. Keep in mind, however, that the ownership of a node by its parent VDC is absolute. A node can be used only by the virtual servers hosted in one VDC at a time; its physical resources cannot be shared by the virtual servers in any other VDC.

Step 3. After you assign a node to a VDC, information about the node appears in the **Summary** tab as shown in Figure 78. The node icon is green to show that it is **Free** for use within the VDC. Table 4 explains node states and their associated colors.

Figure 78. Node Summary Tab

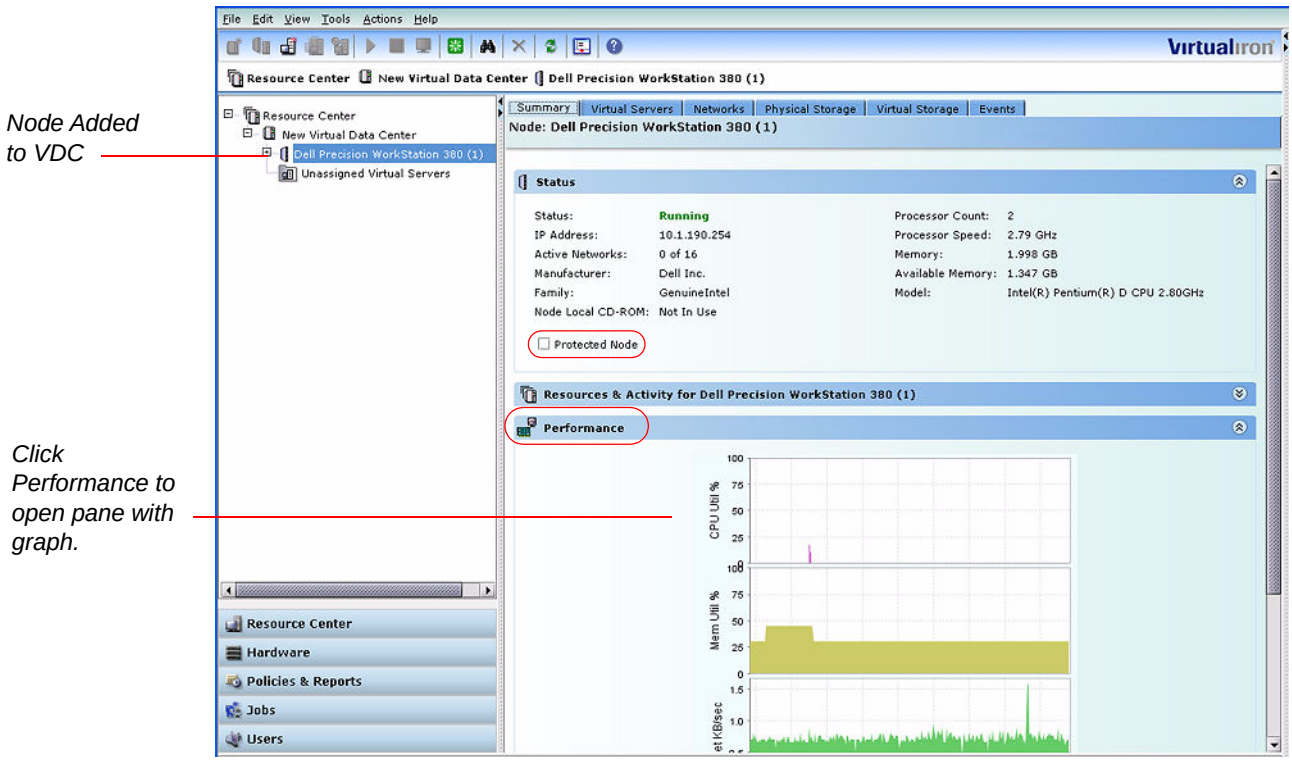


Table 4. Node States and Colors

	State	Meaning
Green	Free	Available for use within the VDC.
Gray	In Use	The node is hosting at least one virtual server.
Yellow	Warning	Warning messages have been received.
Red	Error	The node is in error.

Click the **Protected Node** check box if you do not want virtual servers to be moved to it from other nodes during LiveMigrate® See Figure 78. See LiveCapacity® for information on LiveMigrate®.

Click the **Display** check boxes to see node resources and activity or performance data.

VDCs and Unassigned Virtual Servers

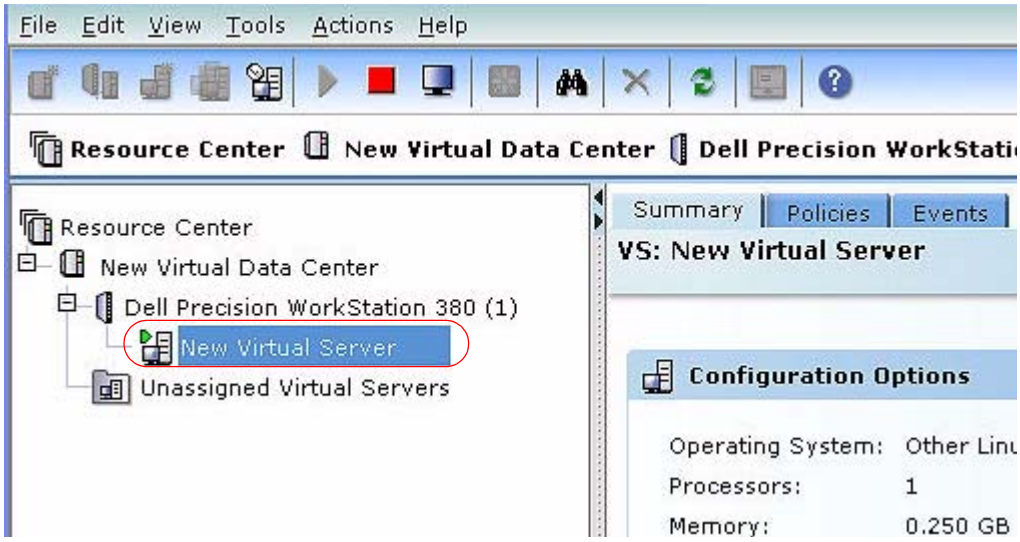
When you create a virtual data center, an **Unassigned Virtual Servers** folder is automatically created in the navigation tree. Use this folder to:

- Create and configure virtual servers for later deployment in the VDC
- Store virtual servers that are stopped, so that they do not use the memory associated with any node in the VDC
- Store virtual server clones

See. Figure 79.

Figure 79. Unassigned Virtual Servers Folder in Navigation Tree

.



About Unassigned Virtual Servers

Unassigned virtual servers are fully or partially configured virtual servers that are housed in a VDC, but do not consume any of that VDC's resources. Memory and processor parameters, network, and SAN access can be specified, but an inactive virtual server cannot be run until it is assigned to a node. At that time, its defined parameters are mapped to the node's resources.

Unassigned virtual servers are located in a separate folder at the bottom of each VDC. Once created, unassigned virtual servers can be dragged and dropped on a node within its parent VDC.

Configuring Unassigned Virtual Servers

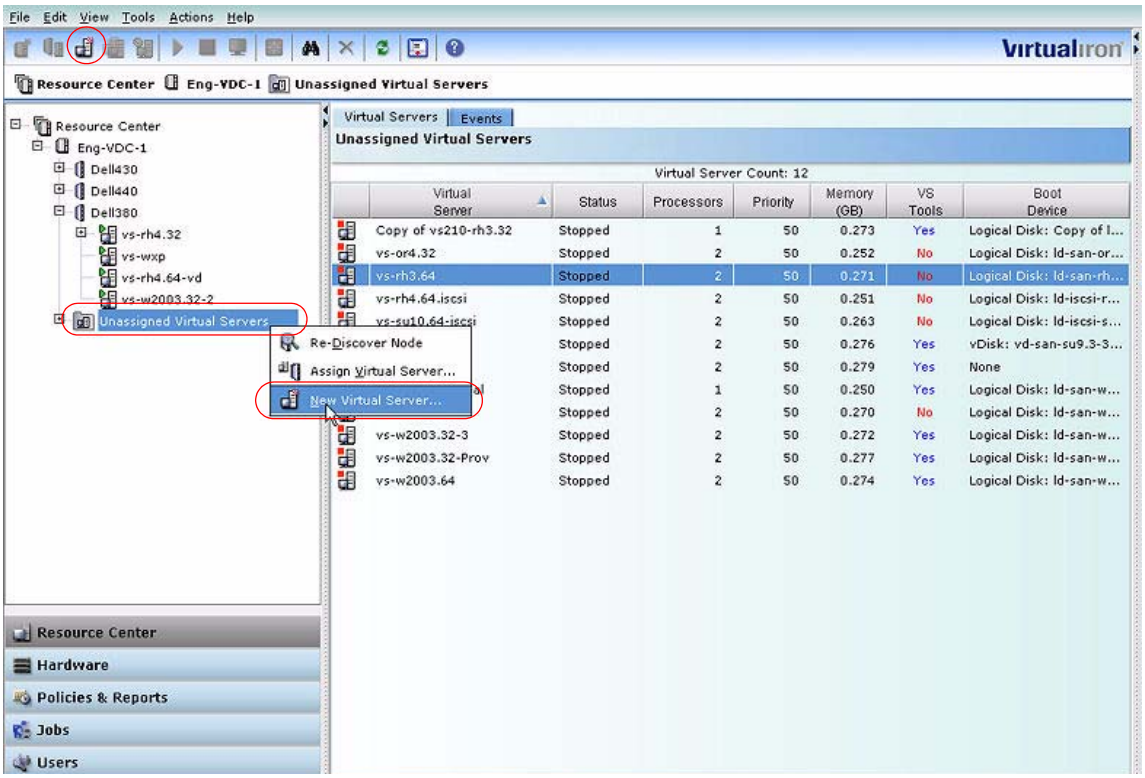
To configure an unassigned virtual server:

Step 1. Left-click the **Unassigned Virtual Servers** folder in the navigation tree to select it (see Figure 80). Then do one of the following:

- Right-click the selected icon and select **New Virtual Server**.
- Click the **Create New Virtual Server** icon in the action toolbar.

Step 2. Configure the virtual server: The New Virtual Server Wizard appears. Follow the steps outlined in Creating a Virtual Server.

Figure 80. Unassigned Virtual Servers

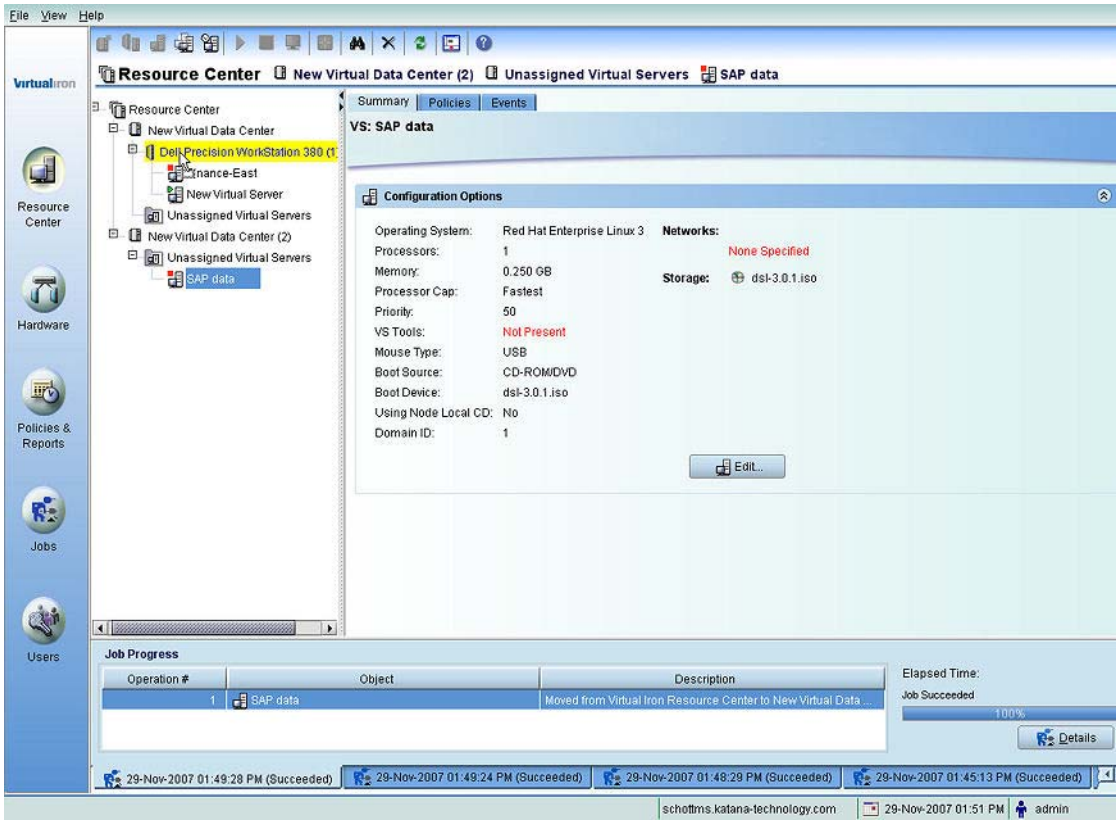


Deploying an Unassigned Virtual Server

After creating an unassigned virtual server, you can click and drag it to a node and start it. Figure 81 shows the unassigned virtual server *SAP data* being dragged to a node. Before the move is allowed, VI-Center checks:

- Memory and processing resources in the target node
- Access to OS (on network or SAN) from the target node

Figure 81. Moving an Unassigned Virtual Server to a Node



The virtual server begins using the memory and processors configured for it as soon as it is moved to a node. If the target node does not have enough processors or memory, the UI disallows the operation.

Moving Virtual Servers to Unassigned Folders

Use the **Unassigned Virtual Servers** folder to park virtual servers that are not currently in use. To run the virtual server, move it back to its original parent node and restart it. Or, reconfigure the virtual server, and then move it to a different node.

CONSERVING MEMORY

The storage capability provided by Unassigned folders is extremely useful. When a virtual server exists on a node, it is allocated and consumes a certain amount of that node's available memory, whether or not the virtual server is running. Moving a stopped virtual server to the Unassigned Virtual Servers area prevents the virtual server from using any node memory. All information associated with the virtual server is maintained.

To use the virtual server, simply move it from the unassigned area to a node with sufficient processing and memory resources, and start it.

VIRTUAL SERVERS

Make sure you have completed the following before you create a virtual server:

- Prepared nodes to be managed. See Managed Node Configuration.
- Cabled all nodes properly. See Site Preparation.
- Installed the Virtual Iron® software. See Installing Virtual Iron®.
- Established a connection to the Virtual Iron® management server.
- Defined connections between system nodes and physical networks. See Mapping Physical Ports to Logical Networks.
- Created a Virtual Data Center (VDC). See Creating Virtual Data Centers.
- Assigned a node to the VDC. See Assigning Nodes to Virtual Data Centers.

Once you complete these tasks, you have created the basis for virtualizing the resources of one or more nodes. All that remains is to create virtual servers.

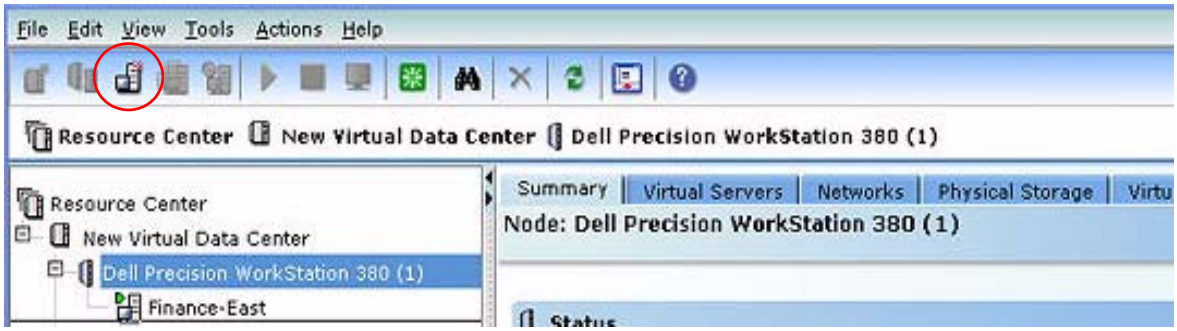
Note: If you are configuring a Windows Guest Operating System for your virtual server, and you wish to use more than 4 GB, you will need to add a "/PAE" switch to the boot.ini file.

Creating a Virtual Server

This procedure describes how to create, configure and deploy a new virtual server on a managed node.

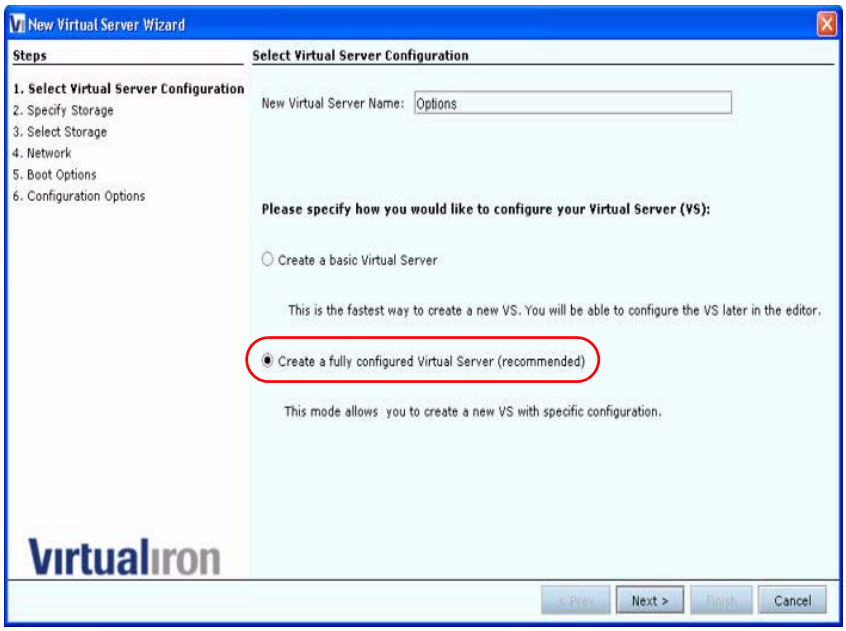
Step 1. Select the node you added earlier. Click the **Create Virtual Server** icon on the application tool bar.

Figure 82. Create Virtual Server Icon



Step 2. The new virtual server appears under **Unassigned Virtual Servers**, and the **New Virtual Server Wizard** appears. See Figure 83.

Figure 83. New Virtual Server Wizard



Step 3. Name the virtual server. In this example, the virtual server has been named Options.

The example shows the default setting, **Create a fully configured Virtual Server**.

NOTE: Choose **Create a Basic Virtual Server** to configure the virtual server later. Click its icon in the navigation pane. In the **New Virtual Server** window, click **Edit**.

Step 4. Click **Next**.

Step 5. Select or create storage for the virtual server. See Figure 84. For unconfigured systems, the default setting is **Create New Disks**.

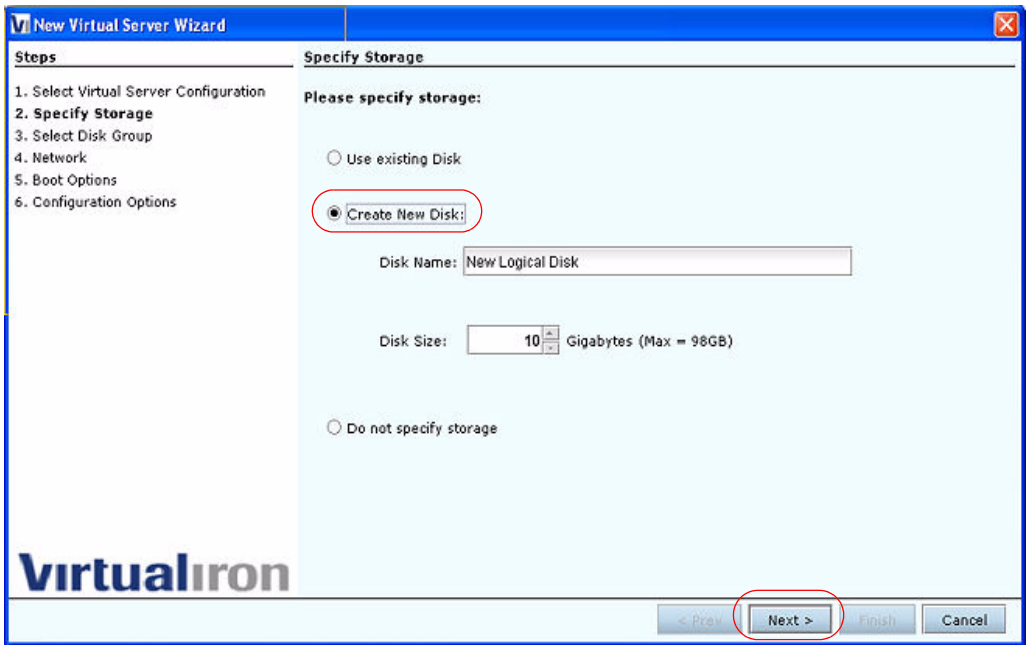
- If you have previously created logical disks, Use Existing Disk is the default. The next screen that appears displays the list of logical disks.
- If you select **Do not specify storage**, you can go back later to configure storage. Meanwhile, the virtual server just runs in memory. It will boot, but you can not run applications.

Step 6. Type a name for the new logical disk.

Step 7. Select a disk size from the pulldown menu. Default is 10 Gigabytes.

Step 8. Click **Next**.

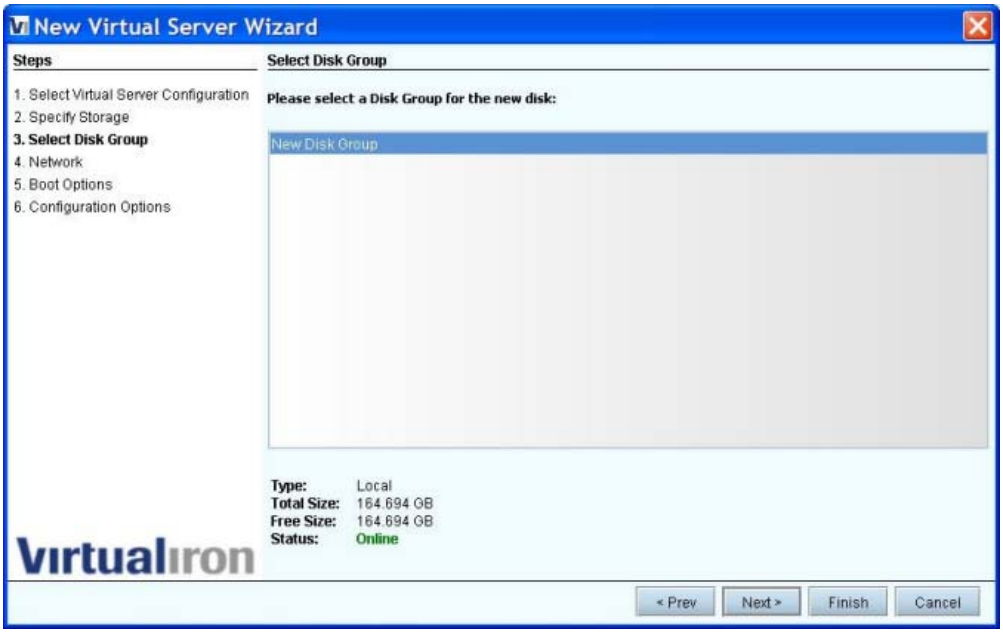
Figure 84. New Virtual Server Wizard: Specify Storage



Step 9. Select the disk group in which the newly created logical disk will be placed. See Figure 85.

Step 10. Click **Next**.

Figure 85. New Virtual Server Wizard: Select Disk Group



Configure network adaptors. Each network adapter consists of a virtual network identification card (VNIC), associated with an external subnet. You can add more than one VNIC to each virtual server, each allowing the virtual server to connect to and communicate with multiple networks. See Figure 86.

Note: You need to install VS Tools on an OS so the virtual server booting that OS can use more than one VNIC. See Installing VS Tools on Virtual Servers.

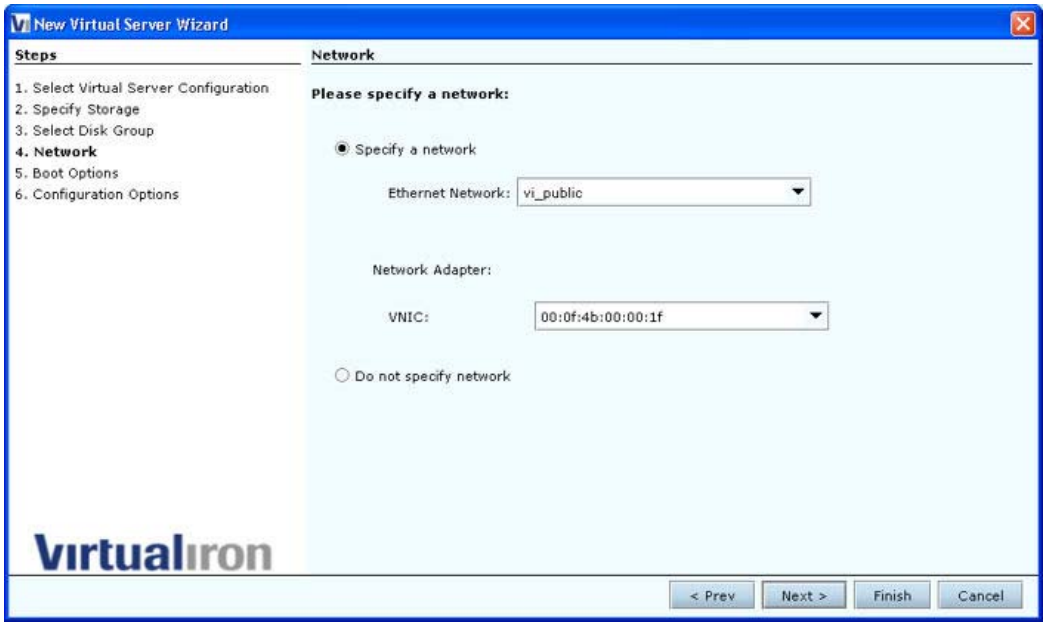
Step 11. Select an Ethernet network from the pulldown menu.

If you have not set up a network yet, select **Do not specify network**. You can set up the network later by clicking on the virtual server in the navigation pane and editing the virtual server.

Step 12. Select a VNIC from the Network Adapter pulldown menu to choose a specific VNIC from the drop-down list.

Step 13. Click **Next**.

Figure 86. New Virtual Server Wizard: Network



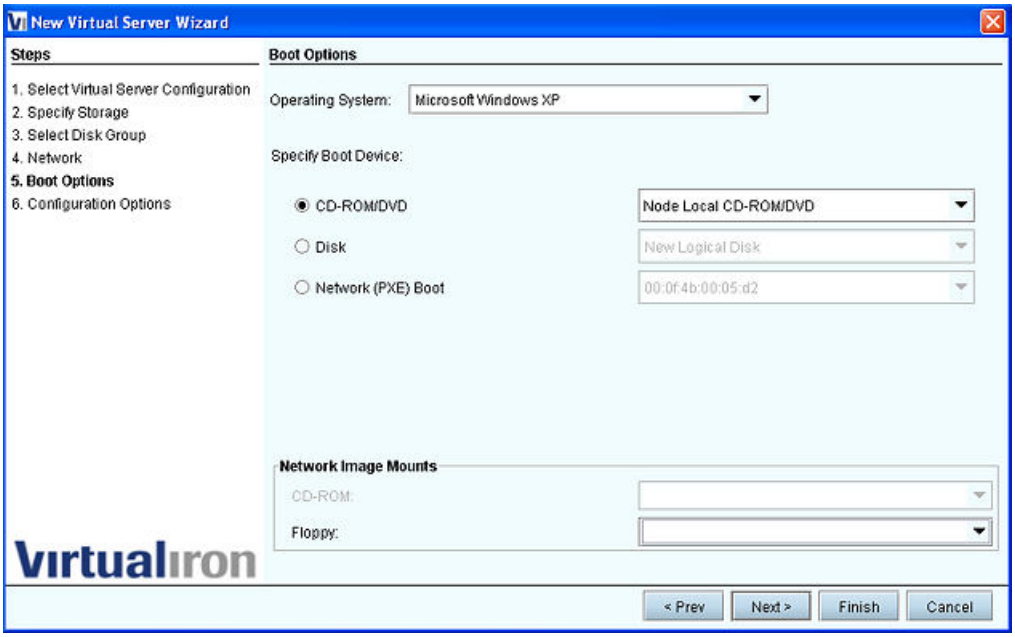
Step 14. Virtual Iron® enables virtual servers to boot over a SAN from a CDROM, or from a Network Boot Device. In the boot options window, select an operating system and then choose a boot method for the virtual server:

Note the following rules for physical CD-ROM/DVD boot options:

- Only virtual servers on the node on which the physical CD-ROM is located can use the physical CD-ROM.
- Only one virtual server at a time can use the physical CD-ROM.
- You can not associate more than one physical CD-ROM or ISO image with each virtual server.
- You can not have physical CD-ROMs *and* ISO images, or two ISO images, associated with a virtual server.

  - If you choose **CD/DVD**, select a specific drive if booting from a hard disk. This selection tells the virtual server to boot from the CD ROM device on the node where the virtual server is located. For example, if you are installing a Windows Operating System onto a logical disk, as in Figure 87, select Microsoft Windows XP for the operating system. You will need a Microsoft Windows XP CD and license key later, when you install Windows onto a logical disk that you specify.

Figure 87. New Virtual Server Boot Options:



- If you choose **CD/DVD** and specify to boot from an .iso file listed in the pulldown menu, the virtual server will boot from the .iso file on the node where the virtual server is located. See Figure 88. You can associate any of those applications to any virtual server. On Linux, ISO images are located in

  /opt/virtualiron/nbd

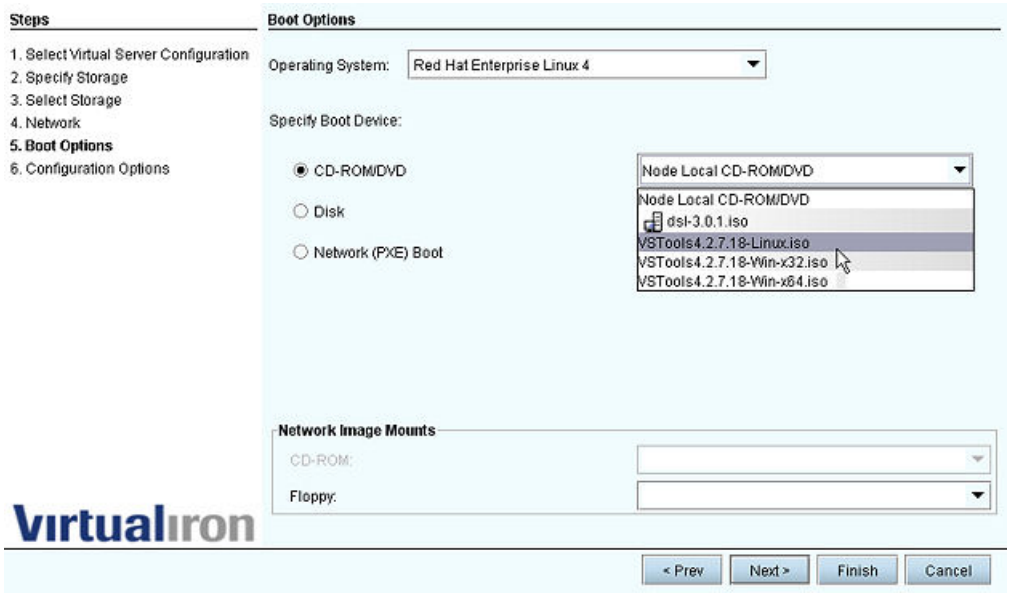
  On Windows™, they are located in

  C:\Program files\VirtualIron\nbd.

  See Figure 88.

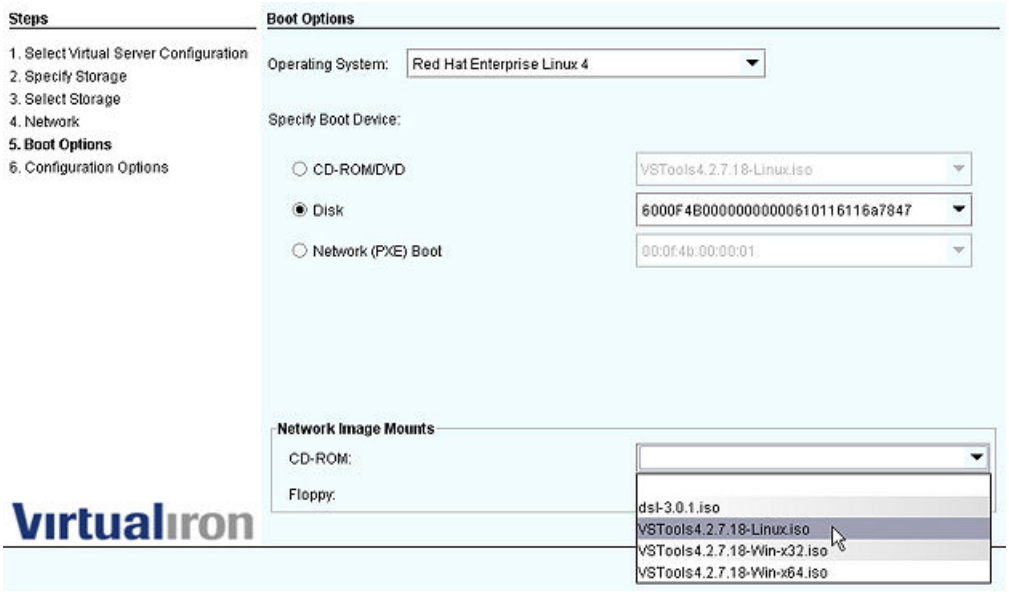
- If you also want a floppy associated with this virtual server, in **Network Image Mounts**, specify the **Floppy** from the pulldown menu.

Figure 88. New Virtual Server Wizard: .iso Boot Option



- Choose **Disk** to boot from the logical disk or SAN assigned as the boot device for the virtual server.
- If you also want a CD-ROM or floppy associated with this virtual server, in **Network Image Mounts**, specify the .iso file from the pulldown menu. See Figure 89. You can have one CD total and one floppy total.

Figure 89. New Virtual Server Wizard: Network Image Mounts



- Choose **Network PXE Boot** to PXE boot the virtual server from a public network. If you boot off a PXE, you can have one CD total and one floppy total.

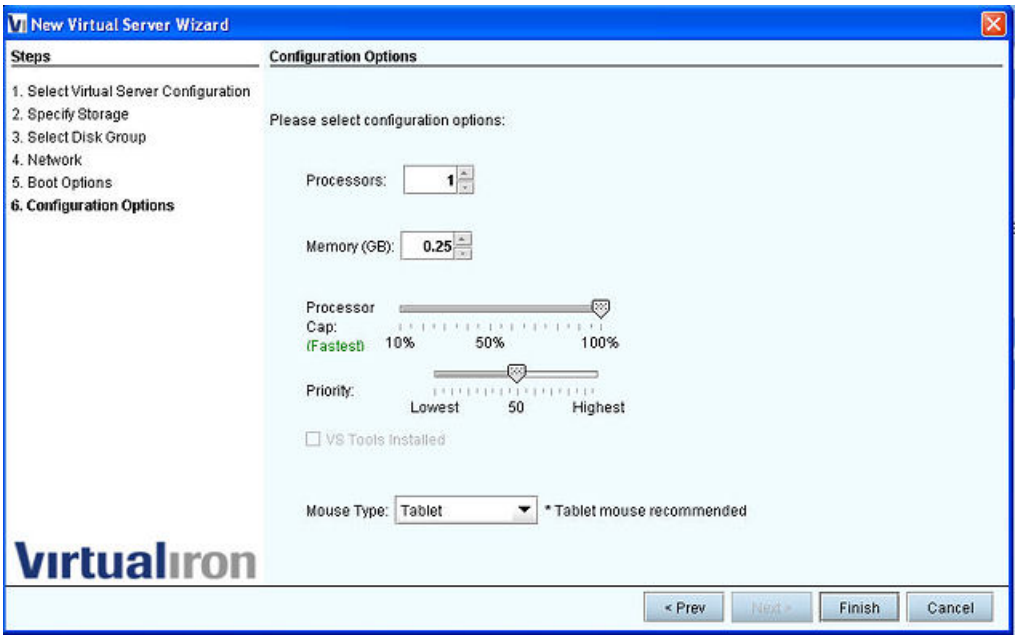
  You will not be able to configure a LUN unless you have configured SAN access and designated a boot disk, as described in Discovery and Management of Physical Disks.

Note: See Installing VS Tools on Virtual Servers to install VS Tools on an OS. A specific set of VS Tools are shipped for each guest OS supported by Virtual Iron. For enhanced performance and statistics gathering, Virtual Iron® strongly recommends that you use VS Tools.

Step 15. Click **Next**.

Step 16. Configure the number of processors and the amount of node memory allocated to the virtual server, and schedule the priority of this virtual server in relation to others running on the same managed node. See Figure 90. Each of the options is described below.

Figure 90. New Virtual Server Wizard: Configuration Options



- **Processors**—Configure the number of processors you want the virtual server to use. Note that multiple virtual servers can share the CPUs available on a managed node. If two virtual servers are running on the same node, you can assign two processors to each of them. Virtual Iron® time-shares available processors among the virtual servers in a manner that is transparent to all of them. Default for Processors = 1.

- **Memory**—Specify the amount of memory to be allocated to this virtual server. Unlike processors, memory is not shared among virtual servers, and cannot be oversubscribed. For example, if Virtual Servers A, B, and C are created on a managed node with 3 GB of memory, and A and B are each allocated 1 GB of memory, C can only be allocated up to 1 GB of memory. If the memory allocations of either A or B (or both) are reduced, C's allocation can be increased commensurately. To determine how much memory is available on a node, consult the node's Virtual Server tab. The default for memory = 256MB (.25 GB).
- **Processor Cap**—The cap optionally fixes the maximum amount of CPU that can be consumed, even if the host has idle CPU cycles. Use the cap to keep low priority virtual servers from consuming too many cycles on a node.

Note: The virtualization services component running on a managed node consumes a small amount of memory. For this reason, the memory available to virtual servers running on a node is below the total memory available on that node.

- **Priority**—If more than one virtual server is running on the same managed node, use the **Priority** setting to give highest priority to one virtual server, and less (or equal) priority to others. Priority levels determine which virtual server is allowed to run first, in the event two are contending for the same physical processors. Set the Priority for a virtual server from lowest (1) to highest (100). Default for Priority = 50.

Note: To improve performance, If you are mixing iSCSI-based virtual servers with SAN or local disk virtual servers, set the priority of the CPU on the iSCSI virtual server higher than the SAN or local disk virtual server's priority.

- **VS Tools Installed**—Check **VS Tools Installed** if you have installed the VS Tools package on the OS, and you wish to use VS Tools. A specific set of VS Tools is shipped for each guest OS supported by Virtual Iron®. Before enabling VS Tools for a guest OS, read Installing VS Tools on Virtual Servers and follow the installation instructions for Windows® or Linux.
- **Mouse type**—Depending on the operating system you specified earlier, **Tablet**, **PS2** or **USB** is set as the default.

CLONING VIRTUAL SERVERS

Cloning creates a copy of a virtual server. The cloned virtual server has the same processing, memory, and other characteristics of the original virtual server, and has created clones of the logical disks assigned to the original. However, cloned virtual servers are not exact replicas of their originals; the cloning operation assigns a new VNIC to the clone (rather than the VNIC used by its parent).

VI-Center does not allow you to move a cloned virtual server to a VDC unless the VDC has access to the networks or storage configured for that virtual server.

The virtual server clone is automatically placed in the **Unassigned** folder of the VDC containing the original virtual server. To start the virtual server, move it from Unassigned to a VDC with sufficient memory to accommodate its needs.

Before cloning a virtual server:

- Stop the virtual server. Running virtual servers cannot be cloned.
- Assign a guest OS to the virtual server.
- Make sure the virtual server is not assigned to a local disk or raw disk.

Preparing a Windows Virtual Server for Cloning

Use the Windows utility *sysprep* to prepare a Windows virtual server for cloning. Computers running Windows operating systems have a Security ID (SID) that uniquely identifies the computer or domain, and user. When you clone a Windows virtual server, it is important to ensure that duplicate SIDs are not created.

Sysprep personalizes the cloned computer with characteristics you provide. At the same time, it modifies the local computer SID to make it unique to each computer.

PRIOR TO CLONING WINDOWS VIRTUAL SERVERS

Step 1. Create, install, and configure the Windows virtual server as desired.

- If the virtual server you are cloning has storage disks, the clone option displays a dialog box with options for cloning the disks.
- If the virtual server does not have storage, you will not see the dialog box.

Step 2. Apply all relevant Windows service packs and updates.

Step 3. If you have not done so already, install VS Tools. See Installing VS Tools on Virtual Servers.

Step 4. Install desired applications and apply settings as needed.

Step 5. Copy the contents of

\support\tools\deploy.cab

from the Windows product CD to a new \sysprep folder in the virtual server.

Step 6. Create an answer file with setupmgr.exe.

Step 7. Run sysprep. This shuts down the virtual server when it completes.

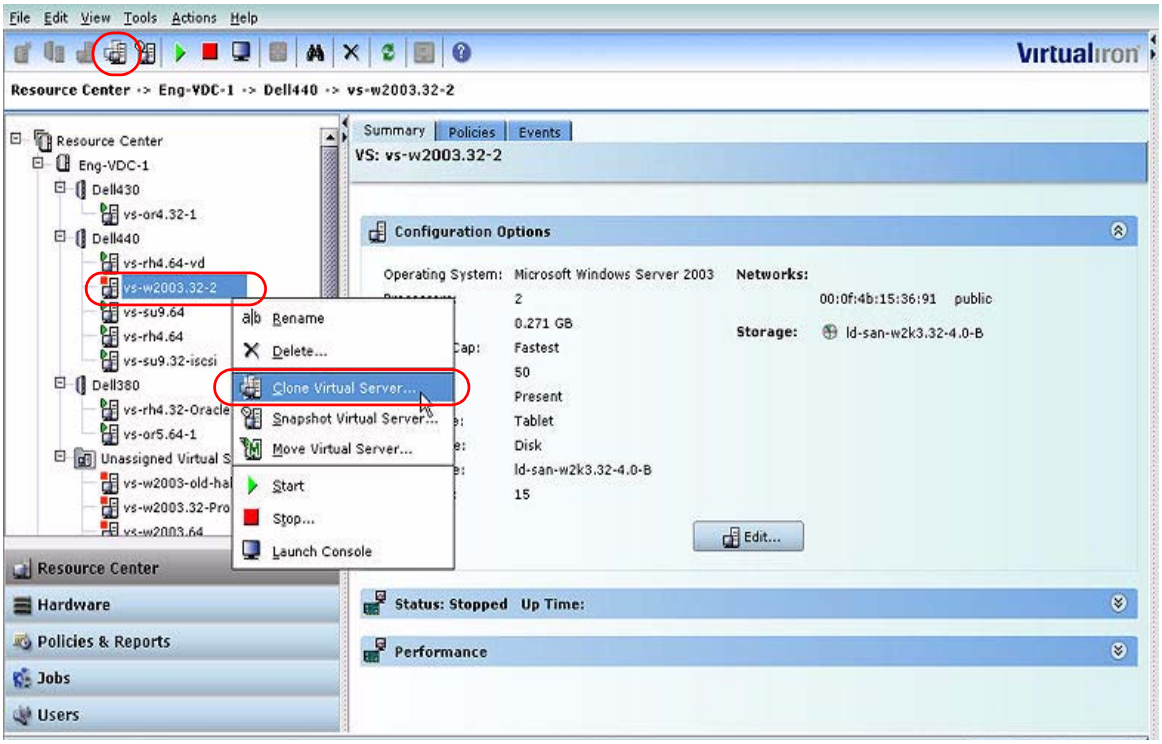
Step 8. Clone the newly created template into new virtual servers as required.

Cloning a Virtual Server

Step 1. In the **Resource Center** view, select the virtual server in the navigation tree, right-click and select **Stop**, or click the **Stop** icon.

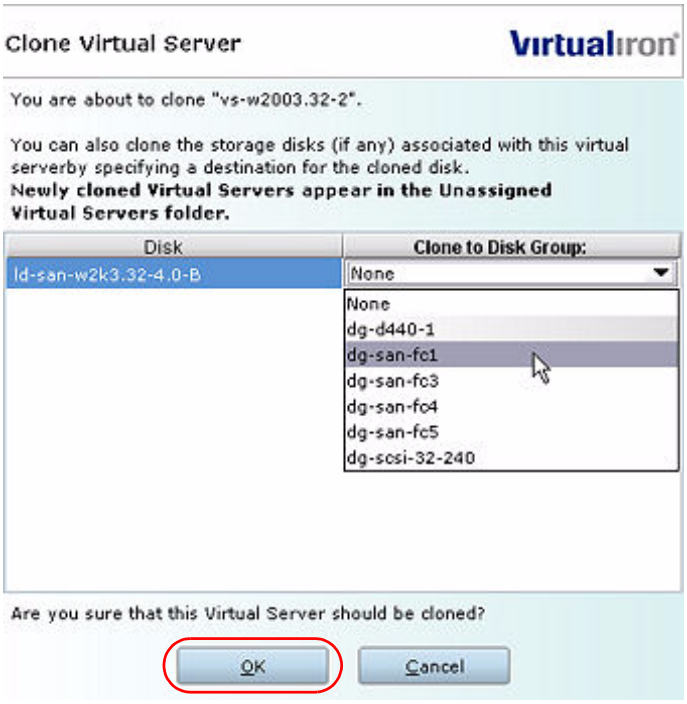
Step 2. Right-click the stopped virtual server and select **Clone Virtual Server** or click the **Clone** icon. See Figure 91.

Figure 91. Clone Virtual Server Icon and Menu Option



Step 3. The dialog box shown in Figure 92 appears. If you also want to clone specific storage disks associated with the virtual server, select the storage disk(s) and specify a destination from the pulldown menu. Otherwise, choose **None** from the pulldown to clone only the virtual server.

Figure 92. Clone Virtual Server Dialog Box

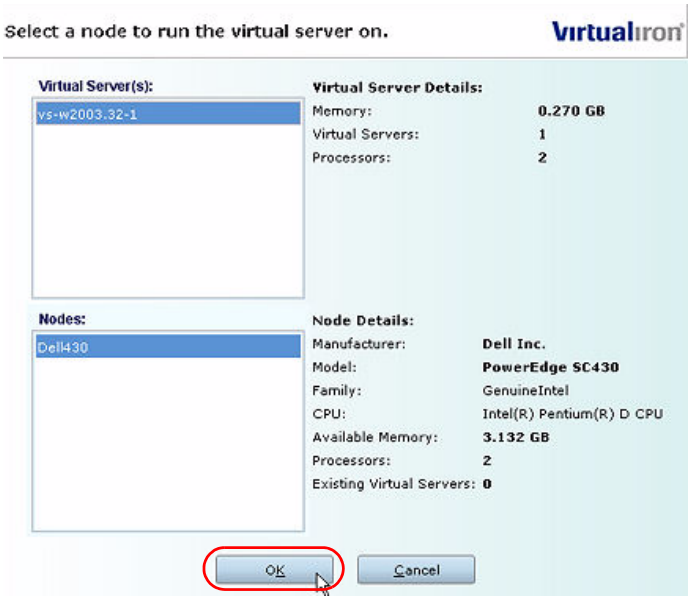


Step 4. The cloned virtual server appears in the **Unassigned Virtual Servers** folder of the VDC. By default, the cloned virtual server is labeled **Copy of (virtual server Name)**.

Step 5. The cloned virtual server has all the configuration characteristics of the original. To run the virtual server, you can do one of the following:

- Drag and drop it back to its original parent node and restart it. See Deploying an Unassigned Virtual Server.
- Right-click the virtual server in the Unassigned Virtual Servers Folder to bring up the dialog box shown in Figure 93, which shows all nodes with sufficient space to accommodate the cloned virtual server.
- Reconfigure the virtual server, and move it to a different node.

Figure 93. Select a Node for Cloned Virtual Server



VIRTUAL SERVER SNAPSHOTS

The virtual server Snapshot feature is useful for patch management and backups. Once you have set up a virtual server, assigned storage to it, and are running the virtual server, there are cases when you may want to preserve its current state.

In the case of patch management, for example, you might want to apply a code patch to a virtual server. If you are unsure whether the patch will be successful or could negatively affect your applications, you can select the virtual server and create a snapshot of it. You now have a new virtual server, configured exactly the same as the original, with a snapshot copy of the storage that the original virtual server was using.

If you have high confidence in the patch, you can apply it to your virtual server; if you have low confidence, you can apply it to your snapshot virtual server. In either case, if the patch fails, you can delete the affected virtual server and have a copy that is ready to go in its place.

With backups, you might have a policy specifying that your virtual servers and their data are backed up at regular intervals. Since you cannot clone or export a virtual server when it is running, you can instead use the Snapshot feature. Once you Snapshot the data, you can use Export to pull the data out to a disk for restoring later. See also Snapshots And Disk Space Usage.

For information on starting or stopping the Snapshot policy, see Virtual Server Snapshots.

OPERATIONAL CONSIDERATIONS

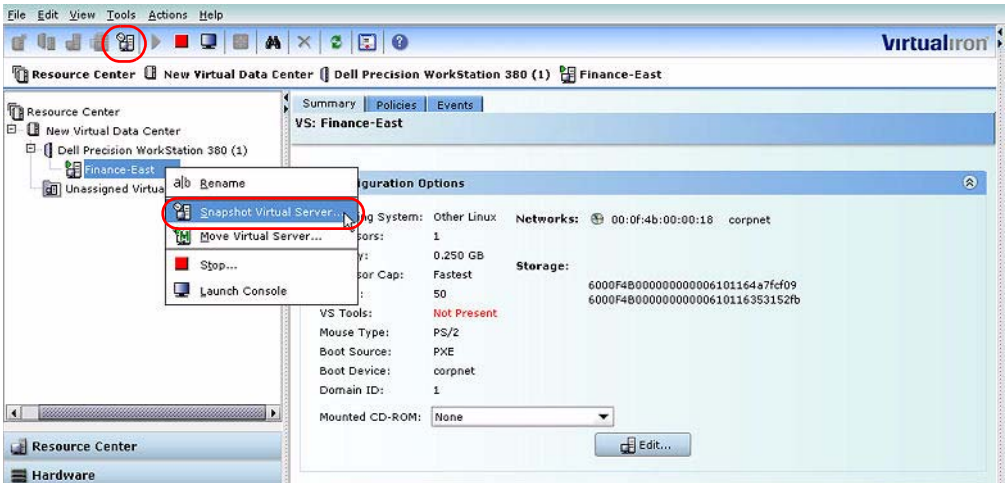
Once you have created a virtual server snapshot, observe these operational considerations.

- A snapshot virtual server can be stopped, started, renamed, cloned, and deleted.
- When you take a snapshot of a server with multiple disks, you get a snapshot of *all* the disks.
- A snapshot virtual server *cannot* be moved off the node where the parent virtual server resides—can not use LiveMigrate.

Creating a Snapshot of a Virtual Server

Step 1. Select a virtual server in the Resource Center and either click the **Snapshot** icon in the toolbar or right click and select **Create Snapshot** from the menu. See Figure 94.

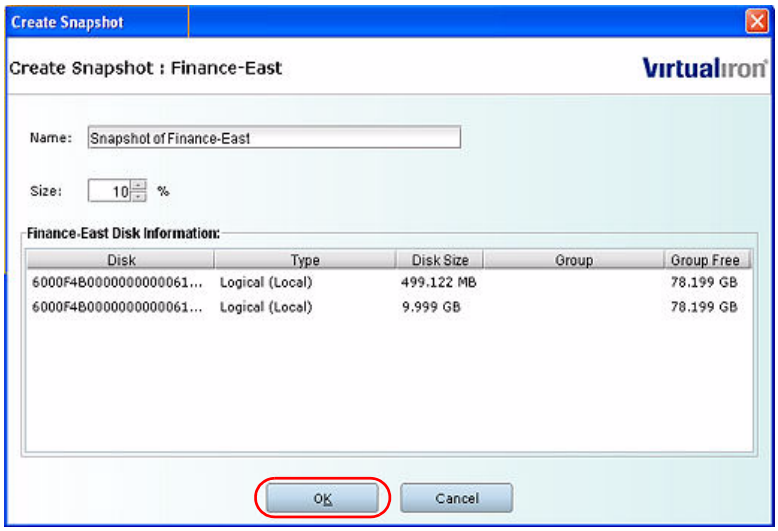
Figure 94. Snapshot Icon and Menu Selection



Step 2. In the **Create Snapshot** window, enter a percentage for **Size**. This is the initial percentage of space to be allocated for snapshot storage. The default is 10%. When half of this allocated free space on the snapshot logical disk is consumed as a result of subsequent writes to the disk, the space utilization is dynamically increased by enough space to keep the storage used at 30%. The system issues warning events and the snapshot disk icon changes to yellow.

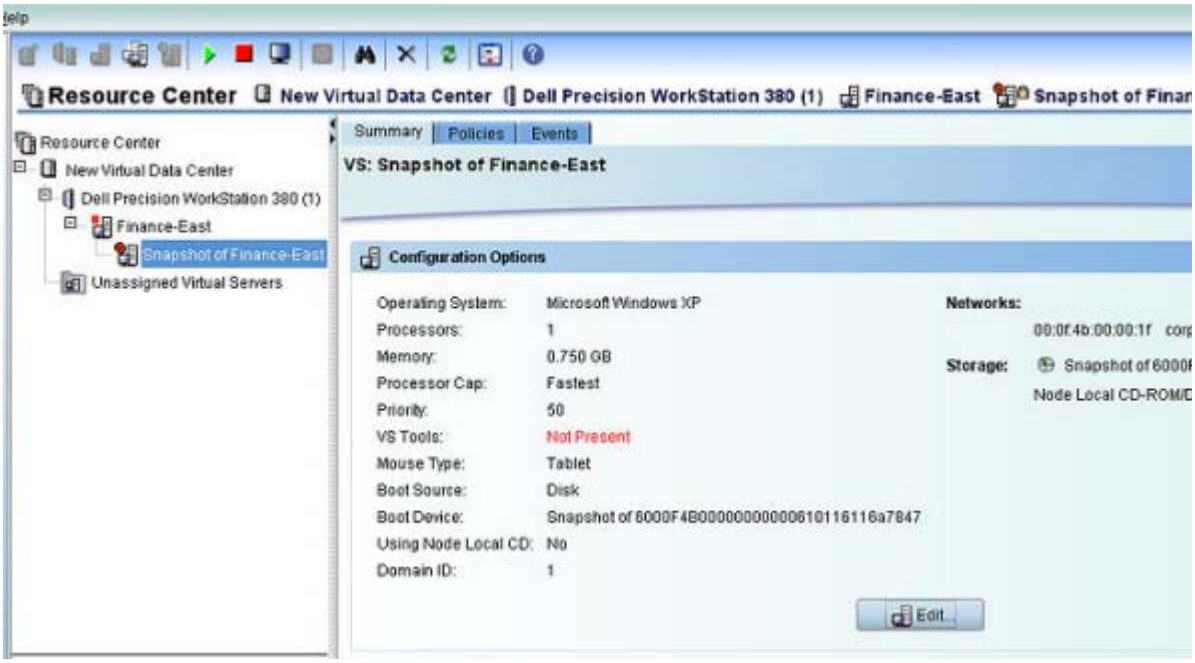
See Virtual Server Snapshots.

Step 3. Click **OK**.



The snapshot of the virtual server appears in the navigation tree and the **Storage** section of the Summary window. See Figure 95.

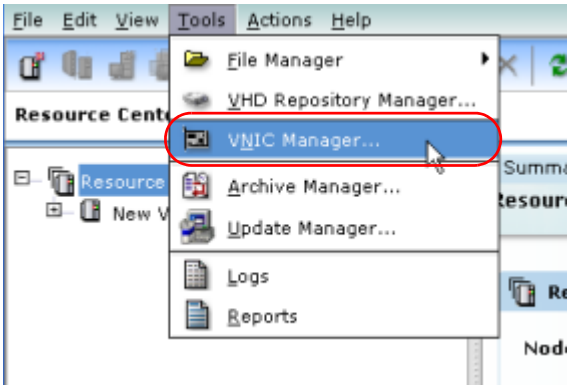
Figure 95. Virtual Server Snapshot in Navigation Tree and Summary Screen



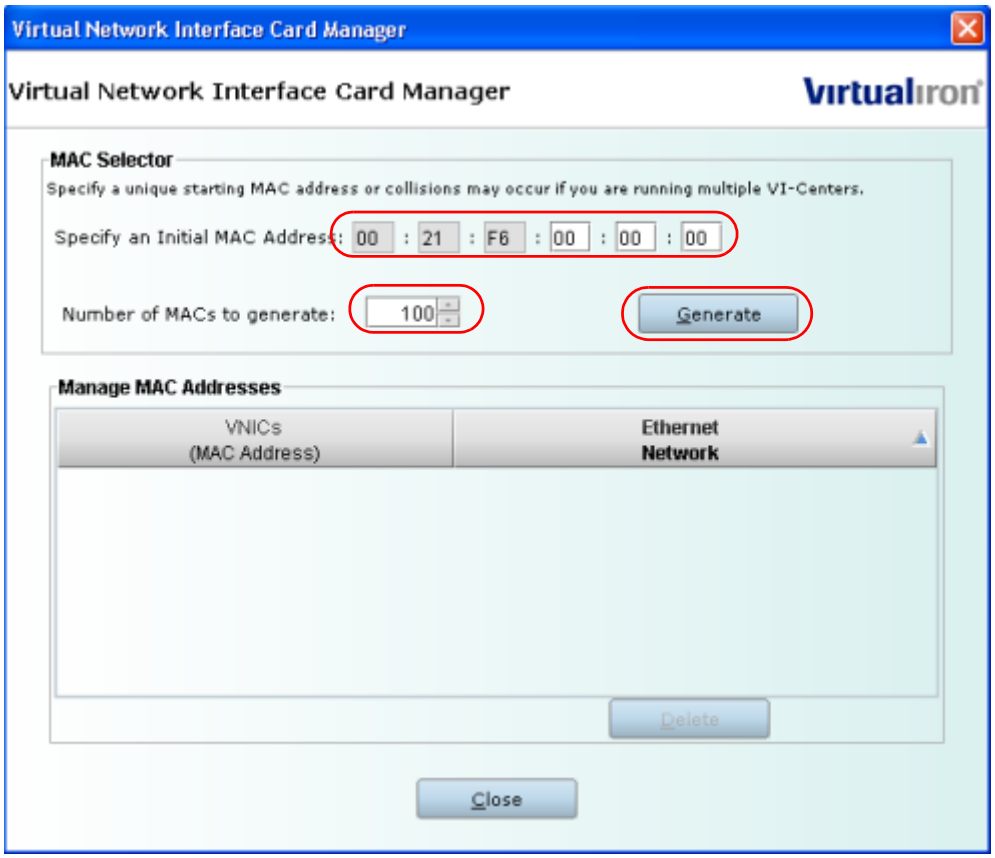
Creating a Virtual NIC

Before you can create a virtual server, you must have at least one MAC address. You can create an unlimited number of VNICs using the VNIC Manager available in the Tools menu. The VNIC Manager allows you to manage your VNICs over a range of MAC addresses.

Step 1. In the VI-Center click Tools, VNIC Manager.



Step 2. The VNIC Manager appears.



Step 3. Set the number of VNICs you want to create in the Number of MACs to Generate field.

Step 4. If you want, specify the first in the series of MAC addresses you want by editing the numbers in the last three boxes of the Specify an Initial MAC Address field.

Step 5. Click Generate.

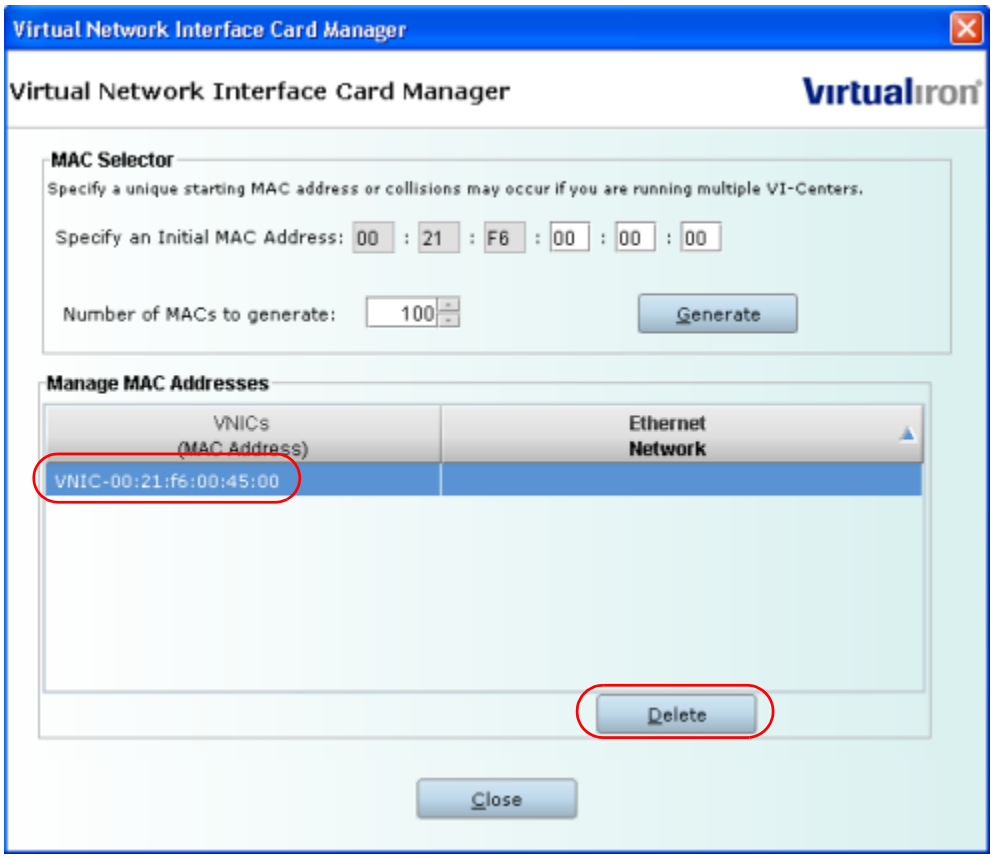
Step 6. The new VNICs appear in the bottom of the dialog.

Step 7. Click Close to exit the VNIC Manager.

Deleting a Virtual NIC

Step 1. Click Tools, VNIC Manager.

Step 2. In VNIC Manager, select the VNIC you want to delete.



Step 3. Click Delete.

INSTALLING A GUEST OS

You can install an operating system and applications to a virtual server's disks the same way you would on a physical server. Use a physical CDROM (and the installation media provided by your operating system provider) or a network .iso image. If you prefer using .iso images, you can copy them to the NBD directory on the management server and boot using that method. For storage, use either a raw SAN LUN or a logical disk.

Installing an OS from a CDROM involves:

- Creating a virtual server, and moving it to a managed node that:
  - Contains a CDROM drive or has access to an ISO image of the installation.
  - Is connected to the disk on which you intend to install the OS.
- Starting the virtual server.
- Installing the OS on a specific disk, using your OS's installation program.

Use the following steps for any supported operating system.

Step 1. Within VI-Center, create a virtual server.

Step 2. Drag and drop this virtual server to a managed node with a CDROM drive. Choose **CD-ROM/DVD** as the boot option for the virtual server. Do not enable VS Tools.

If you are using an .iso image, you can use a node with or without a physical CD-ROM drive.

Step 3. Create a logical group and logical disk on the managed node. Then assign the logical disk to the virtual server.

- See Configuring Logical Disks for instructions on creating a disk group and logical disk.
- See Virtual Servers for instructions for assigning a logical disk to a virtual server.

Step 4. Disregard this step if you are using a network .iso image:

Insert OS installation Disk 1 in the managed node in which you intend to run the virtual server. Note that this node must be connected to the disk to which you intend to install the OS.

Step 5. Start the virtual server. This begins a standard installation from the CD.

Step 6. Open a virtual server console as explained in Launching a Virtual Server Console. The OS installer takes you through available options. If installing Red Hat, or SUSE without networking, continue to the next section.

If Installing SUSE Linux Using a Network Installation...

When prompted for installation components, do the following:

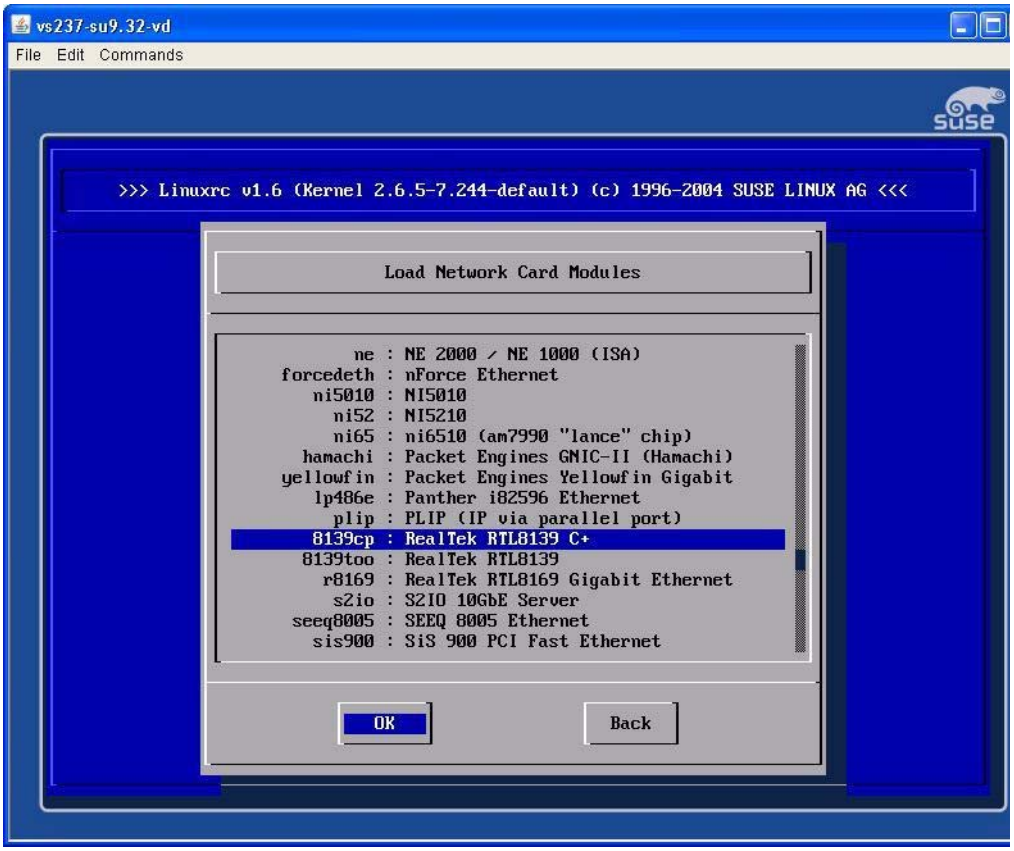
Step 1. Choose **Kernel Modules (Hardware Drivers)**

Step 2. Choose **Load Network Card Modules**

Step 3. Select this driver: **rt18139_cp**

This emulated network driver is included in the Virtual Iron Services layer. Figure 96 shows selection of this driver in the context of a SUSE installation.

Figure 96. Choose Hardware Driver, SUSE Linux Installation



Step 4. Continue the installation according to the instructions in your installation program.

Step 5. When the installation program completes, it instructs you to reboot. *Before you reboot*, in VI-Center, select the virtual server and click **Edit** to change the virtual server boot option to **Disk Device**. See Figure 98 for an example of the Edit window. Do **not** enable **VSTools Installed**.

Step 6. Reboot the OS as prompted by the installer. The virtual server boots from the disk you specified.

INSTALLING VS TOOLS ON VIRTUAL SERVERS

Virtual Iron® provides VSTools for use by guest operating systems. VSTools provide increased performance and a set of enhanced capabilities:

- Accelerated network and storage block drivers
- The collection of virtual server statistics
- Control of virtual servers (shutdown/restart)
- LiveMigration™ of virtual servers

To make use of these capabilities, install VS Tools on the disk from which the guest OS is booted.

Note: If VSTools are not provided for the kernal you are using, you can build VSTools. For instructions, see the Readme file located in the srpms directory in VSTools.

Installing VS Tools on Linux Virtual Servers Using a Browser

Virtual Iron supports the base kernel as shipped and the latest security kernel. While the use of VS Tools is optional, Virtual Iron® strongly recommends that you install the VS Tools package on the OS disk.

To copy and install VS Tools for a Linux virtual server, do the following:

Step 1. Determine the kernel you are using by entering the uname -a command.

Step 2. Go to the VSTools directory:

/opt/VirtualIron/VirtualizationManager/system/vstools/rpms

Step 3. Locate the appropriate rpm kit in the list.

- It is important to select only the 32- or 64-bit rpm associated with the OS.
- Note that the RPM kit files are release-dependent, as shown in the following example, where x.x.x-yy represents the release:

virtualiron-2.6.5-7.244-bigsmp-x.x.x-yy.i386.rpm

Step 4. Copy the appropriate rpm kit from the management server to the virtual server.You can do this from the virtual server console. In this example, the rpm is being copied from the management server (10.1.3.6) to the virtual server (vs037).

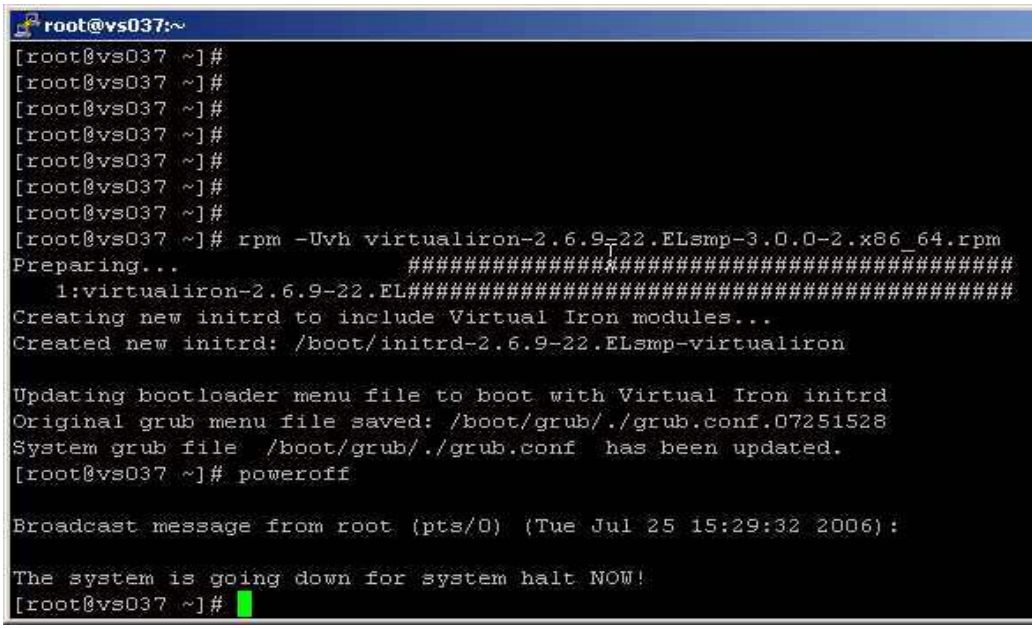
[root@vs037 ~]# scp 10.1.3.6:/opt/VirtualIron/VirtualizationManager/system/vstools/rpms/virtualiron-2.6.9-22.ELsmp-x.x.x-yy.x86_64.rpm.

Step 5. Install the VSTools package on the virtual server, using an rpm command as follows:

```
# rpm -Uvh <rpm kit>
```

A sample of the installation of the rpm for Red Hat Linux (64 bit) is shown in Figure 97.

Figure 97. Sample Installation of RPM Kit

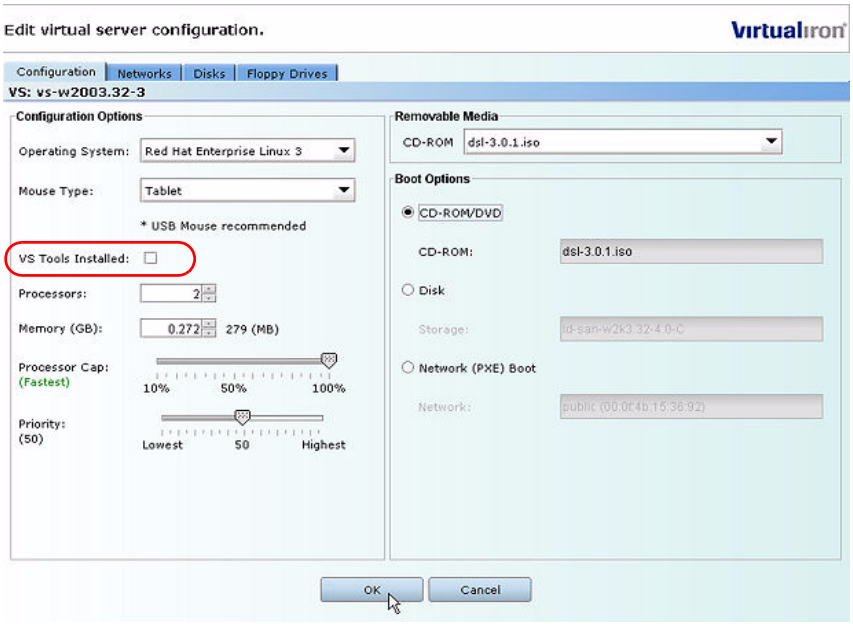


Note: VS Tools for RH3 have separate RPMs for Intel and AMD processors. The RPM you install in a virtual server must match the processor type (Intel or AMD) of the node (physical server) on which the virtual server is installed. Name these virtual servers, since they will only run on that processor type from that point forward.

Step 6. After installing the rpm, power off the virtual server from the console as shown in Figure 97.

Step 7. Open the **Edit Virtual Server Configuration** window in VI-Center. Check **VS Tools Installed** for the virtual server as shown in Figure 98. Click **OK**.

Figure 98. Enable VSTools for a Virtual Server



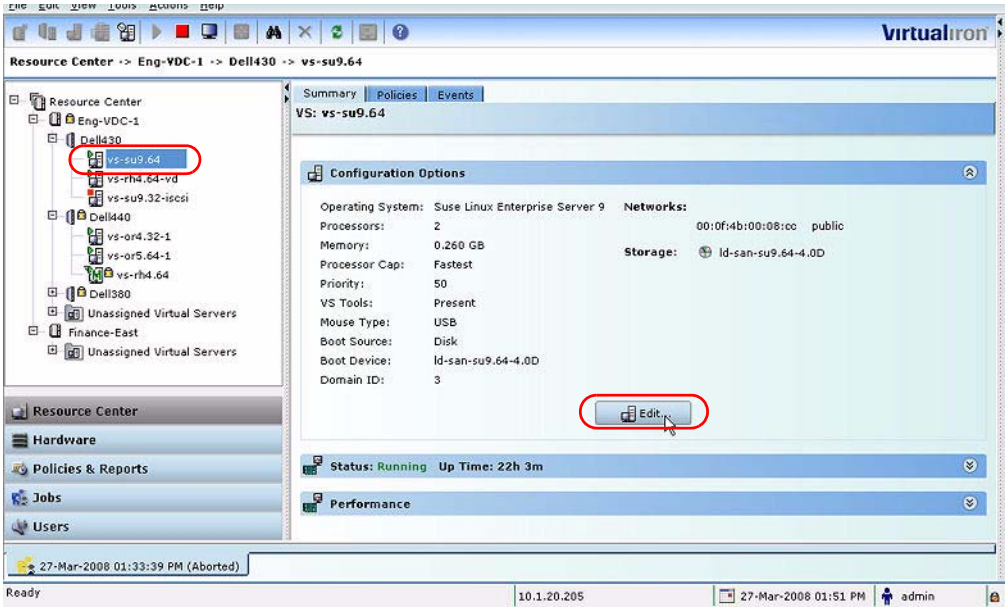
Step 8. Start the virtual server as described in Installing a Guest OS. Open a virtual server console and observe the boot process. When the virtual server starts, it will boot the VS Tools package you installed, as shown in Figure 101.

Installing VS Tools on Linux Virtual Servers Using ISO Images

Step 1. In the **Resource Center**, select the virtual server.

Step 2. In the Summary screen, click the **Edit** button as shown in Figure 99.

Figure 99. Selected Virtual Server Summary Screen

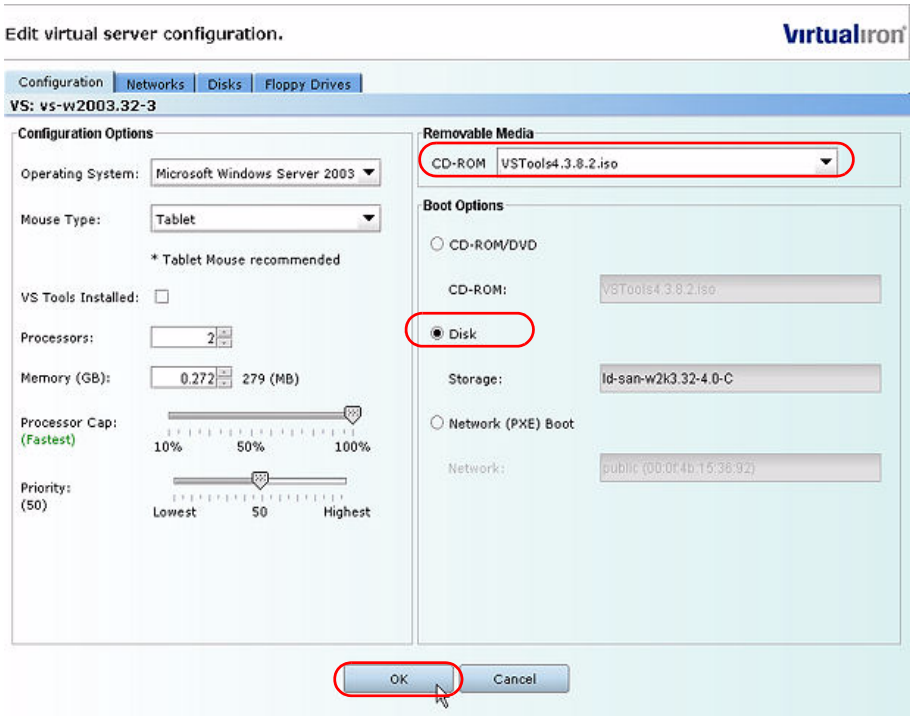


Step 3. In the Edit Virtual Server Configuration screen, select the VSTools .iso file from the **Removable Media** CDROM pulldown list.

Step 4. Click the **Disk** radio button.

Step 5. Click **OK** to add the .iso file. See Figure 100.

Figure 100. Select VSTools .iso File



Step 6. Click the **Start** icon and wait for the virtual server to start.

Step 7. Click the **Console** icon in the VI-Center action toolbar and login to the console.

Step 8. If the CD-ROM is not automatically mounted, enter the following:

```
mount /dev/hdd /cdrom
```

Step 9. Locate the appropriate rpm kit in the list. If no appropriate kit exists, compile using the SRPM. For supported guest operating systems (see GOSs Supported On Virtual Servers), use the SRPM package. For guest operating systems that are not supported, use either the SRPM or the compressed .tar file. Refer to the README file in the SRPM directory.

- It is important to select only the 32- or 64-bit rpm associated with the OS.
- Note that the RPM kit files are release-dependent, as shown in the following example, where x.x.x-yy represents the release:

```
virtualiron-2.6.5-7.244-bigsmp-x.x.x-yy.i386.rpm
```

Step 10. Install the VSTools package on the virtual server, using an rpm command as follows:

```
# rpm -Uvh <rpm kit>
```

A sample of the installation of the rpm for Red Hat Linux (64 bit) is shown in Figure 97.

Step 11. After installing the rpm, power off the virtual server from the console as shown in Figure 97.

Step 12. Open the Virtual Server boot options window in VI-Center. Check **VS Tools Installed** for the virtual server as shown in Figure 98. Click **OK**.

Step 13. Start the virtual server as described in Installing a Guest OS. Open a virtual server console and observe the boot process. When the virtual server starts, it will boot the VS Tools package you installed, as shown in Figure 101.

Figure 101. Virtual Server Startup, with VS Tools Installed

VERIFYING THAT VS TOOLS ARE INSTALLED

To see whether VS Tools is installed on a Linux virtual server, issue this command:

```
# rpm -qa | grep virtualiron
```

UNINSTALLING VS TOOLS

You can uninstall the VS Tools package by issuing this command at the operating system prompt:

```
# rpm -e <rpm kit>
```

Note: If you uninstall VS Tools, make sure you un-check VSTools for virtual servers that boot the associated OS. See Figure 98.

Installing the AMD-V Optimization Driver for Windows XP

The AMD-V Optimization driver improves the performance of the Windows XP operating system running on AMD machines. Use the following procedure to install the AMD-V Optimization driver:

Step 1. Click the **Console** icon in the toolbar and open a browser within the virtual server.

Step 2. Enter the IP address of the VI-Center and click the VS Tools Installers link.

Step 3. Click the /win/advanced directory.

Step 4. Click the AMD driver link (amdtpropt-vX.X.XX.exe).

Step 5. Follow the installer instructions.

VS Tools Silent Install: Windows XP and Windows 2003

The following procedure automatically installs VS Tools for Windows and is intended for unattended installation using applications such as Microsoft Active Directory Group Policies. Use this command with your automated installation application:

```
./qn_
```

Please see

```
http://support.microsoft.com/kb/816102
```

for more information.

Step 1. In Windows **Start** menu, select **Run**.

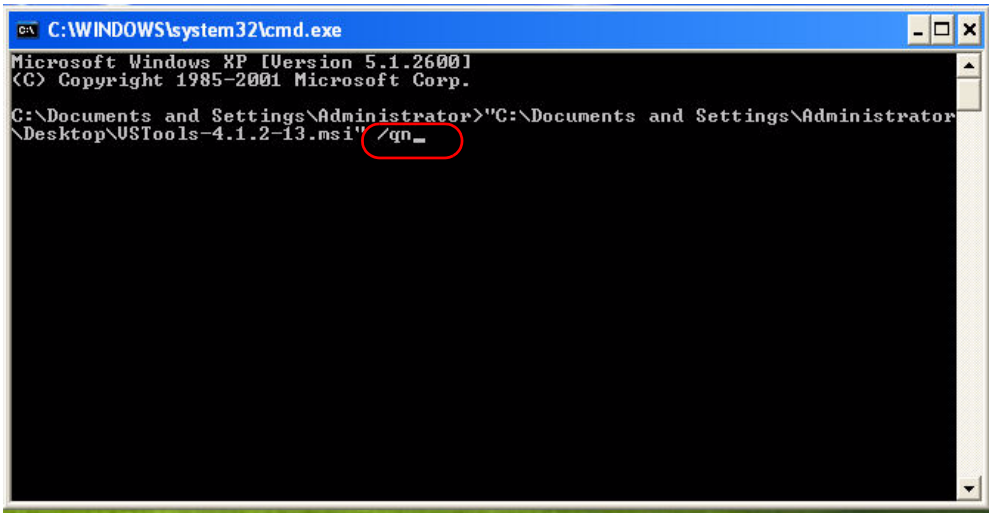
Step 2. In the **Run** window, type **cmd**. Press **Enter**.

Step 3. In the command console, click the **VSTools.msi** icon and drag it into the console window.

Step 4. The command string is automatically entered. Press the space bar.

Step 5. In the console window, type **/qn**, as shown in Figure 102**.** Press **Enter**.

Figure 102. Windows Console, VS Tools Silent Install



Step 6. The VSTools installation starts downloading. Open the VS Configuration window, and check **VS Tools Installed**. Click **OK**.

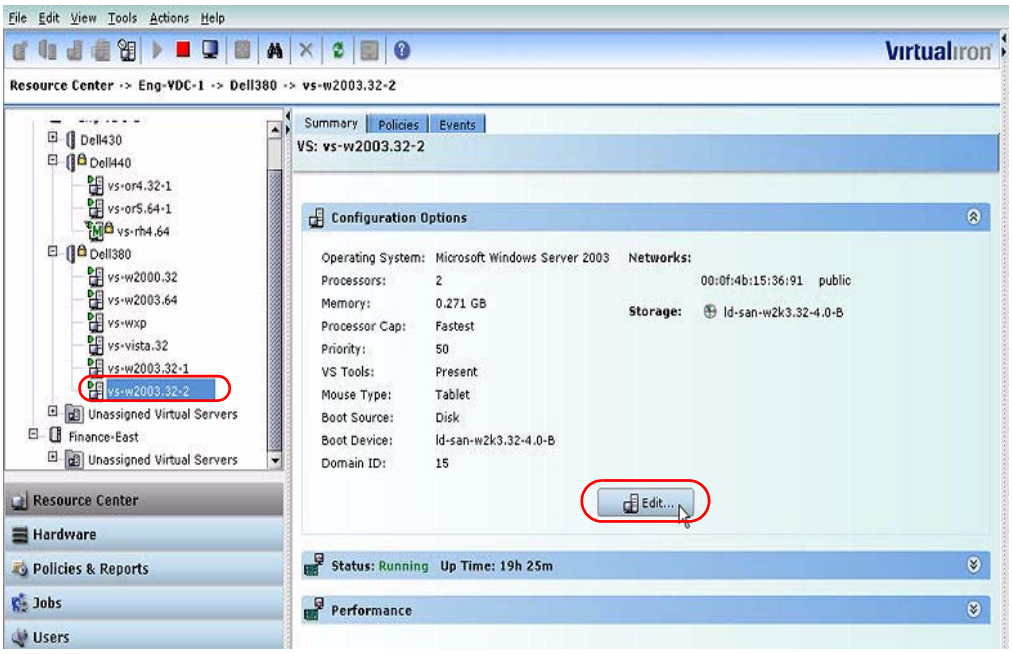
You can choose to disassociate the CD-ROM if you wish.

Installing VS Tools on Windows Virtual Servers Using ISO Images

Step 1. In the **Resource Center**, select the virtual server.

Step 2. In the Summary screen, click the **Edit** button. See Figure 103.

Figure 103. Selected Virtual Server Summary Screen: Windows

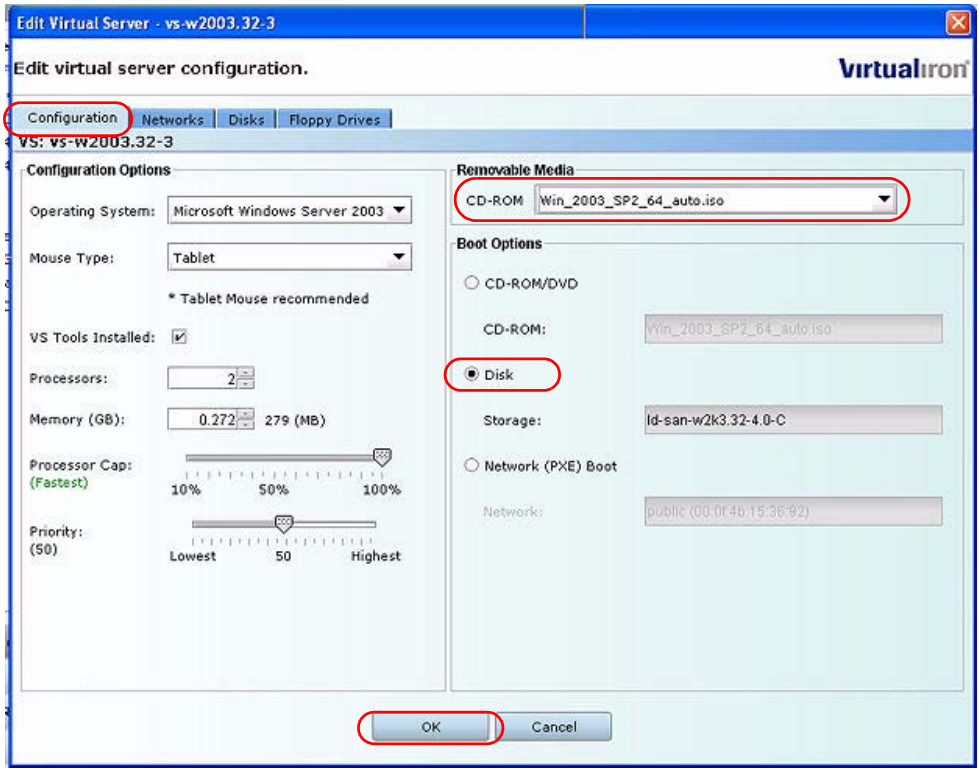


Step 3. In the Edit Virtual Server Configuration screen, select the 32-bit or 64-bit VSTools .iso file from the **Removable Media** CDROM pulldown list.

Step 4. Under **Boot Options**, click the **Disk** radio button.

Step 5. Click **OK** to add the .iso file. See Figure 104.

Figure 104. Select VSTools .iso File



Step 6. Click the **Start** icon in the VI-Center application toolbar and wait for the virtual server to start.

Step 7. Click the **Console** icon in the action toolbar and login to the console.

Step 8. .On your Desktop, open My Computer and double-click on the CD-ROM drive. The installation starts automatically.

Step 9. Follow the prompts in the Virtual Server Tools Setup Wizard.

Auto-updating VS Tools on Windows Virtual Servers

You can automatically upgrade your VS Tools on Windows Virtual Servers without manual intervention.

TO SET UP A WINDOWS VIRTUAL SERVER FOR VS TOOLS AUTO-UPDATE

Use the following procedure to put a properties file on a virtual server which checks for the latest version on your management server, updating as necessary. You must perform this procedure for each virtual server you want to auto-update.

Step 1. Manually install or upgrade the 4.5 or later version of VS Tools in your Windows Virtual Server.

Step 2. Locate the VS Tools install directory on the virtual server. This is usual located at:

C:\Program Files\Virtual Iron Virtual Server Tools

Step 3. In that directory, find the file named VSTupdated.exn and rename it to VSTupdater.exe.

Step 4. Also in that directory, copy VSTupdater.txt and rename the copy VSTupdater.properties.

Step 5. Use a text editor to edit the following line in VSTupdater.properties:

vsToolsUrl=http://n.n.n.n/vstools/updaterDeployment/

If the VSTools are located on the VI-Center, simply edit the above IP address (n.n.n.n) and replace it with the IP address of the VI-Center. You can also place the Windows VS Tools files that are used for updates on any available server with http access.

Step 6. On the VI-Center server, if that is your http server, locate the vstools directory. This is usually at:

C:\Program Files\VirtualIron\VirtualizationManager\system\vstools\win\advanced

Step 7. In the advanced directory, copy (do not move) these 2 files:

Setup-VSToolsx.x.x.x-x32_unattended.exe

Setup-VSToolsx.x.x.x-x64_unattended.exe

to this directory:

VirtualIron\VirtualizationManager\system\vstools\updaterDeployment

Step 8. Test the program by executing VSTupdater.exe in a command window on the Virtual Server. Verify that no errors occur during execution.

Step 9. If there are problems, you can diagnose issues by reviewing the updater log file (VSTupdater.log) in the Virtual Iron Virtual Server Tools directory.

Step 10. In the VS, open up System Tools > Scheduled Tasks and use the wizard to addVsToolsUpdater.exe to run as a scheduled task. "Daily" is a good period to use.

In Windows Vista and Windows 2008 Scheduled Tasks, you will need to explicitly specify the directory in which the task will be run. You do this by opening the Properties Page for the task and selecting the Actions tab. In the "Start in (optional):" field, you must then enter the Virtual Iron Virtual Server Tools directory. This parameter, usually C:\Program Files\Virtual Iron VirtualServer Tools\ must NOT have quotes around it in this field.

Once done, this will check for new VS Tools every day and update as necessary. It's a good idea to test run this after you finish the task and check the log file (mentioned in step 9) to verify that the program ran correctly.

Note: When a new version of VI-Center is released, simply copy the 2 files listed in Step 5 to the updateDeployment directory and the VS's will

automatically update them. Copying these files should only be done after the nodes have all been upgraded to the new version.

Auto-updating VS Tools on Linux Virtual Servers

VSTupdater.py is a script made available to Virtual Iron customers who would like to automatically upgrade their VS Tools on their Virtual Servers without manual intervention. You must manually upgrade to version 4.5 once this procedure is complete, but all future upgrades are done automatically.

The program will use the VSTupdater.properties file which contains the http url of the location of the vstools\advanced directory. The program will read that location and parse the version of the Setup-VSToolsx.x.x.x-x32_unattended.exe file to determine its version. If the version is newer than the currently installed version, the program will copy over the new version and upgrade the VS Tools. The new version will take effect at the next reboot of the VS.

HOW TO SET UP AUTO-UPDATING OF VS TOOLS

Step 1. Locate the VS Tools install directory on the Linux Virtual Server. This is usually located at:

/usr/lib/virtualiron

Step 2. Create a copy of VSTupdater.txt (do not move or rename the original file) and name the copy VSTupdater.properties.

Step 3. Use a text editor to edit this line in VSTupdater.properties:

vsToolsUrl=http://*n.n.n.n*/vstools/updaterDeployment/

If the VSTools are located on the VI-Center, simply edit the above IP address (*n.n.n.n*) and replace it with the IP address of the VI-Center. You can also place the Windows VS Tools files that are used for updates on any available server with http access.

Step 4. On the VI-Center server (if that is your http server), locate the vstools directory.

This is usually at:

/opt/VirtualIron/VirtualizationManager/system/vstools/rpms

Step 5. From the advanced directory, copy (not move) the rpms that you would like updated to this directory:

/opt/VirtualIron/VirtualizationManager/system/vstools/updaterDeployment

Step 6. Test the program by executing VSTupdater.py on the Virtual Server. Verify that no errors occur during execution.

Step 7. If there are problems, the program writes out a log (VSTupdater.log) to the /usr/lib/virtualiron directory.

Step 8. In the VS, set up a cron job to run the python script daily to check for new VS Tools.

Once done, this will check for new VS Tools every day and update as necessary.

Note: When a new version of VI-Center is released, simply copy the new files listed in Step 5 to the updateDeployment directory and the VS's will automatically update them. Copying these files should only be done after the nodes have all been upgraded to the new version.

Upgrading a Guest Operating System on a Virtual Server

Use this procedure to upgrade an operating system running on a virtual server:

Step 1. Uninstall VSTools on the virtual server you want to upgrade. See Uninstalling VS Tools.

Step 2. Upgrade the operating system.

Step 3. Re-install VSTools.

SPECIAL CONSIDERATIONS FOR WINDOWS 2000 OS

When a Windows 2000 system without VSTools is idle, it will appear to be consuming no CPU resources. Task Manager will show that the CPU is idle. However, Windows 2000 is actually executing instructions in its idle loop. These cycles will not be available for use by other virtual servers on the same node. In order to get Windows 2000 to act like the other more recent Windows operating systems and actually relinquish the CPUs when idle, do the following:

Step 1. Make sure VS Tools are loaded and running in the Windows 2000 virtual server.

Step 2. Open a browser within the Windows 2000 virtual server, and navigate to the VI-Center's IP address. You will see the Virtual Iron VI-Center home page.

Step 3. Click the **VS Tools Installers** link.

Step 4. Click the **win /link**.

Step 5. Click the **Win2000_idler_on.reg** link and download that file to the virtual server. Do the same for **Win2000_idler_off.reg**.

Step 6. Double click **Win2000_idler_on.reg** to read the idler information into the Windows Registry.

Step 7. On the Windows 2000 desktop. Right click the **My Computer** icon and select **Manage**.

Step 8. Navigate to **Services** and **Applications > Services**.

Step 9. Find the Virtual Iron Service and right-click **Restart**.

A side-effect of the idler is that it will appear that the **ViStats.exe** process is consuming all idle cycles in the virtual server. In fact, it only appears this way; it is actually releasing control to the underlying virtualization services so that idle cycles can be used by other virtual servers.

Turn the idler off by double-clicking the **Win2000_idler_off.reg** file and then restarting the Virtual Iron Service. Virtual Iron recommends that the idler is turned on.

STARTING AND STOPPING VIRTUAL SERVERS

Virtual servers that are running are marked with a green triangle in the navigation tree. Virtual servers in a Stopped state are marked with a red box in the navigation tree.

Starting a Virtual Server

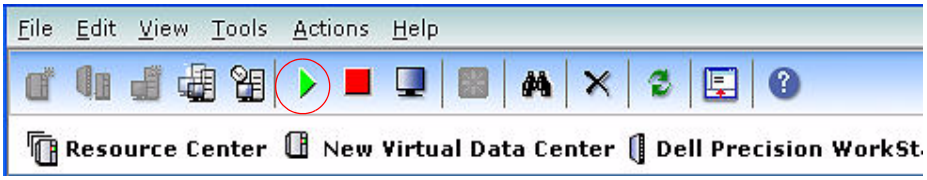
To start a virtual server:

Step 1. A stopped virtual server is marked with a red square in the navigation tree. Click the virtual server to select it, and perform one of the following actions:

- Select the Start Virtual Server icon in the application toolbar. This icon is shown in Figure 105.

Figure 105. Start Virtual Server Icon

Start and Stop virtual server icons



- Right click on the virtual server and select **Start** from the pop-up menu.
- Select **Start** from the **Actions** menu.

Step 2. When you issue a Start command, the command appears as an operation in the Job Operations tab at the bottom of the management pane.

Stopping a Virtual Server

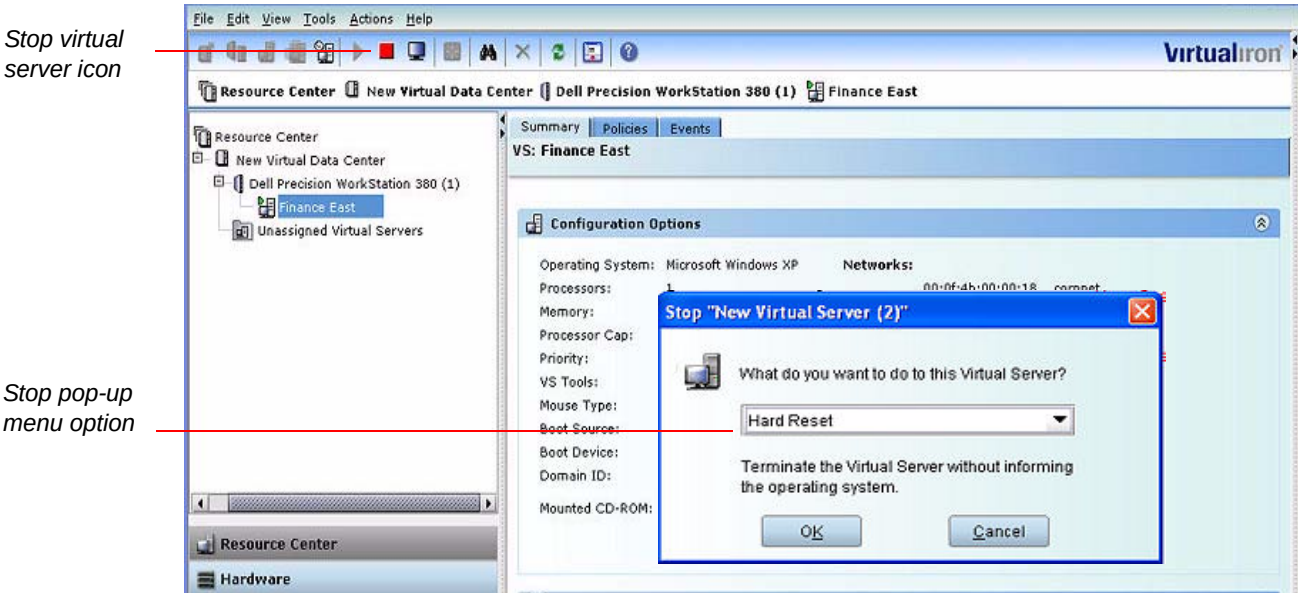
To stop a running virtual server:

Step 1. Select the virtual server in the navigation tree.

Step 2. Stop the server in by doing one of the following:

- Click the **Stop** icon in the application toolbar.
- Select the server and choose an option from the **Stop (New Virtual Server)** pop up menu as shown in Figure 106.
- Select **Stop** from the **Actions** menu.

Figure 106. Stopping a Virtual Server



Step 3. If you do not have VSTools installed, **HardReset** is the only option, as shown in Figure 106. Click **OK**.

If VSTools are installed, choose from the options in the **Stop (New Virtual Server)** popup, shown in Figure 107, and described below:

Figure 107. Virtual Server Stop Options

- **Shutdown**—Performs an orderly OS shutdown. This requires VSTools installation, as explained in Installing VS Tools on Virtual Servers.
- **Restart**—Performs an orderly OS shutdown followed by a virtual server restart.
- **Hard Reset**—Performs a forced stop. The virtual server is terminated without informing the OS. Perform a Hard Reset only when the virtual server does not respond to Shutdown or Restart commands. You may need to perform a hard reset if a virtual server does not have VS Tools installed.

Choose a shutdown option for the server and click **OK**.

LAUNCHING A VIRTUAL SERVER CONSOLE

To open a console for a virtual server:

Step 1. Select the virtual server in the navigation tree.

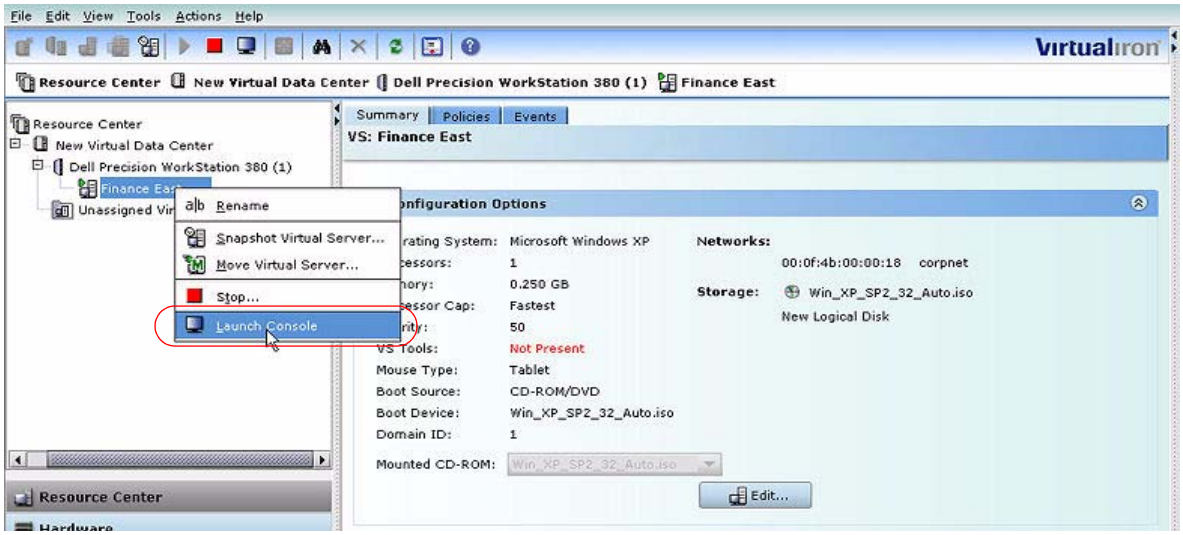
Step 2. Launch a console by doing one of the following:

- Click the console icon in the application toolbar. See Figure 108.

Figure 108. Launch Virtual Server Console icon

- Right-click on a running virtual server and choose **Launch console** from the menu options as shown in Figure 109.

Figure 109. Launch virtual server option, pop-up menu



Step 3. Press **Enter** several times in the open console window to get to the OS prompt. The console can be resized, run in the background, and dismissed (closed) as needed.

The virtual console shows the boot sequence for Red Hat Linux or the boot sequence for Window® XP Professional.

Note: To improve performance, disable the following on all Virtual Servers:
- screen savers
- hibernation

- standby
- the “Turn off hard disks” in power schemes

CONFIGURING POLICY-BASED MANAGEMENT

Virtual Iron® provides advanced features that support high-availability for virtual servers:

- **LiveCapacity®**—Automatically balances processing loads across a set of physical machines
- **LivePower™**—Dynamically migrates virtual servers from under utilized nodes and shuts them down, conserving power until they are needed again
- **LiveRecovery™**—Moves running virtual servers from host nodes to different machines to facilitate maintenance operations
- **LiveMaintenance™**—Automatically moves and restarts virtual servers on a new node if a hosting node fails.

These and other features provide policy-based automation of virtual and physical resources. This allows administrators to manage and deliver services more efficiently by reducing the complexity and costs involved with operating enterprise data centers. See System Policies for detailed information and policy procedures.

LiveCapacity®

LiveCapacity® optimizes virtual server use across a shared pool of nodes. It automatically moves running virtual servers to a new physical server in a VDC if any of the servers exceed a specified CPU threshold for a specified period of time.

LiveCapacity® continuously samples performance data from every node and every virtual server. The movement of virtual servers is policy-driven. When a threshold is reached, Virtual Iron® LiveMigrate® technology relocates running GOSs and their applications from one physical server to another without down time. VI-Center™ allows you to specify a LiveCapacity® threshold for each Virtual Data Center, and to choose which set of nodes participate in the policy.

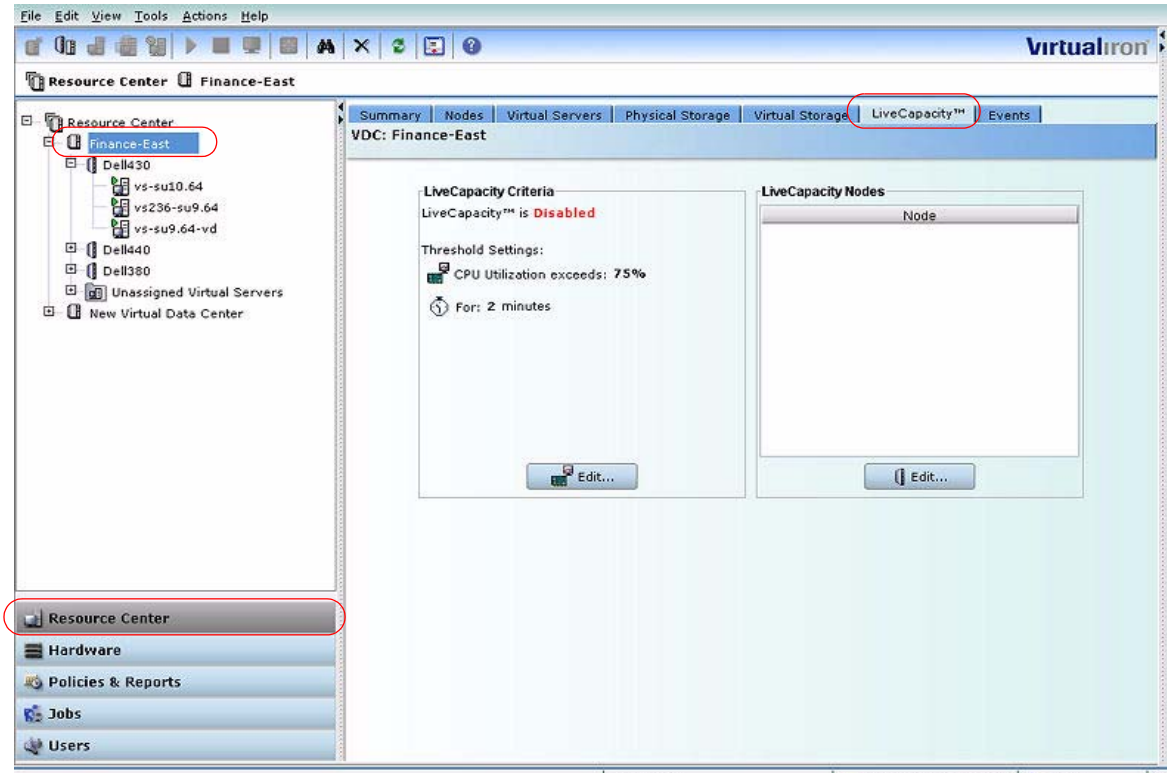
For information and procedures on scheduling LiveCapacity® on a per-node basis, see LiveCapacity in Policies and Reports.

CONFIGURING LIVECAPACITY®

Step 1. In the **Resource Center** view, select the virtual data center in the navigation tree.

Step 2. Select the **LiveCapacity®** tab. Note that LiveCapacity® shows as **Disabled**, and that current threshold settings are listed. See Figure 110.

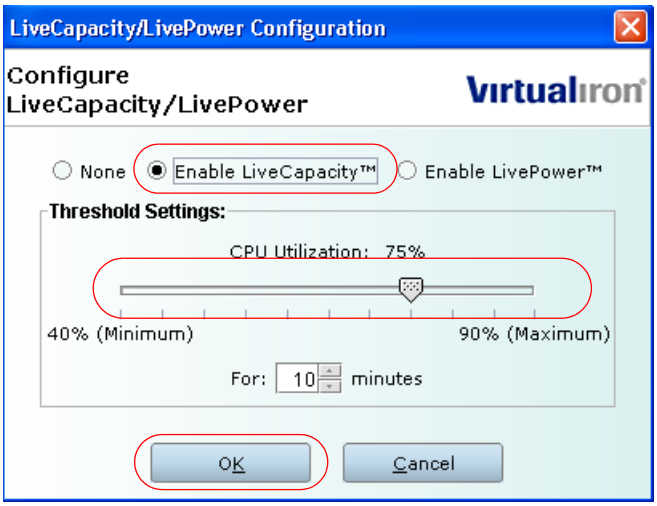
Figure 110. LiveCapacity® Criteria and Threshold Parameters



Step 3. Click the **Edit** button in the LiveCapacity® Criteria portion of the screen.

Step 4. In the LiveCapacity® Configuration window, click the **Enable LiveCapacity®** checkbox. Set a percentage for CPU utilization and a maximum time period for that threshold to exist. Click **OK**.

Note that Live Capacity is now Enabled in the LiveCapacity® Criteria window.



Step 5. Click **Edit** in the **LiveCapacity® Nodes** section of the window as shown in Figure 110, to Add or Remove available nodes to or from the pool of nodes that will participate in the policy. Click **OK**.

LivePower™

LivePower™ dynamically migrates virtual servers from under-utilized nodes and shuts the node down, conserving power until the node is needed again.

LivePower™ keeps only the minimum necessary number of nodes running to conserve power. If a periodic check reveals that a node is operating at below a user-set CPU level, LivePower™ locates another node or nodes to off-load the node's virtual servers. Virtual servers are Live Migrated using Virtual Iron® LiveMigrate® technology to other nodes in the same Virtual Data Center. When all virtual servers are migrated, the node is shut down.

If a node exceeds the LivePower™ policy CPU threshold, the policy looks for other nodes to migrate Virtual Servers to from the busy node. If no powered nodes are available, the policy finds and starts a powered-off node to start using Wake-on-LAN. Once that node is running, the policy off-loads Virtual Servers from the busy node to the newly started node.

VI-Center™ allows you to specify a LivePower™ threshold for each VDC, and to choose which set of nodes participate in the policy.

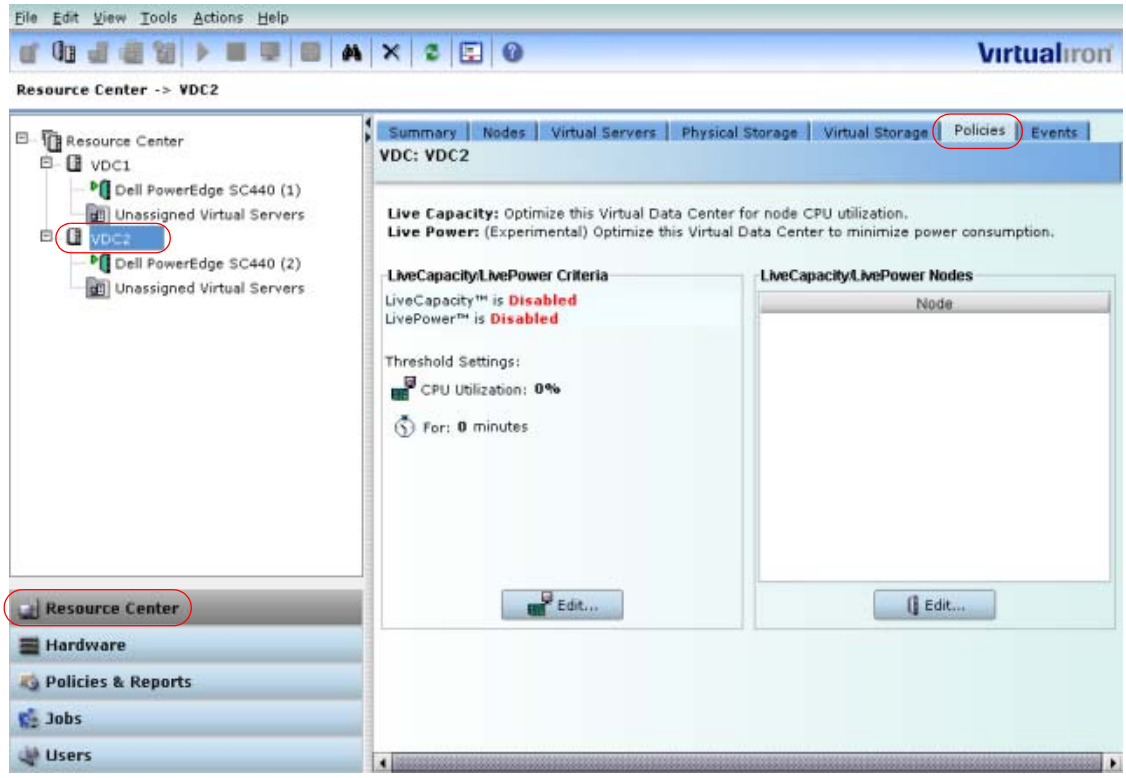
Note: Before you enable LivePower™, you must first make sure all the affected nodes are capable of starting up via IPMI or Wake-on-LAN. Wake on LAN is a motherboard setting configurable in the BIOS. Consult your motherboard documentation for instructions on how to set Wake on LAN for your machine. For instructions on configuring IPMI on individual nodes, see Configure IPMI or ILO for each Node. Once you have enabled Wake-on-LAN or IPMI, check each node by stopping and restarting. See Stopping a Node and Starting a Node.

CONFIGURING LIVEPOWER™

Step 1. In the **Resource Center** view, select the virtual data center in the navigation tree.

Step 2. Select the **Policies** tab. Note that LivePower™ shows as **Disabled**, and that current threshold settings are listed. See Figure 111.

Figure 111. LivePower™ Criteria and Threshold Parameters

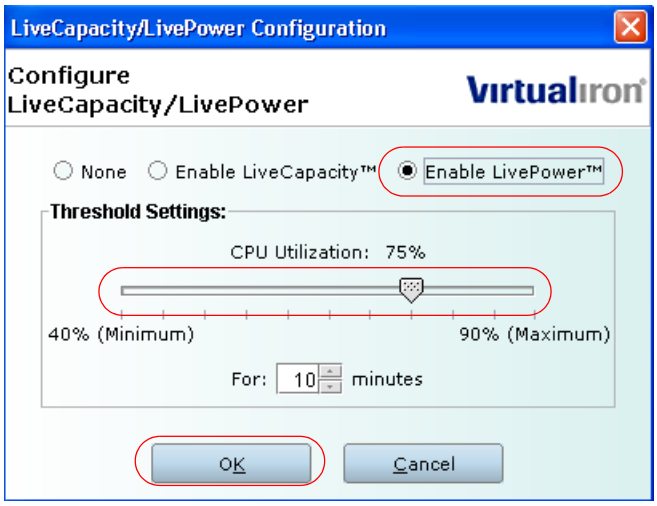


Step 3. Click the **Edit** button in the LiveCapacity®/LivePower™ Criteria portion of the screen.

Step 4. In the LiveCapacity®/LivePower™ Configuration window, click the **Enable LivePower™** radio button. Set a percentage for **CPU Utilization** and a maximum time period for that threshold to exist. Click **OK**. As a general rule, you should not set the CPU Utilization slider below 60-70%.

Note that LivePower™ is now Enabled in the LivePower™ Criteria

window.



Step 5. Click **Edit** in the **LivePower™ Nodes** section of the window as shown in Figure 111, to Add or Remove available nodes to or from the pool of nodes that will participate in the policy. Click **OK**.

LIVEPOWER BEST PRACTICES

- Set the CPU Utilization slider to no lower than 60-70% at first.
- Group processors of the same manufacturer (AMD/Intel). This is not required, but if you mix manufacturers, LivePower splits them into separate groups and balances them within those groups.

LiveRecovery™

LiveRecovery™ provides high availability for virtual servers by automatically moving them to a new physical server if their managed node fails. In contrast to LiveCapacity®, which is enabled at the VDC level, LiveRecovery™ is enabled for each virtual server on a case-by-case basis.

Once enabled, LiveRecovery™ checks the virtual servers as they start running to test whether they can respond to a ping to any of their IP addresses. If pings to any interface are successful, the virtual server is declared a candidate for LiveRecovery™ and the virtual server is shown as protected.

Once configured for a virtual server, you can schedule LiveRecovery™. See Scheduling AutoRecovery.

LiveRecovery™ Requirements

For LiveRecovery™ to operate properly, certain conditions must be met for each virtual server.

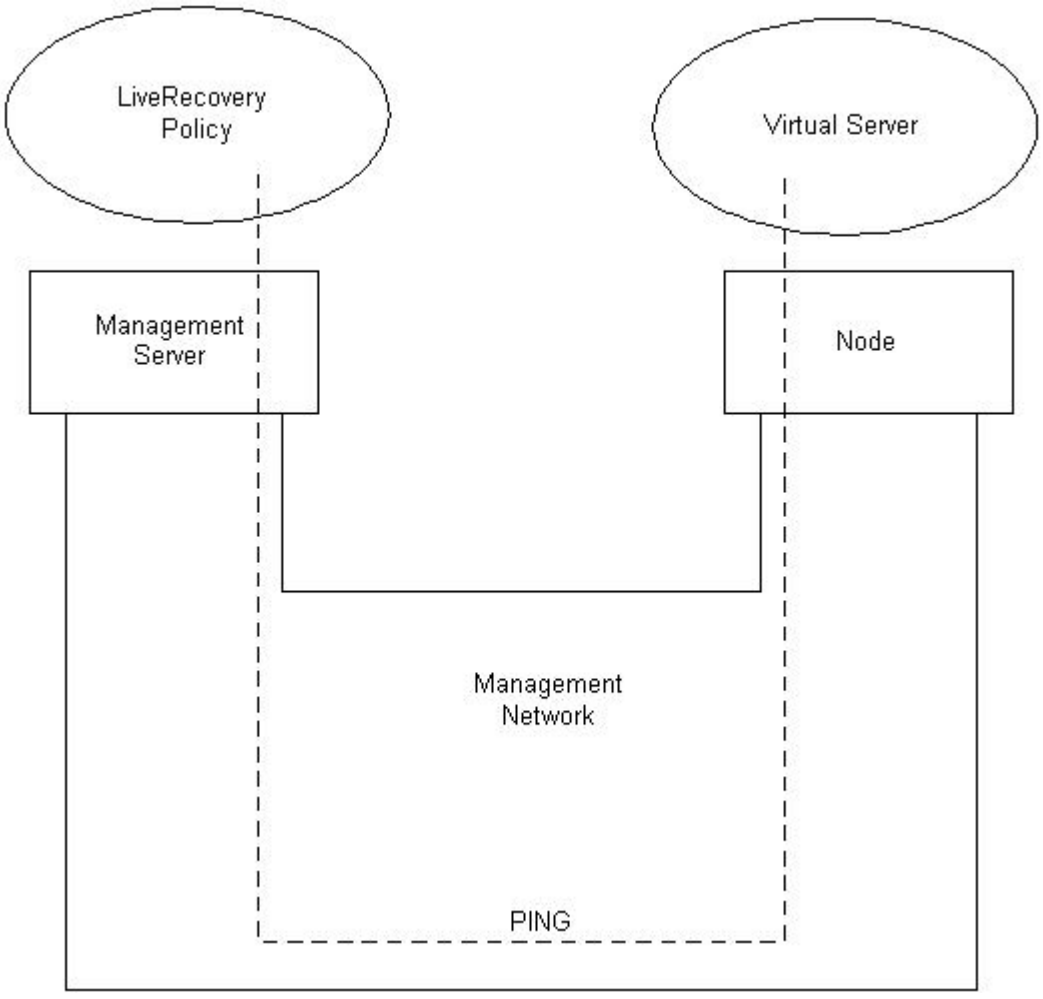
- Assure that the virtual server is *not* configured with a network (image) boot device.
- **VS Tools** *must* be enabled on the virtual server to get the virtual server's IP address.
- Check that the virtual server is reachable by the management server via at least one of its Ethernet networks, and that ICMP is enabled in the virtual server. ICMP is required to allow the virtual server to respond to a network ping.
- Assure that at least one node that meets the following requirements is available in the VDC:
  - Enough free memory to accommodate the moved virtual server.
  - A running destination node.
  - The same as, or greater than, the number of CPUs in the virtual server.
  - Connectivity to all the disks assigned to the virtual server. This means that LiveRecovery™ will not work on a virtual server with any local storage assigned to it.
  - Connectivity to the networks configured on the virtual server. LiveRecovery™ checks all the networks assigned to the virtual server's VNICs, so a destination node must have all those networks configured on them.

How LiveRecovery™ Works

The LiveRecovery™ policy uses the Management Network to detect that a node is disabled. However, if this were the only determinant, a pulled cable on the Management Network would initiate LiveRecovery™, with the undesirable result of having two virtual servers writing to the same set of disks.

Therefore, the LiveRecovery™ policy checks whether the node is really down by pinging all the network interfaces on all the virtual servers on the suspected inoperable node. If any interfaces respond, the policy assumes the node is still operating and does not perform a LiveRecovery™.

Figure 112. LiveRecovery™



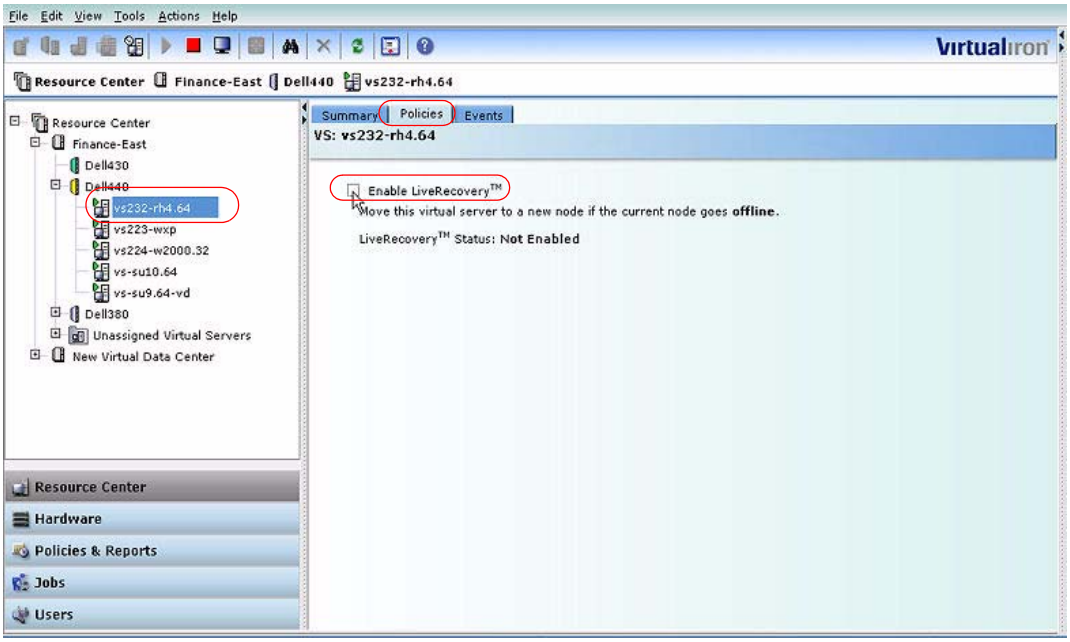
CONFIGURING LIVERECOVERY™

Step 1. In the **Resource Center** view, select the virtual server.

Step 2. Select the **Policies** tab.

Step 3. Check the **Enable LiveRecovery™** tab. See Figure 113. Note that the status changes from Unprotected to Protected.

Figure 113. Enable LiveRecovery™



Checking LiveRecovery™ Status

To check the status of LiveRecovery™ for any virtual server, in the **Resource Center** view, select the virtual server and the **Policies** tab. Click the Virtual Server **Policies** tab to see the state of LiveRecovery™ for the virtual server:

State	Meaning
Not Enabled	The LiveRecovery™ option is not selected for this virtual server.
Inactive	The LiveRecovery™ policy is not running.
Initializing	LiveRecovery™ is attempting to contact (ping) the node on which the virtual server is running.
Not Protected	Contact attempt (ping) was unsuccessful; the virtual server will not be moved to a new node and restarted if the current node fails.

State	Meaning
Protected	Contact attempt (ping) was successful; the virtual server will be moved to a new node and restarted if the current node fails and a suitable new node is available.

LiveMaintenance™

LiveMaintainence™ moves virtual servers to a new machine based on administrative intervention in the event a host server needs service. Server maintenance can be performed outside of scheduled maintenance windows without application downtime. With LiveMaintenance™, physical servers can be removed and reinstated at any time. The pool's capacity changes dynamically and the placement of virtual servers is automatically optimized. Operating system and application patch management activities can be tested with a snapshot of a "live" configuration before production deployment.

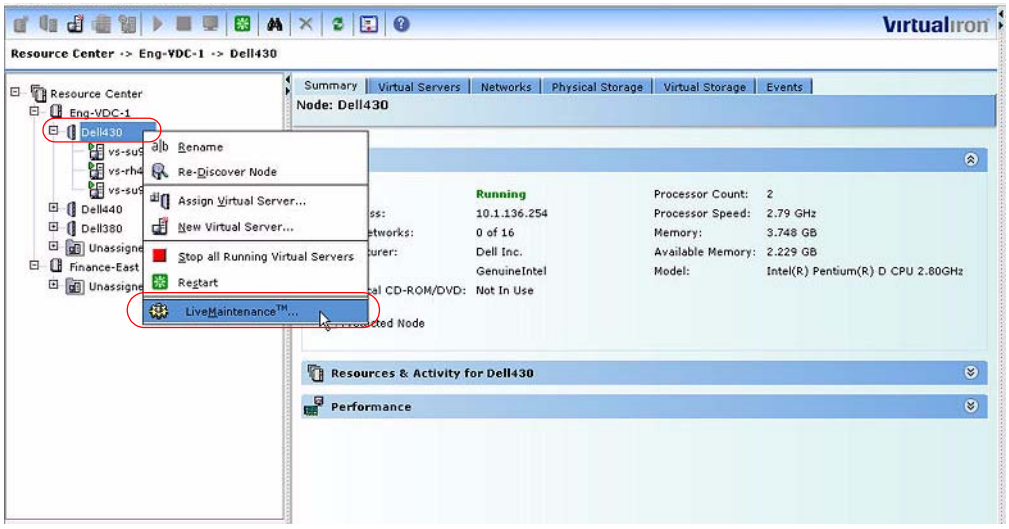
CONFIGURING LIVEMAINTENANCE™

Step 1. In the **Resource Center** view, select and right-click the node.

Step 2. Highlight LiveMaintenance™. See Figure 114.

Figure 114. LiveMaintenance™ Control

Moving virtual servers with LiveMaintenance



Step 3. Click **OK** in the pop-up window.

MOVING VIRTUAL SERVERS AND NODES

Virtual Iron® can adapt on-demand to changing business requirements. In this framework, virtual servers and the managed nodes that host them can be moved to accommodate administrative requirements.

You can drag and drop managed nodes, or move a running or offline virtual server from one physical server to another with LiveMigrate. See LiveMigrate: Conditions for Virtual Server Movement.

Objects that can be moved are described in Table 5:

Table 5. Object Movement in the Virtual Iron® Framework

	Movement From, To...
Node	• VDC to VDC • VDC to Resource Center
Virtual Server	• Node to node • Node to VDC • Node to Unassigned

The Role of the Resource Center

Resource Center is the top-level object in the navigation tree. This object contains all VDCs, nodes, and virtual servers under management by Virtual Iron. Within the Resource Center, you can create separate node groups called Virtual Data Centers (VDCs). Each VDC is an administrative entity that can contain one or more managed nodes and the virtual servers hosted by these nodes.

Moving Nodes to a VDC

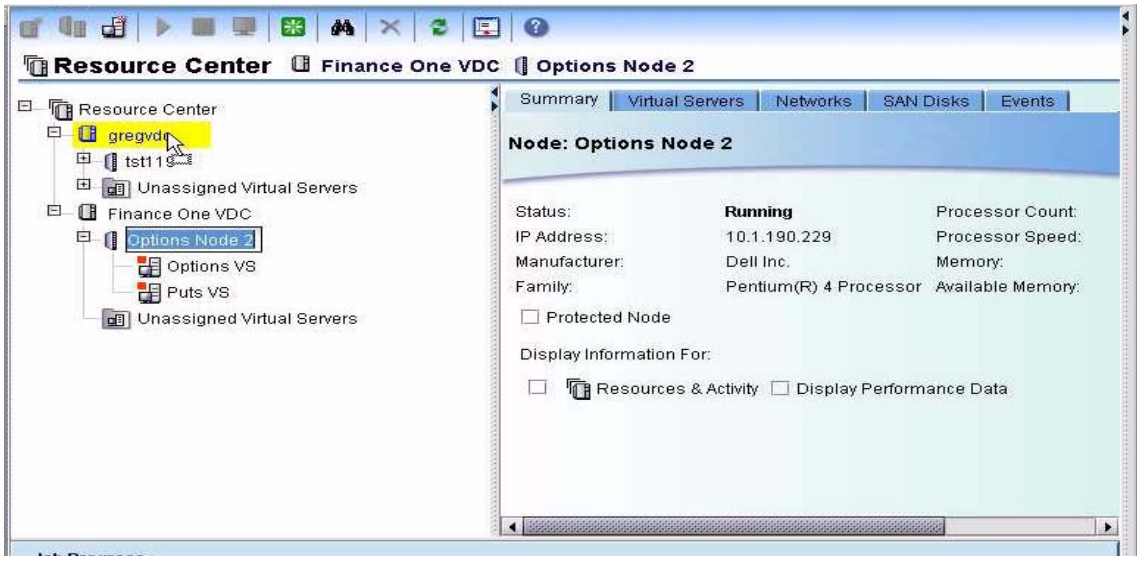
VI-Center supports drag-and-drop control for managed nodes. Use drag-and-drop to move a node from one VDC to another, or to or from the Resource Center. An example is shown in Figure 115. To move a node:

Step 1. Select the node you want to move by depressing a mouse key.

Step 2. Drag the node to its new location, and release the mouse key.

Figure 115 shows managed node Options Node 2 (located in Finance One VDC) being dropped on *gregvdc*.

Figure 115. Dragging a Node to a New VDC



Moving a Node to a Resource Center

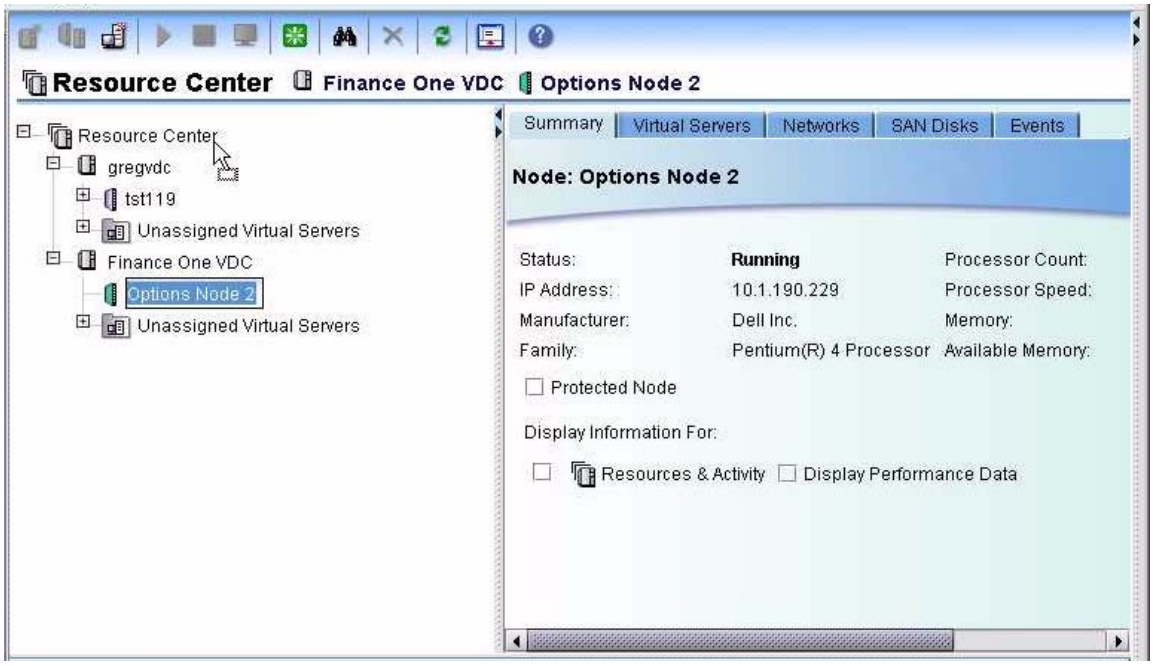
Managed nodes can only be used to host virtual servers when they belong to a VDC. Moving a node to a VDC places the node under ownership of that VDC. Moving a node from a VDC to Resource Center frees the node, making it available for reassignment to another VDC.

Since virtual servers consume node memory (even when offline), nodes that host virtual servers cannot be moved out of their current VDC. Any attempt to move a node that still hosts virtual servers produces the message shown in Figure 116.

Figure 116. Message: Cannot Move Node with Virtual Servers

Figure 117 shows a node being moved from a VDC and dropped on **Resource Center**.

Figure 117. Node moved to Resource Center



LiveMigrate: Conditions for Virtual Server Movement

In multi-node environments, Virtual Iron® allows you to move a running or offline virtual server from one physical server to another with LiveMigrate®. You may do so without affecting applications. Simply drag and drop the virtual server from its existing location to another node or virtual data center.

To LiveMigrate Two Virtual Servers Simultaneously

You can move two virtual servers at the same time from one managed node to another. See Moving Two Virtual Servers Simultaneously.

LIVEMIGRATE® REQUIREMENTS

Before you can move a virtual server from one managed node to another node or to a new VDC, VI-Center evaluates the following:

- Does the managed node have enough memory to accommodate the virtual server? There must be at least the same amount of memory in the target node as in the original node.
- Are the processors of the same processor family? Only Intel-to-Intel or AMD-to-AMD migration is allowed.
- Are there the same or a greater number of CPUs?
- Is there access to a common physical disk pool?
- Does the node have access to the same network and/or SAN resources needed by the virtual server?

If the virtual server is running:

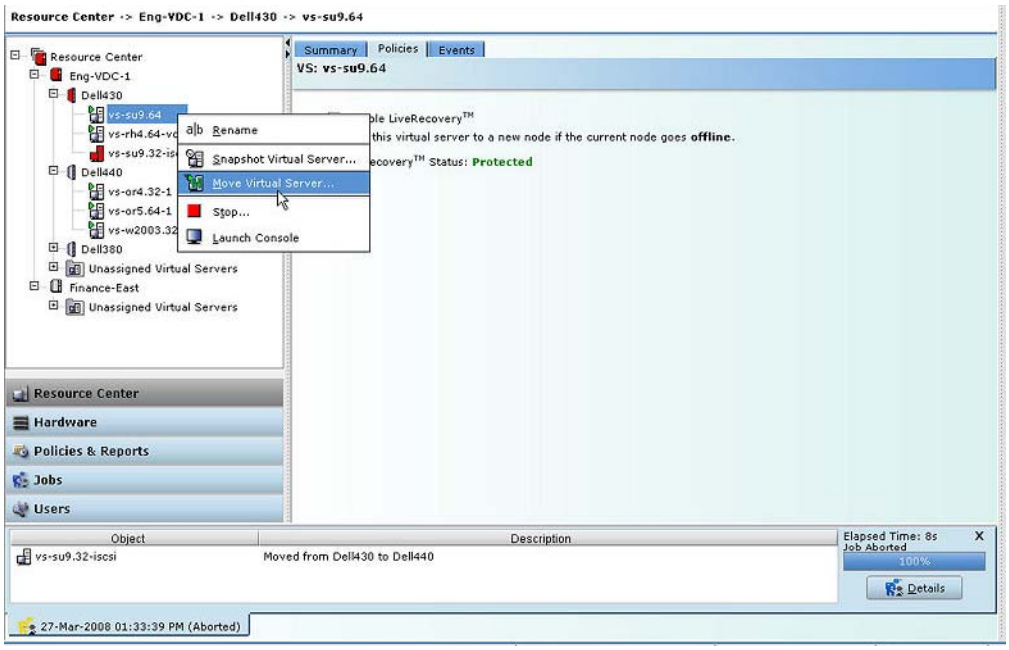
- The destination mode must be running also.
- VS Tools must be enabled
  - Accelerated drivers must be installed on the virtual server
  - The VS Tools checkbox must be checked.

MOVING A VIRTUAL SERVER TO A NEW NODE OR VDC

Before you can place a virtual server on a different managed node, VI-Center checks the LiveMigrate requirements. If the virtual servers on the source node can function on the target managed node, VI-Center allows the operation. If they are not met, movement of the virtual server is disallowed.

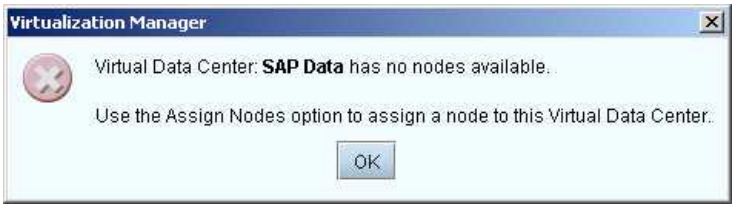
Step 1. In the **Resource Center** view, right click a virtual server and select **Move Virtual Server**. See Figure 118.

Figure 118. Move Virtual Server



VI-Center disallows movement of a virtual server to a VDC that has no nodes. If you attempt this operation, the dialog shown in Figure 119 appears:

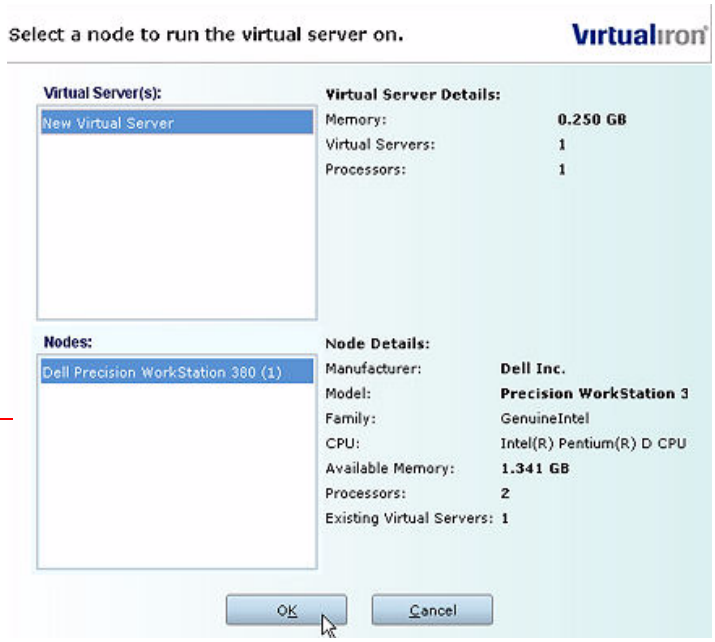
Figure 119. No Nodes Available



If a VDC contains more than one node that is eligible to host the virtual server you are moving, To complete the operation, select a node from the list of those available, and click **OK**.

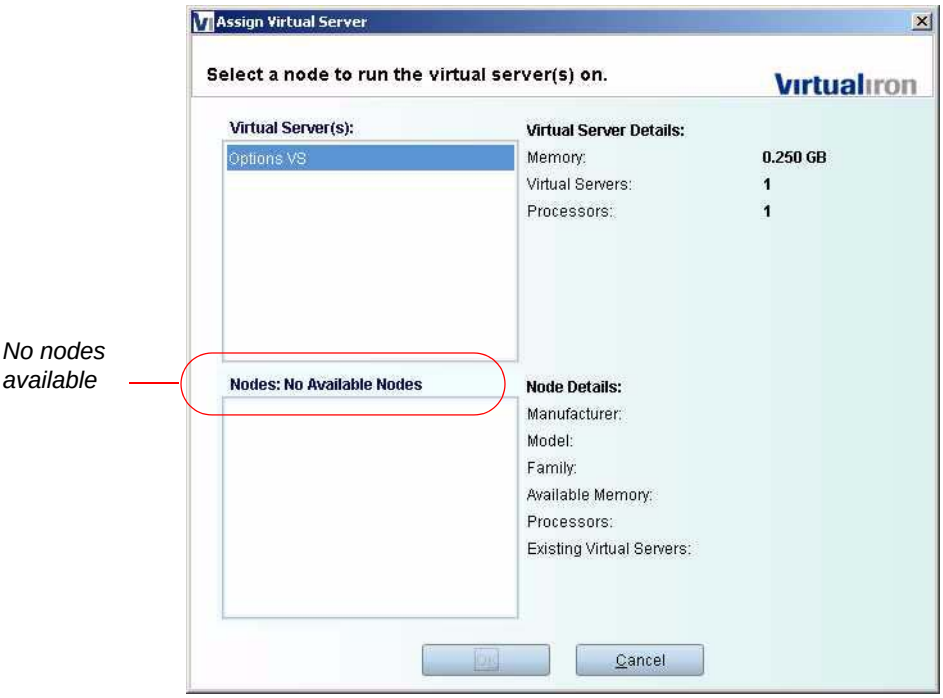
Figure 120. Select a Node to host a Virtual Server

Available Node



If you attempt to move a virtual server to a new VDC that does not have sufficient memory, processors, or access to the required SAN and Networks, the following dialog box appears.

Figure 121. No Available Nodes for use by Virtual Server



MOVING TWO VIRTUAL SERVERS SIMULTANEOUSLY

Step 1. In the **Resource Center** view, select a virtual data center icon in the navigation tree.

Step 2. Select the Virtual Servers tab.

Step 3. In the Virtual Servers table, left-click on one virtual server to select it.

Step 4. With the Shift key depressed, place the mouse pointer on another virtual server in the table and click and *hold down the left mouse button*.

Step 5. Drag the mouse cursor to the node where you want to move the selected virtual servers.

Step 6. Release the left mouse button.

PROVISIONING VIRTUAL SERVERS WITH GOLD MASTERS

It is useful to create a *gold master* for each GOS supported in your data center. This is a logical disk that serves as a container for an installed GOS. When you need to create a new virtual server running that GOS, simply clone the master logical disk and assign it to the LV. You can boot the virtual server without going through the OS installation process again. Simply create a new virtual server and assign the cloned master logical disk to it.

If you need to rapidly provision new virtual servers on an ongoing basis, it makes sense to maintain a set of gold masters. This saves time, since you perform an installation of each GOS only once. Thereafter, you can clone the GOS to make use of it as often as needed.

Since the cloning operation copies the entire content of a logical disk to a new location, you can copy applications as well as GOSs. For example, you can create a GOS with a specific Linux or Windows distribution and the set of applications required by a particular set of work requirements. As a result, you can automate the delivery of fully or partially configured systems to specific functional areas as needed.

Note: Before creating and using a gold master, you should familiarize yourself with license requirements that may apply to the use of OSs and applications.

Creating a Gold Master Logical Disk

Follow these steps to create a gold master for any guest operating system supported by Virtual Iron®.

Step 1. Create a virtual server and configure it. Assign a logical disk to it. At this time, the logical disk is empty. Its purpose is to hold a bootable gold master. Rename the logical disk in a way that distinguishes it as such. For example, *Gold-Win2008-04-25*.

Step 2. Copy the OS .iso files onto a publicly addressable web server. This makes the files available for boot later on.

Step 3. Copy the disk1.iso of the OS to the NBD directory of the Virtual Iron® management server.

Step 4. Configure the virtual server to boot from the NBD as described in Creating a Virtual Server.

Step 5. Boot the virtual server from the .iso file.

Step 6. During the http installation process, you will be prompted for the location of the CD .iso. Point to the web server containing the additional .iso files.

Step 7. The installation proceeds, and installs the OS on the logical disk.

Step 8. Shut down the virtual server, clone the gold master to a new logical disk, and boot the virtual server from that logical disk, instead of the

original master.

Cloning and Booting from a Gold Master Logical Disk

From this point, use the logical disk as a gold master. When you need to install the same guest operating system to another virtual server proceed as follows:

Step 1. Clone the gold master to a new logical disk.

Step 2. Export the logical disk clone to a disk group.

Step 3. Assign the disk group to the virtual server.

Step 4. In the Virtual Server Configuration window, designate the logical disk clone as the boot disk.

Step 5. Boot the virtual server.

You can also install applications on the gold master, so that these can be cloned (along with their guest operating system) for use by new virtual servers.

See Cloning Disks for information on cloning logical disks.

7

POLICIES AND REPORTS

This chapter shows how to use VI-Center to configure policies and generate reports.

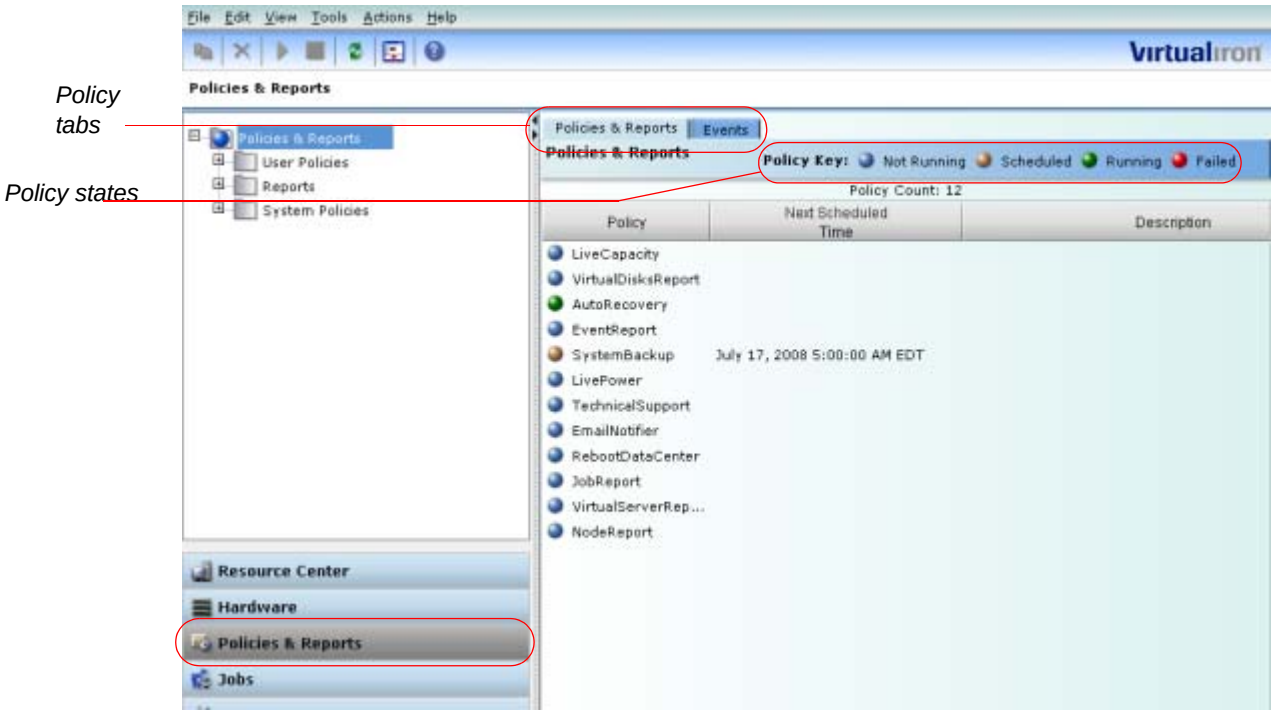
ACCESSING POLICIES AND REPORTS

VI-Center™ supports a set of policies and reports that you configure in various templates. To access these policy and report templates or to view generated reports:

- Click **Policies & Reports** in the application toolbar, or
- In the **View** menu, select the **Policies & Reports** menu option.

This opens the view shown in Figure 122.

Figure 122. Policies and Reports, Main View



Note that there are three categories of policies and reports, each of which is described in detail in the following sections:

- User Policies
- Reports
- System Policies

Policies and Reports States

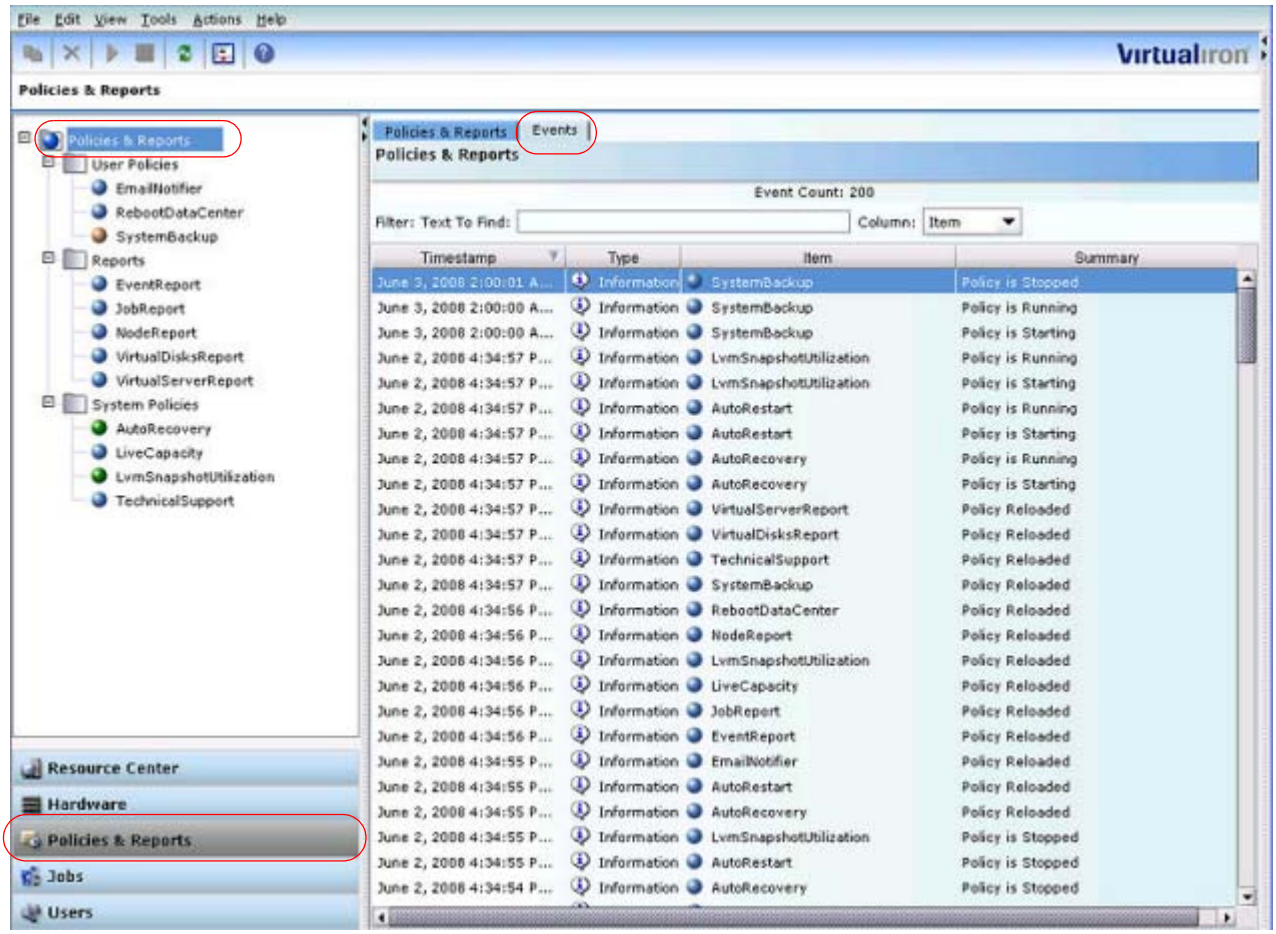
The navigation tree displays all the policies and reports available to you within these categories. The **Policies and Reports** tab lists all policies and their current states. These states are denoted by color coded icons:

- Not running: blue
- Scheduled: gold
- Running: green
- Failed: red

If a policy or report is scheduled to run at a specific time, the time is listed.

Events Tab

Click the **Events** tab to see all user- or system-related events associated with configured policies or reports. Click any of the column headings in the Policies & Reports or Events windows to sort the data in ascending or descending order by time, type, or description.



USER POLICIES

User policies are administratively configured to perform specified actions in response to certain conditions. Supported policies are shown in Table 6:

Table 6. VI-Center™ User Policies

	Purpose
EmailNotifier	Allows you to send email to one or more addresses in response to specified events.
RebootDataCenter	Use to specify which nodes to reboot in the selected Virtual Data Centers. Virtual servers that are running are stopped and restarted when their parent nodes return online. Virtual servers with VSTools installed are shut down; virtual servers without VSTools are that are starting up, are hard reset, if desired. However, it is preferable to shut down those virtual servers directly from within each guest.
SystemBackup	Allows you to specify where backups of the VI-Center database are to be stored, and the number of copies to retain.

Configuring and Starting User Policies

A user policy instructs VI-Center to perform certain actions in response to specified conditions, and schedules when those actions are to be taken.

An example of an email policy might be:

Send email to me and my colleague if any VS is in error.

Another email policy might be:

Send email to me if any node is in error, or if a warning message is issued in relation to a specific VDC.

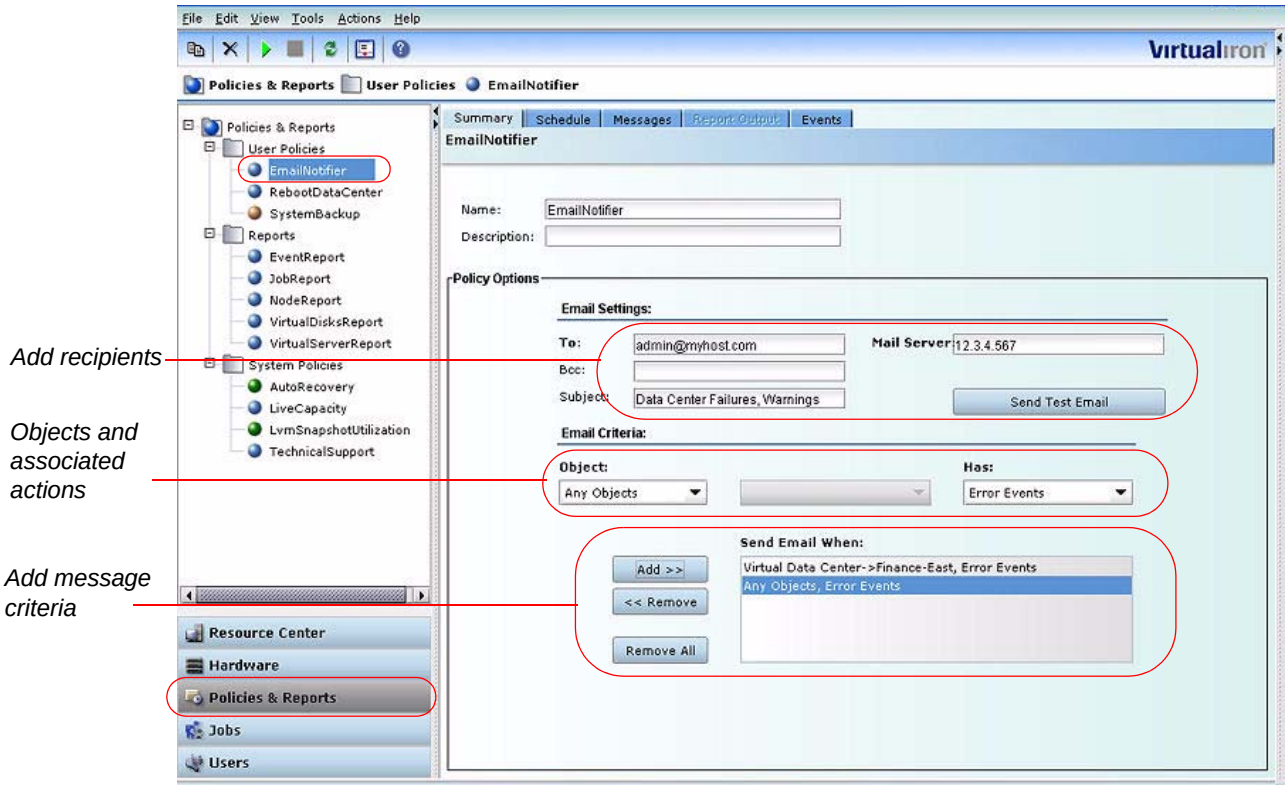
CONFIGURING AN EMAIL POLICY

Step 1. If you are editing an existing email policy, click the **Stop** icon in the task bar to stop the policy.

Step 2. Click **Policies & Reports**. In the navigation pane under **User Policies**, select **EmailNotifier**.

Step 3. In the **Summary** screen, provide information on policy actions, as shown in Figure 123:

Figure 123. Options, Sample Email Policy



Identify a recipient, a mail host, and a subject for the email message (the latter is optional).

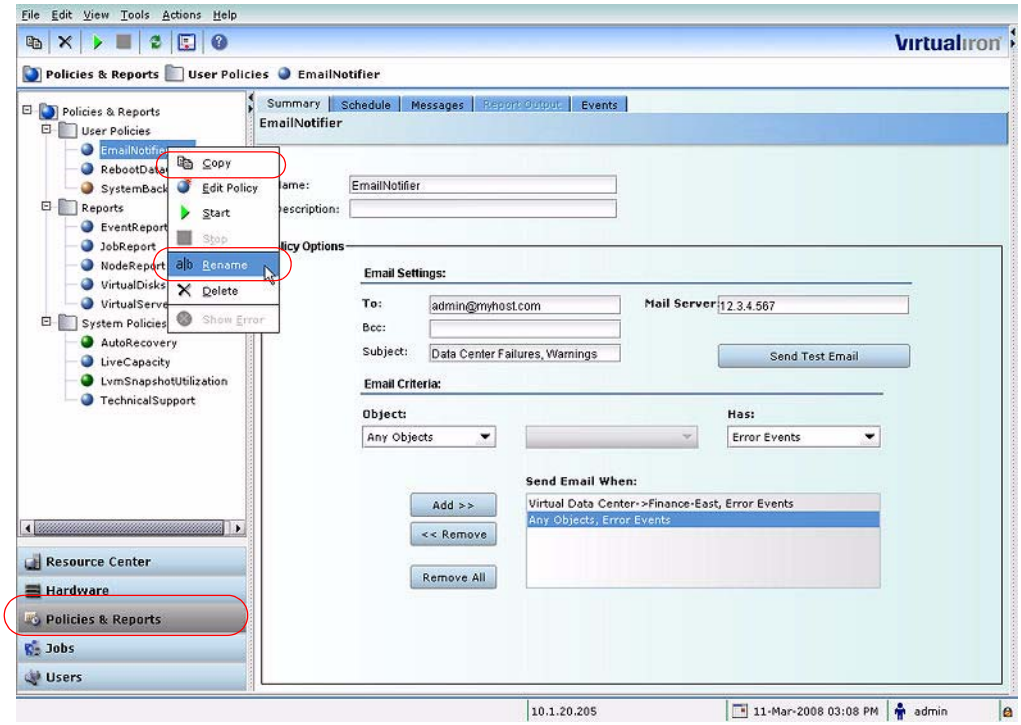
Step 4. The basis of the policy is the criteria that trigger the email message. These criteria determine when the message ("Data Center Failures, Warnings") will be sent. In this case, email will be sent when any of these criteria are met:

- Any object experiences an error event
- A specific virtual data center (Finance-East) has warning events

Specify these criteria by choosing physical and/or virtual objects and the states associated with them from the pulldown menus. Choose an object type from the **Object** pull-down and select an associated action from the **Has** pull-down. Click **Add>>** to add the criteria to the list.

Step 5. Rename the template if you wish. Right-click **EmailNotifier** and select **Rename** from the pop up menu; or right-click and select **Copy** to copy the template and rename it. See Figure 124.

Figure 124. Renaming an Email Template



Step 6. To schedule when and under what conditions to run the email notifier, see Scheduling Policies.

Step 7. When you have completed the email policy configuration, click the **Start** icon in the task bar.

REPORTS

A report is the result of specifying criteria in a report template and displaying the output in either HTML or CSV format. As with other policies, you can schedule reports or run them as needed. These pre-formatted report templates are provided:

Table 7. VI-Center™ Reports

Report Type	Purpose
EventReport	Specify time interval or date range, event severity, and optional description.
JobReport	Specify a time interval or date range.
NodeReport	Specify all criteria options, or select from a list that includes Running, Stopped, and Protected. In addition, you can run a report for nodes in all, a specific, or unassigned VDCs.

Report Type	Purpose
VirtualDisksReport	Specify all criteria options, or select from a list that includes Assigned, Unassigned, Mounted, Not Mounted, Local Disks, and SAN disks. You can run a report for virtual disks in all, a specific, or unassigned VDCs, and limit the output to Groups, Volumes or Virtual Disks.
VirtualServerReport	Specify all virtual servers, or select from a list that includes Running, Stopped, AutoRecovered, and Unassigned. You can run a report for virtual servers in all VDCs, or a specific VDC

Report Naming and Types

Reports are named with the name of the template you are using and the date and time. For example:

/opt/VirtualIron/DataCenterManager/system/reports/DataCenter Operations Report_04_28_2008_02_00pm.html

All reports can be exported in CSV or HTML format. These are stored in the reports directory, located at:

/opt/VirtualIron/DataCenterManager/system/reports

Generating Reports

To generate a report, you select criteria in a report template and schedule the report to run immediately, or at specific times during a particular period.

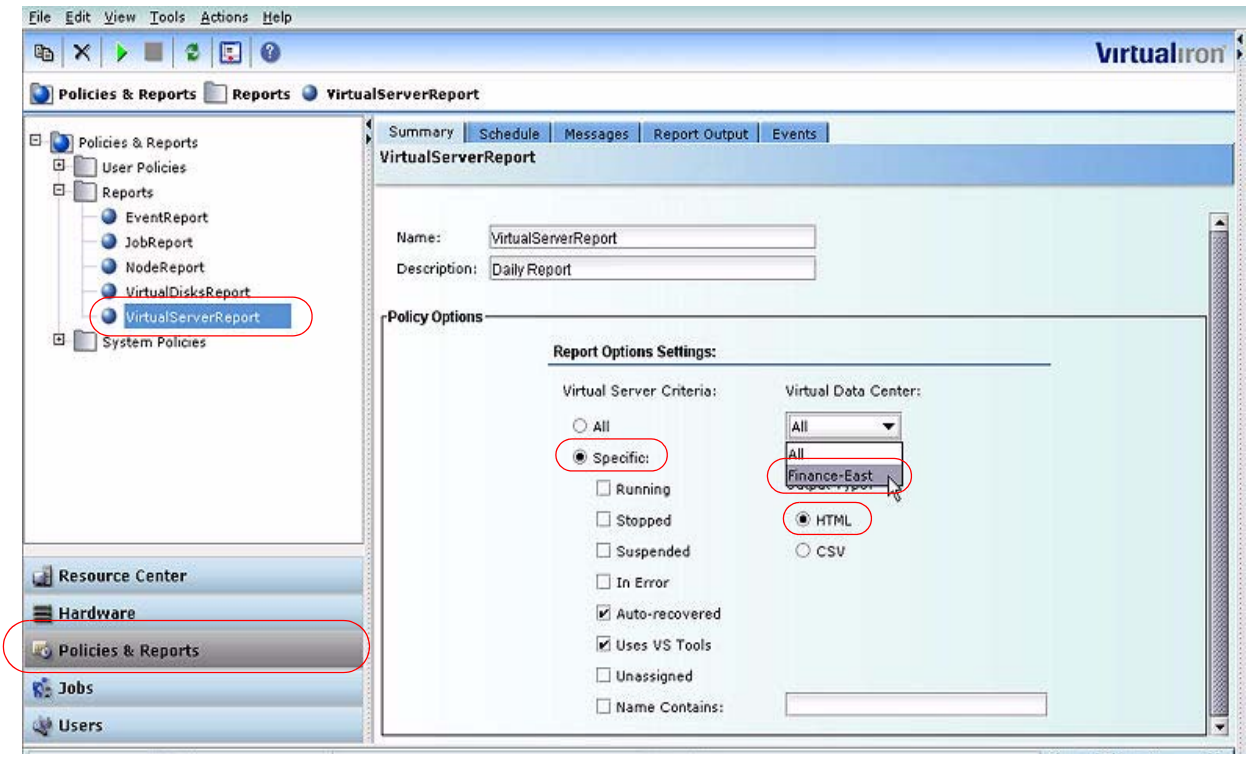
The following example shows how to create a report that shows specific types of virtual server activity:

Step 1. If you are editing an existing report configuration, click the **Stop** icon in the task bar.

Step 2. Click **Policies and Reports**.

Step 3. In the navigation pane, under **Reports**, select the type of report you want to generate. In the sample shown in Figure 125, **VirtualServerReport** has been selected.

Figure 125. Report Template



Step 4. Select **All** from the list of **Virtual Server Criteria** for a report that includes all of the listed criteria, or click one or more specific criteria.

Step 5. From the **Virtual Data Center** pulldown menu, select **All** or choose a data center from the pulldown menu.

Step 6. Choose **HTML** or **CSV** (comma separated values) for the report output. A CSV file is an ASCII file that can be imported into a variety of software applications, such as Microsoft® Excel.

SCHEDULING REPORTS

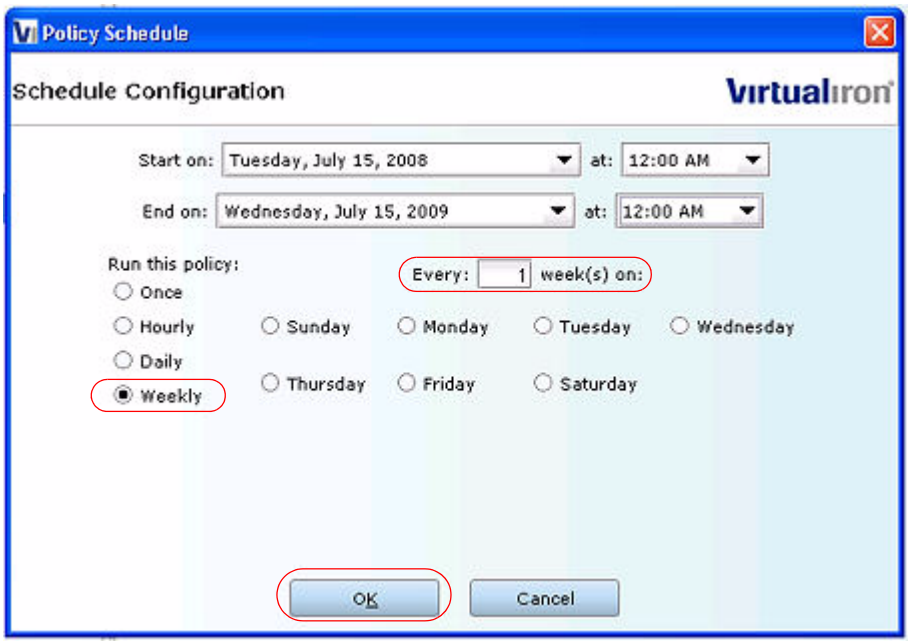
Step 1. Click the **Schedule** tab. Click the **Edit** button.

Step 2. In the **Schedule Configuration** window, use the dropdown menus to choose start and stop dates and times. Click to highlight the hour or minutes and use the up and down arrows to specify the time.

Step 3. Specify a run schedule for the report. You can choose to run a report once (immediately), daily, weekly, or monthly. See Figure 126. Click the down arrow in the **Start on** and **End on** fields to open a calendar.

If you choose to run a report immediately, you do not have to specify a date—only the start time.

Figure 126. Schedule Configuration Window

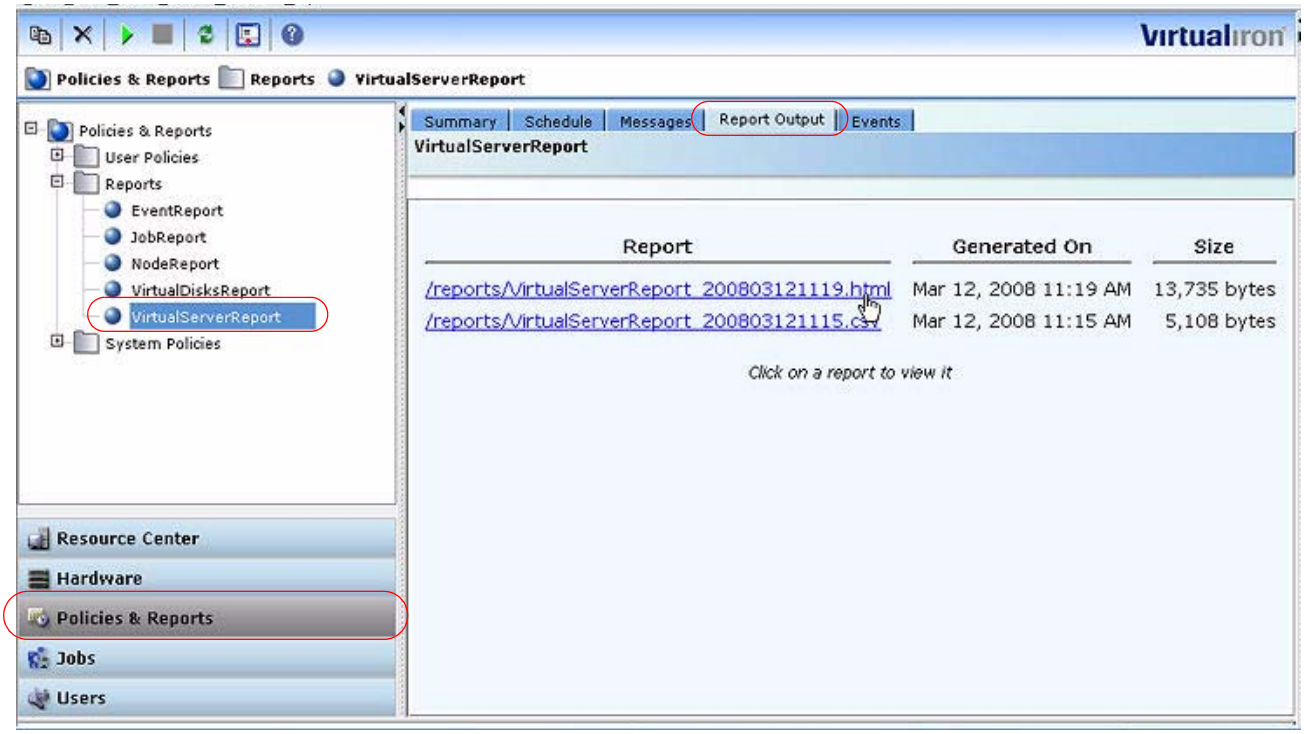


Step 4. Click **OK**.

Step 5. Click the **Start** icon in the task bar.

Step 6. Once the report has been generated, click the **Report Output** tab. Click the link to open the report. See Figure 127. See Report Examples for an example of each type of report you can generate.

Figure 127. Report Output Tab



Report Examples

Following are sample reports generated with the pre-formatted templates supplied with the Virtual Iron™ software. Except where indicated, each of the reports was generated with HTML as the specified output format. See Figure 126.

EVENT REPORT

This report provides details on the events specified in the Summary tab, and the time specified in the Schedule tab.

This reports shows all Warning and Error events. The Informational Events and Event Descriptions options were not selected.

Figure 128. Event Report Sample

VirtualIron

Name: **EventReport**
Generated On: Wednesday March 12, 2008 at 1:59 PM EDT
Report Period: 2008-03-12 00:00 to 2008-03-12 13:59 EDT
Include: Warning Events, Error Events

Time	Event	Source	Summary
Wed Mar 12 09:53 AM EDT 2008	Error	Dell440	Node Connection Failure
Wed Mar 12 09:53 AM EDT 2008	Error	vs-su9.64-vd	Virtual Server is in Error
Wed Mar 12 09:53 AM EDT 2008	Error	This Job	Job Internal Error (Operation): 7 of 12
Wed Mar 12 09:53 AM EDT 2008	Error	This Job	Job Failed to Complete: 6 of 12
Wed Mar 12 09:54 AM EDT 2008	Error	Dell440	Node has Failed Discover
Wed Mar 12 09:54 AM EDT 2008	Error	Dell440	Node is Offline

JOB REPORT

The only configurable options for Job Reports are for scheduling a time period. Figure 129 shows part of a job report for a single day

Figure 129. Job Report Sample

VirtualIron

Name: **JobReport**
Generated On: Wednesday March 12, 2008 at 3:20 PM EDT (Job Count: 93)
Report Period: 2008-03-12 00:00 to 2008-03-12 15:20 EDT

Time	User	Status	Duration	Description
Wed Mar 12 09:51 AM EDT 2008	admin	Done	36 sec	Shutdown

Step	Operation	Foundry Resource
1	Shutdown	vs-su9.64-vd

Time	Event	Source	Summary
Wed Mar 12 09:51 AM EDT 2008	JobConstructingEvent	This Job	Job Construction: 0 of 0
Wed Mar 12 09:51 AM EDT 2008	VirtualServerStoppingEvent	vs-su9.64-vd	Virtual Server is Stopping
Wed Mar 12 09:51 AM EDT 2008	JobRunningEvent	This Job	Job Running: 4 of 4
Wed Mar 12 09:51 AM EDT 2008	VirtualServerStoppedEvent	vs-su9.64-vd	Virtual Server is Stopped
Wed Mar 12 09:51 AM EDT 2008	JobDoneEvent	This Job	Job Finished: 4 of 4

Time	User	Status	Duration	Description
Wed Mar 12 09:52 AM EDT 2008	admin	Error	6 sec	Start Virtual Server vs-su9.64-vd - May not be combined with other job operations

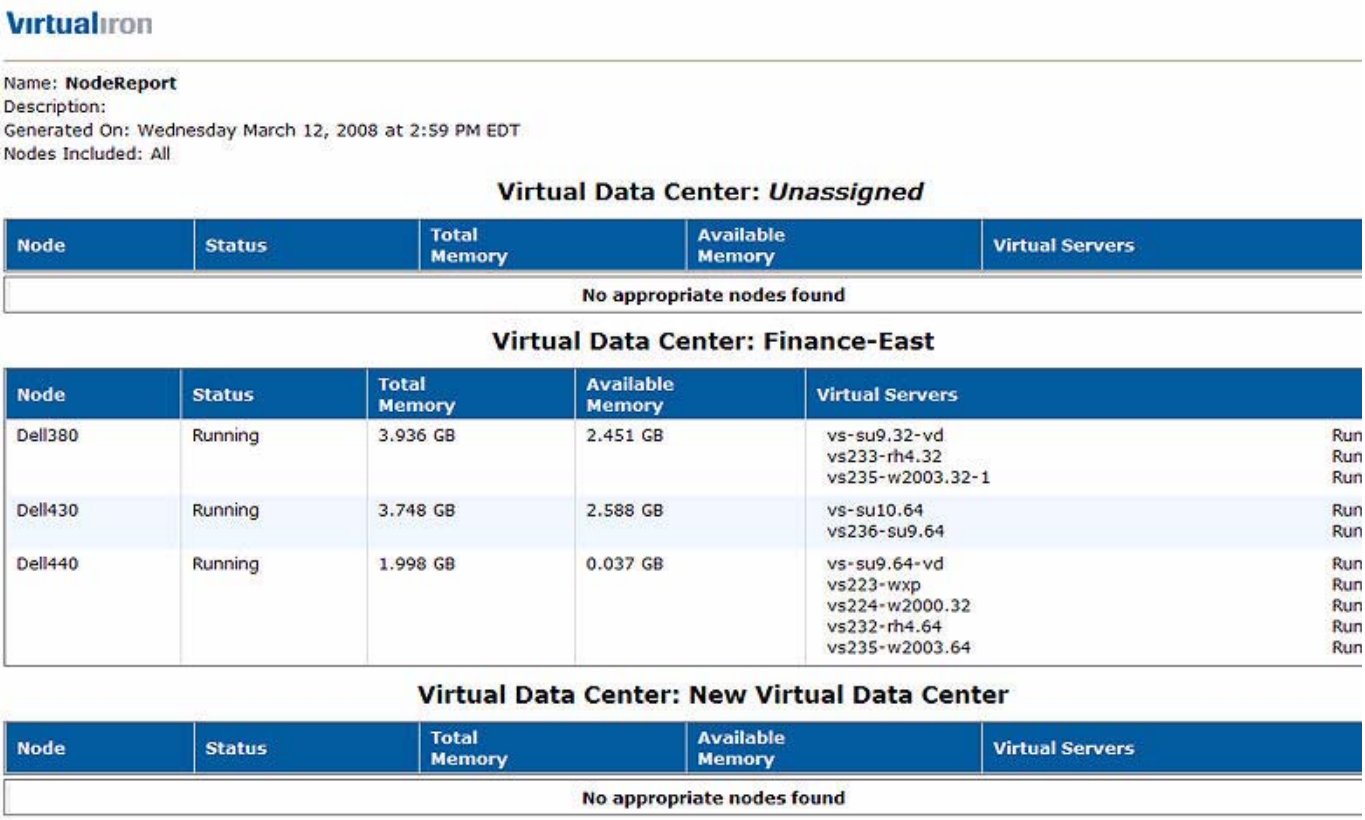
Step	Operation	Foundry Resource
1	Start Virtual Server vs-su9.64-vd - May not be combined with other job operations	Dell440

Time	Event	Source	Summary
Wed Mar 12 09:52 AM EDT 2008	JobConstructingEvent	This Job	Job Construction: 0 of 0
Wed Mar 12 09:52 AM EDT 2008	VirtualServerStartingEvent	vs-su9.64-vd	Virtual Server is Starting
Wed Mar 12 09:52 AM EDT 2008	JobRunningEvent	This Job	Job Running: 5 of 12
Wed Mar 12 09:53 AM EDT 2008	JobFailureEvent	This Job	Job Internal Error (Operation): 7 of 12
Wed Mar 12 09:53 AM EDT 2008	JobRollbackEvent	This Job	Job Rollback Starting: 7 of 12
Wed Mar 12 09:53 AM EDT 2008	VirtualServerStoppedEvent	vs-su9.64-vd	Virtual Server is Stopped
Wed Mar 12 09:53 AM EDT 2008	SeverityChangeEvent	vs-su9.64-vd	Changed Severity [Critical to Minor]
Wed Mar 12 09:53 AM EDT 2008	JobRollbackDoneEvent	This Job	Job Rollback Done: 7 of 12
Wed Mar 12 09:53 AM EDT 2008	JobFailureEvent	This Job	Job Failed to Complete: 6 of 12

NODE REPORT

Report criteria that you can select for a Node Report include Running, Stopped, In Error, Protected, and VI Tools Enabled. These criteria may be applied against New or Unassigned data centers, a specific data center or All. Figure 130 is an example of a report in which All was selected.

Figure 130. Node Report Sample



VirtualIron

Name: **NodeReport**
Description:
Generated On: Wednesday March 12, 2008 at 2:59 PM EDT
Nodes Included: All

Virtual Data Center: *Unassigned*

Node	Status	Total Memory	Available Memory	Virtual Servers
No appropriate nodes found				

Virtual Data Center: Finance-East

Node	Status	Total Memory	Available Memory	Virtual Servers	
Dell380	Running	3.936 GB	2.451 GB	vs-su9.32-vd vs233-rh4.32 vs235-w2003.32-1	Run Run Run
Dell430	Running	3.748 GB	2.588 GB	vs-su10.64 vs236-su9.64	Run Run
Dell440	Running	1.998 GB	0.037 GB	vs-su9.64-vd vs223-wxp vs224-w2000.32 vs232-rh4.64 vs235-w2003.64	Run Run Run Run Run

Virtual Data Center: New Virtual Data Center

Node	Status	Total Memory	Available Memory	Virtual Servers
No appropriate nodes found				

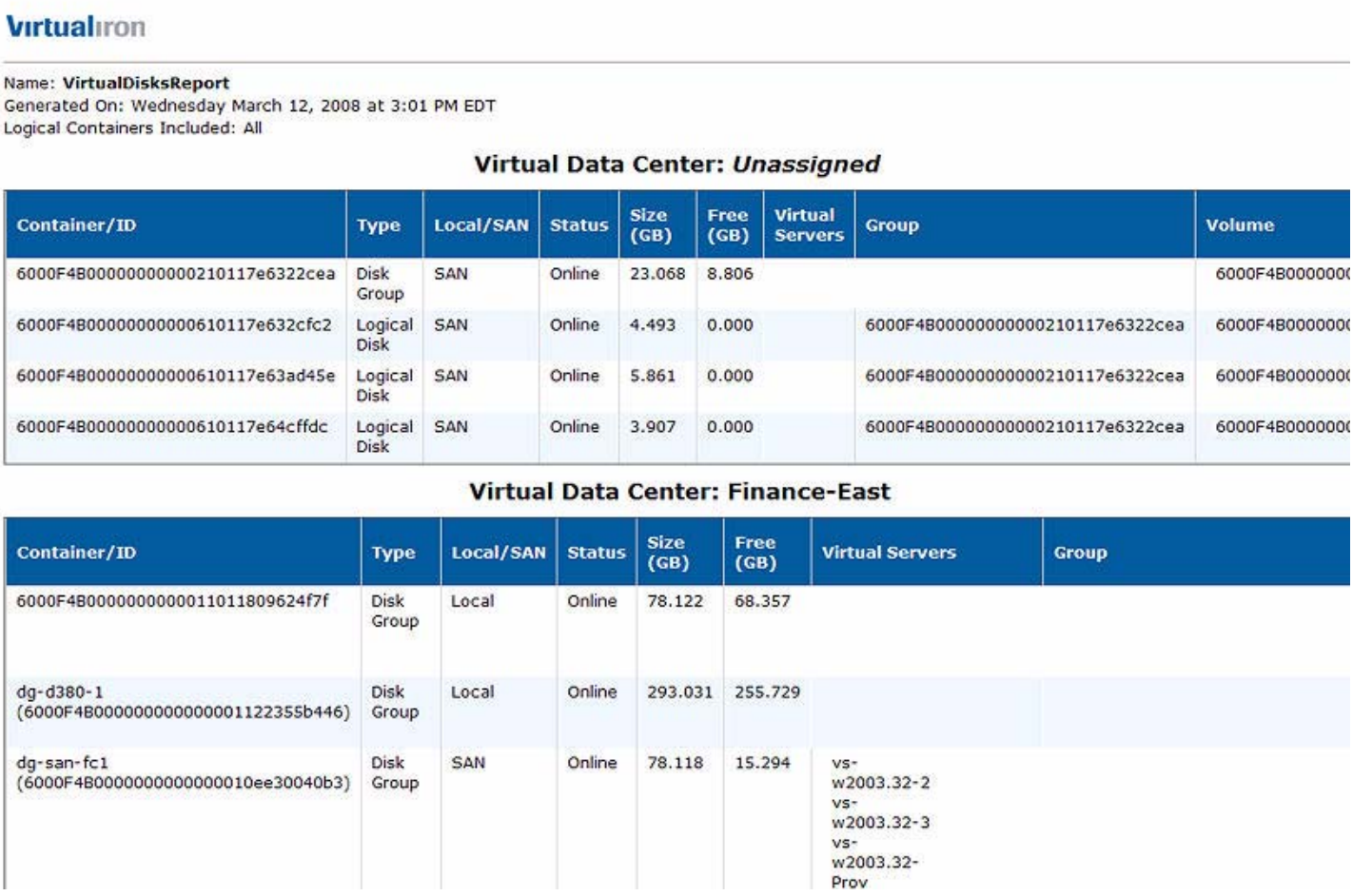
VIRTUAL DISKS REPORT

Report criteria that you can select for a Node Report include In Error, Assigned, Unassigned, Online, Offline, Mounted, Not Mounted, Shared Volume, Local Disk, and SAN Disk, or All.

You can apply these criteria to all logical containers, or limit the report to any combination of Groups, Volumes, or Virtual Disks. Figure 131 is an example of a report in which All was selected.

When you generate the report, scroll to the right to see all of its contents.

Figure 131. Virtual Disks Report Sample



VirtualIron

Name: **VirtualDisksReport**
Generated On: Wednesday March 12, 2008 at 3:01 PM EDT
Logical Containers Included: All

Virtual Data Center: *Unassigned*

Container/ID	Type	Local/SAN	Status	Size (GB)	Free (GB)	Virtual Servers	Group	Volume
6000F4B000000000000210117e6322cea	Disk Group	SAN	Online	23.068	8.806			6000F4B000000(
6000F4B000000000000610117e632cfc2	Logical Disk	SAN	Online	4.493	0.000		6000F4B000000000000210117e6322cea	6000F4B000000(
6000F4B000000000000610117e63ad45e	Logical Disk	SAN	Online	5.861	0.000		6000F4B000000000000210117e6322cea	6000F4B000000(
6000F4B000000000000610117e64cffdc	Logical Disk	SAN	Online	3.907	0.000		6000F4B000000000000210117e6322cea	6000F4B000000(

Virtual Data Center: Finance-East

Container/ID	Type	Local/SAN	Status	Size (GB)	Free (GB)	Virtual Servers	Group
6000F4B000000000001011011809624f7f	Disk Group	Local	Online	78.122	68.357		
dg-d380-1 (6000F4B000000000000000001122355b446)	Disk Group	Local	Online	293.031	255.729		
dg-san-fc1 (6000F4B0000000000000010ee30040b3)	Disk Group	SAN	Online	78.118	15.294	vs-w2003.32-2 vs-w2003.32-3 vs-w2003.32-Prov	

VIRTUAL SERVER REPORT

Report criteria that you can select for a Virtual Server Report include Running, Stopped, Suspended, Assigned, In Error, Auto-Recovered, Uses VS Tools, and Unassigned, or All.

You can apply these criteria to all virtual data centers, or limit the report to a New Virtual Data Center or a specific virtual data center. Figure 132 is an example of a report in which All was selected.

When you generate the report, scroll to the right to see all of its contents.

Figure 132. Virtual Server Report Sample

VirtualIron

Name: **VirtualServerReport**
Description: **Daily Report**
Generated On: Wednesday March 12, 2008 at 11:19 AM EDT
Virtual Servers Included: AutoRecovery-enabled, Use VS Tools

Virtual Data Center: Finance-East

Virtual Server	Status	Current Node	OS	Memory	CPUs	VS Tools	Boot Device	Disks
Snapshot of vs224-w2000.32	Stopped	Dell380	Microsoft Windows 2000	256 MB	2	**Yes**	Snapshot of ld-san-w2000.32-4.0 (6000F4B000000000006101189eecd26f)	Snapshot of ld-san-w2000.32-4.0 (6000F4B000000000006101189ee
Snapshot of vs235-w2003.32-1	Running	Dell380	Microsoft Windows Server 2003	256 MB	2	**Yes**	Snapshot of ld-san-w2k3.32-4.0 (6000F4B000000000006101189ee3a3b9)	Snapshot of ld-san-w2k3.32-4.0 (6000F4B000000000006101189ee
vs-or4.32		*Unassigned*	Red Hat Enterprise Linux 4	258 MB	2	**Yes**	ld-san-or4.32 (6000F4B000000000006101168778 8e24)	ld-san-or4.32 (6000F4B000000000006101168777
vs-rh4.64-vd		*Unassigned*	Red Hat Enterprise Linux 4	285 MB	2	**Yes**	vd-san-rh4.64.4-4.0 (6000F4B000000000000001109427 3743)	vd-san-rh4.64.4-4.0 (6000F4B000000000000000110942
vs-rh4.64.iscsi		*Unassigned*	Red Hat Enterprise Linux 4	257 MB	2	**Yes**	**None**	**None**
vs-su10.64	Running	Dell430	Suse Linux Enterprise Server 10	271 MB	2	**Yes**	ld-san-su10.64 (6000F4B000000000006101184 24d0b48)	ld-san-su10.64 (6000F4B000000000006101184 24
vs-su9.32-iscsi		*Unassigned*	Suse Linux Enterprise Server 9	269 MB	2	**Yes**	**None**	**None**
vs-su9.32-vd	Stopped	Dell380	Suse Linux Enterprise Server 9	283 MB	2	**Yes**	vd-san-su9.3-32-4.0 (6000F4B000000000000000 1109e14a8a3)	vd-san-su9.3-32-4.0 (6000F4B000000000000000 1109e1

SYSTEM POLICIES

System policies have system-wide application and run in the background according to specified parameters. Once started, they are always running. Virtual Iron® supports the system policies listed in Table 8.

Table 8. VI-Center™ System Policies

	Purpose
AutoRecovery™	Moves virtual servers on nodes that go offline to a healthy node and then restarts it in the event its host fails.The policy is run automatically by the system when AutoRecovery is enabled for a virtual server. Once enabled, AutoRecovery is applied on a per-server basis in the Resource Center view.
LiveCapacity™	Balances CPU utilization across selected nodes in a virtual data center by using LiveMigrate to perform virtual server migration without downtime. To balance CPU utilization across selected nodes in a virtual data center, enable LiveCapacity on the virtual data center's Live Capacity tab.
Technical Support	Access to Virtual Iron Technical Support.

AutoRecovery

AutoRecovery™ (LiveRecovery) is a system-wide policy that allows a virtual server to move and restart on a new node in the event its host node fails.

ENABLING AUTORECOVERY

Before enabling AutoRecovery/LiveRecovery, make sure your system meets the requirements listed in LiveRecovery™ in Creating and Configuring Virtual Servers.

For other information and configuration procedures, see Configuring LiveRecovery™.

SCHEDULING AUTORECOVERY

You may optionally choose start and stop dates and times to schedule AutoRecovery during peak periods. See Scheduling Policies.

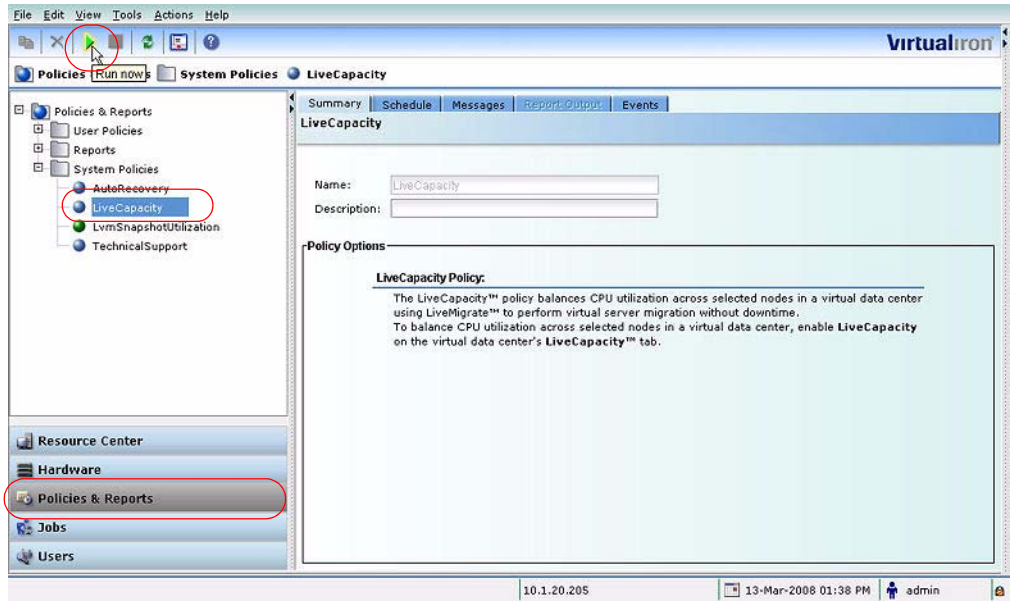
LiveCapacity

LiveCapacity™ is a system-wide policy that enables load-balancing of virtual servers within virtual data centers. The nodes you want to configure with LiveCapacity are selected individually within the Resource Center view. For more information and procedures, see Configuring LiveCapacity®.

MONITORING LIVECAPACITY

LiveCapacity is automatically started when configured. From the Policies and Reports view you can monitor the policy, schedule its execution, view messages and events. Should you need to, you can stop the policy in this view as well.

Figure 133. Starting a Policy



SCHEDULING LIVECAPACITY

To schedule LiveCapacity to better optimize load-balancing according to established traffic patterns in your data center, see Scheduling Policies.

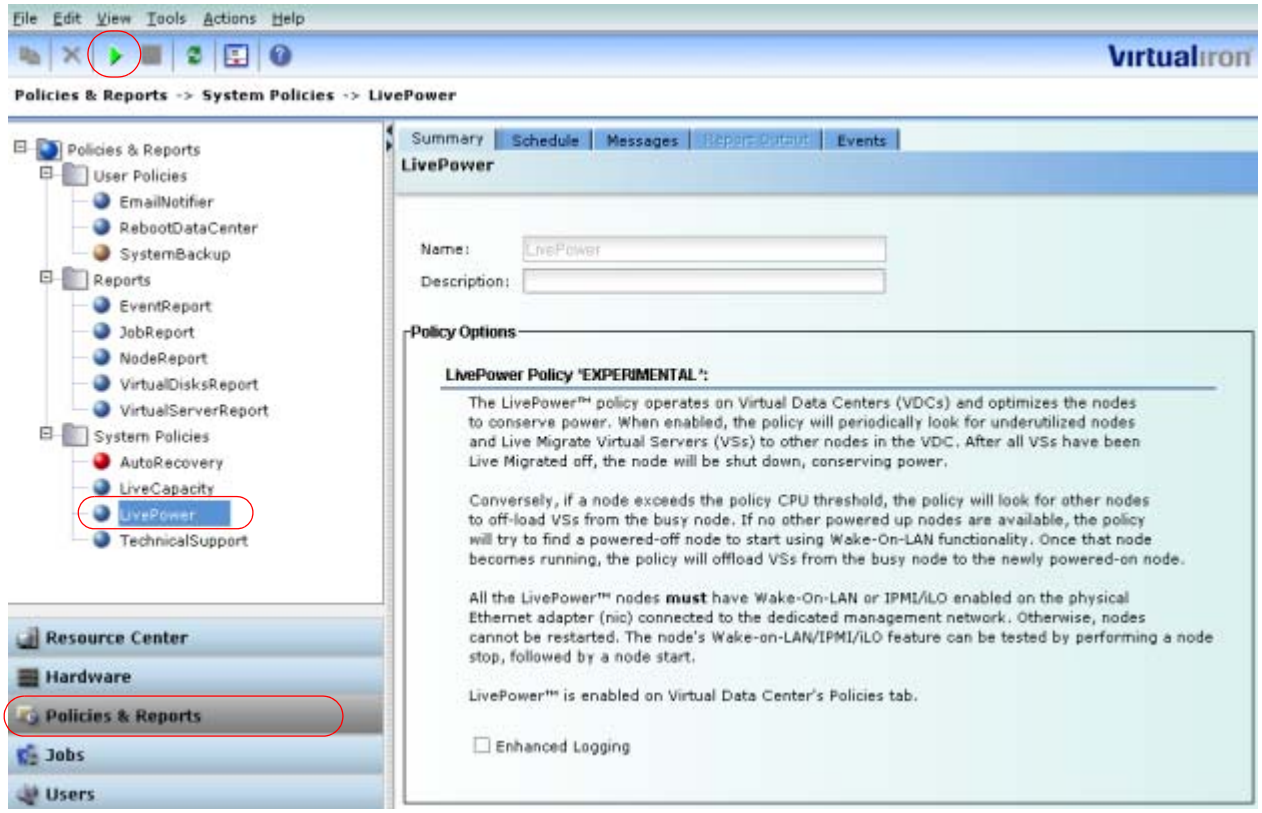
LivePower

LivePower™ is a system-wide policy that enables load-balancing of virtual servers within virtual data centers. The nodes you want to configure with LivePower are selected individually within the Resource Center view. For more information and procedures, see Configuring LivePower™.

MONITORING LIVEPOWER

LivePower is automatically started when configured. From the Policies and Reports view you can monitor the policy, schedule its execution, view messages and events. Should you need to, you can stop the policy in this view as well.

Figure 134. Starting LivePower



SCHEDULING LIVEPOWER

To schedule LivePower to better optimize load-balancing according to established traffic patterns in your data center, see Scheduling Policies.

SCHEDULING POLICIES

You can schedule AutoRecovery or LiveCapacity to be performed on a recurring basis. For example, you may want to turn off LiveCapacity during periods of low use to optimize the management server's CPU processing.

Note: If you are changing the scheduled time or frequency of a configured policy, you must first stop the current policy. To do so, click the red **Stop** icon in the action toolbar at the top of the window.

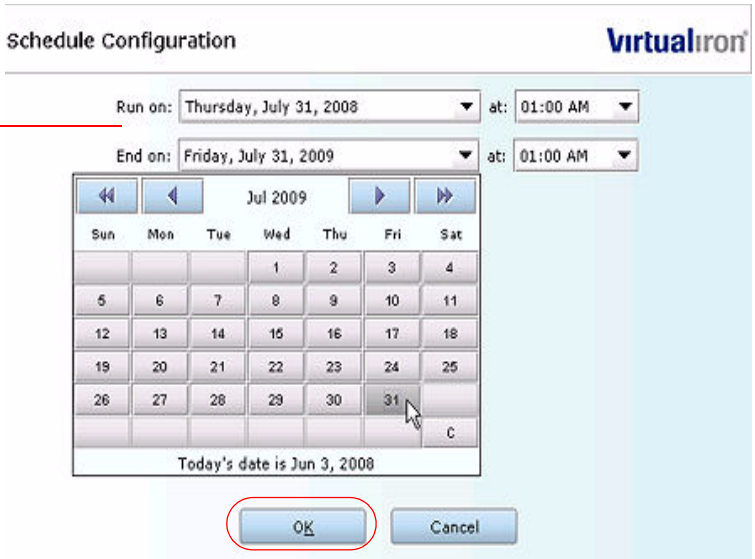
Step 1. In the **Policies & Reports** navigation tree, under **System Policies**, click **AutoRecovery** or **LiveCapacity**.

In the Policy Options window for AutoRecovery, check **Enhanced Logging** only for temporary troubleshooting purposes. This option produces large files which are stored in the data base.

Step 2. Click the **Schedule** tab. Click the **Edit** button.

Step 3. In the **Schedule Configuration** window, use the dropdown menus to choose start and stop dates and (optionally) times. Click to highlight the hour or minutes and use the up and down arrows to specify the time.

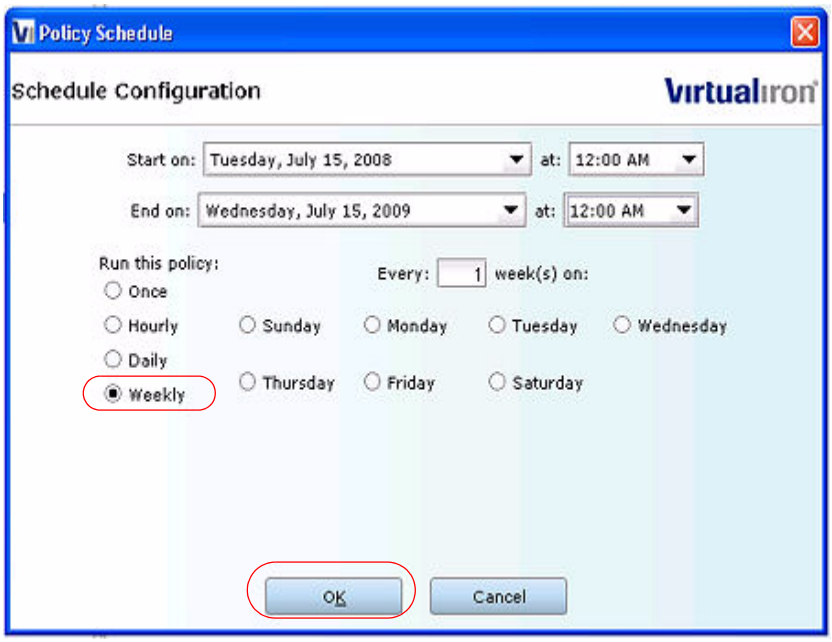
Figure 135. Email Policy, Schedule Tab



Step 4. Specify a run schedule for the policy. You can choose to run a policy once (immediately), daily, weekly, or monthly. See Figure 136. Click the down arrow in the **Start on** and **End on** fields to open a calendar.

If you choose to run a policy immediately, you do not have to specify a date—only the start time.

Figure 136. Schedule Configuration Window



Step 5. Click **OK**.

Step 6. Click the **Start** icon in the task bar.

Step 7. Once the policy has been started, you can click the **Messages** or **Events** tabs for additional information.

8

PERFORMING ADMINISTRATIVE TASKS

This chapter shows how to perform a number of administrative tasks. It contains the following sections.

CONFIGURING USER ACCOUNTS AND ROLES

VI-Center supports user accounts and associated passwords. These accounts can be local, or can exist on an LDAP server. The following section describes how to configure local accounts. See Configuring LDAP for information on configuring LDAP authentication.

Creating Local User Accounts

Only an admin user can create or delete Local user accounts. A default admin account, with username and password **admin,** is created during installation of the software (see Installing Virtual Iron®). To create additional accounts:

Step 1. Log in to VI-Center™ as **admin**.

Step 2. Click **Users** in the Applications Shortcuts or select **Users** from the **View** menu. The Users accounts view opens. See Figure 137.

Step 3. To create a new user account, right-click **Users** in the navigation tree or select **New User Account** from the **File** menu. See Figure 138.

Figure 137. User Account View

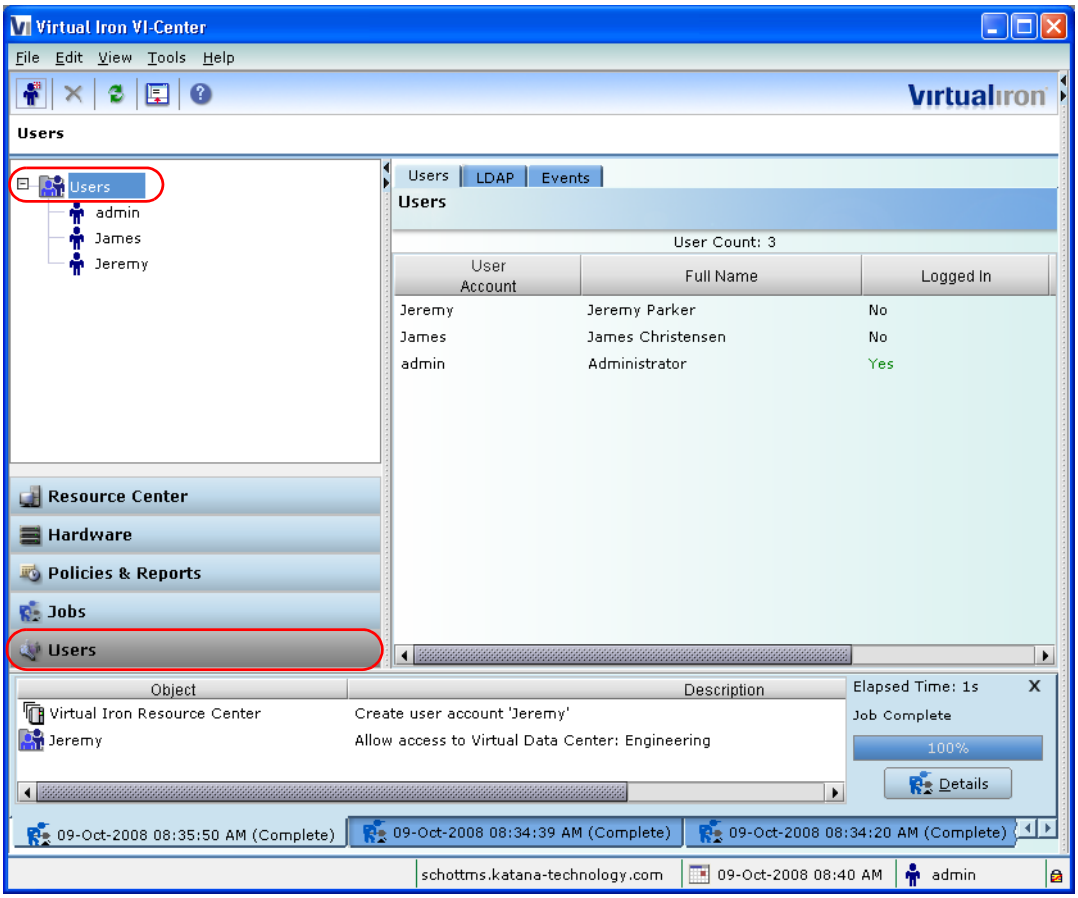
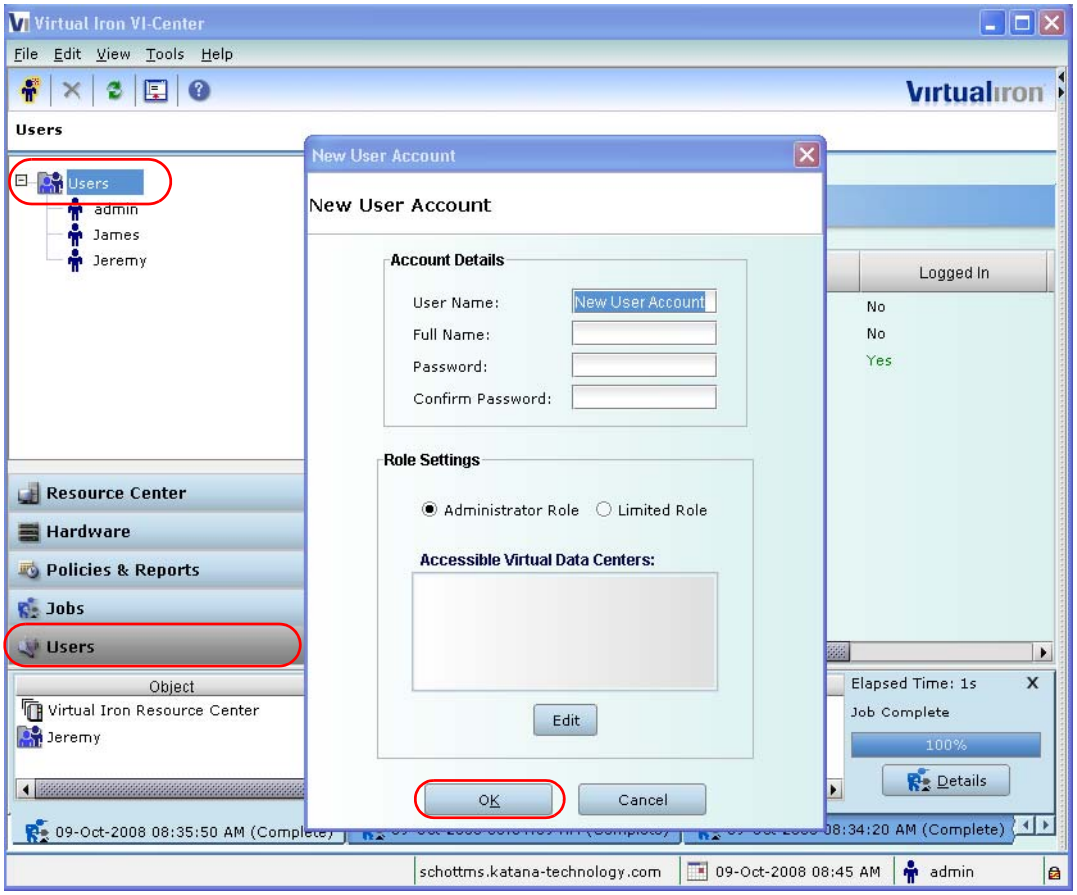


Figure 138. Creating a New User Account



Step 4. The default name *New User Account* is assigned to the account. Enter the user's full name and then enter and confirm a password for the user.

Step 5. Click the **Edit** button.

Step 6. In the **Assign Virtual Data Centers to Users** window, select the VDC or VDCs you want the user to have access to and click the **Add** button and click **OK**.

Step 7. Click **OK** in the New User Account window.

Refresh the screen to see the user's name in the navigation tree.

Changing a User Password

Use the following procedure to change a user password:

Step 1. Select the **User** shortcut.

Step 2. Select the account for which you want to change the password.

Step 3. Select **Edit > User Account**.

Step 4. In the Edit User Account window, do the following:

A. Enter the old password for the account in the **Existing Password** field.

B. Enter the new password in the **Password** field.

C. Enter the new password again in the **Confirm Password** field.

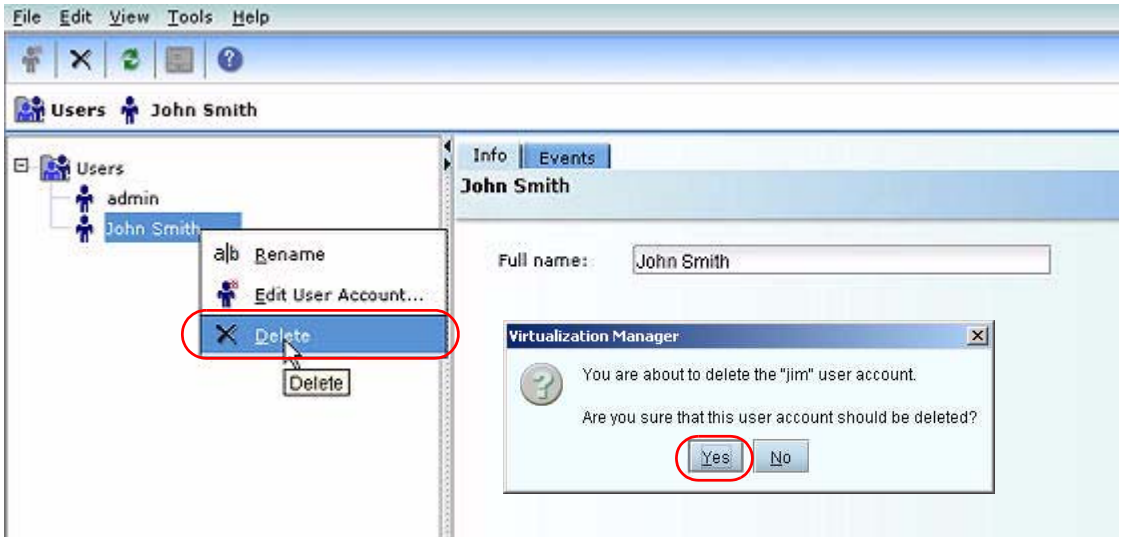
Step 5. Click **OK**.

The new password takes effect when you restart VI-Center

Deleting User Accounts

Only personnel with admin privileges are allowed to delete user accounts. Select the User account in the navigation tree, right-click and select **Delete** or click the **Delete** icon in the toolbar. See Figure 139.

Figure 139. Deleting User Accounts



Editing Account Information

To edit user account information, select an account in the navigation tree and select **Edit User Account**. The dialog box shown in Figure 140 appears. Make the changes, and click **OK**.

Figure 140. Editing Account Information

WORKING WITH ROLES

When you create a new user account a corresponding role is also created.

About User Accounts and Roles

There are two types of roles:

- Admin role—The role created during installation. The admin role is the only one which can create and delete user accounts.
- User role—Users can either have the Administrator Role enabled or the Limited Access enabled.

The administrator role is always **admin**. Non-administrator roles can be anything except admin.

ROLE-BASED ACCESS

Roles allow for Role-based Access which gives you the ability to restrict access to data in the VI-Center. The following table describes the objects

which Role-based Access can restrict access to:

	Description
VDC (Virtual Data Center)	The admin role can add or remove a user's access at the VDC level
Node	The admin role can add or remove a user's access at the node level
VI-Center Functionality	Several features are unavailable to non-admin users.

THE ADMIN ROLE

The admin role is the only one which can do the following:

	Description
Create new user accounts	Users may change their password, but only admin can create or delete a user account.
Create a VDC	You must sign in as admin to create or delete a VDC.
Assign VDCs to a user	Only the Administrator role can assign or unassign a VDC to a user.
Edit user's access	Non-admin users can't edit other users accounts or change their access.
See all user's jobs in the Job view	Only the admin user can view the jobs of all users.

USER ROLES—ADMINISTRATOR ROLE

A user with the Administrator Role can do the following things a user with Limited Role can't:

Administrator Role Functionality	Description
Modify anything in the Hardware view	All options in the Hardware view are grayed out unless you are logged in as admin or have the Administrator Role as a user.
File Manager Tools	Only the admin user can use the File Manager.
VHD Repository Manager	The VHD Repository Manager is unavailable in the Tools menu for all Limited Role users.
NBD Repository Manager	The NBD Repository Manager is unavailable in the Tools menu for all Limited Role users.

Administrator Role Functionality	Description
Update Manager	The Update Manager is unavailable in the Tools menu for all Limited Role users.
See all user's jobs in the Job view	Only the admin user can view the jobs of all users.

USER ROLES—LIMITED ROLE

Users with Limited Role selected can change their password.

Editing User Roles

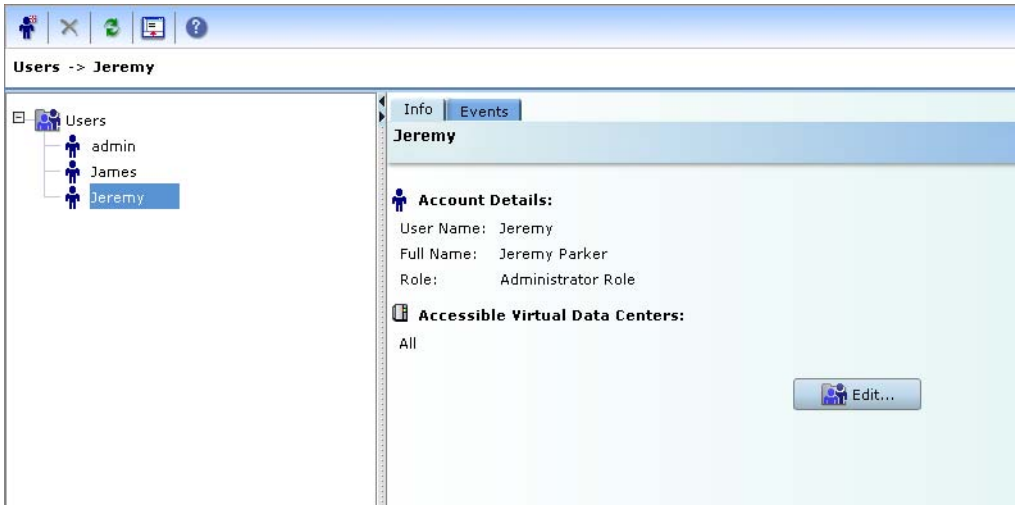
You can edit user roles if you are logged in as admin.

EDITING A USER'S ACCESS

Only an someone with the **admin** role can edit a role's access to a VDC.

Step 1. Select the **User** shortcut.

Step 2. Click the Edit button in the right pane.



Step 3. In the **Edit User Account** window, click the **Edit** button.

Step 4. In the **Assign Virtual Data Centers to Users** window, select a VDC in the left pane and click **Add** to give access to the user, or select a VDC in the right pane and click **Remove** to remove access.

Step 5. Click **OK** in the **Assign Virtual Data Centers to Users** window.

Inspecting a User Account

You can view the VDC access for each user from the User shortcut.

VIEWING A USER'S VDC ACCESS

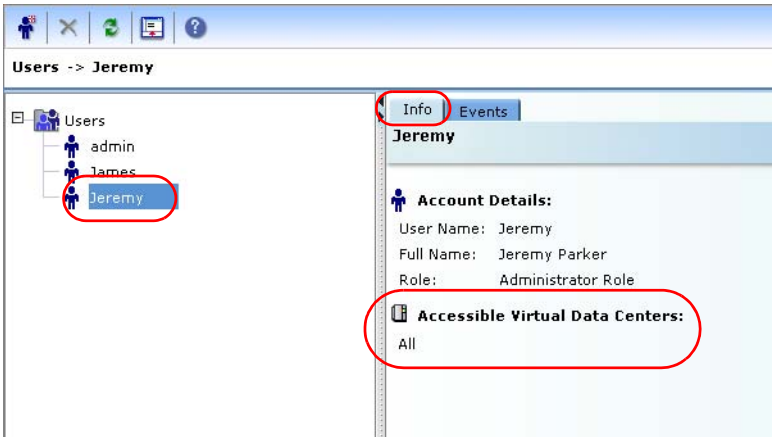
Step 1. Select the **User** shortcut.

Step 2. Select the user whose access you want to view.

Step 3. Click the **Info** tab.

Step 4. The VDCs the user has access to are listed under the **Accessible**

Virtual Data Centers heading.



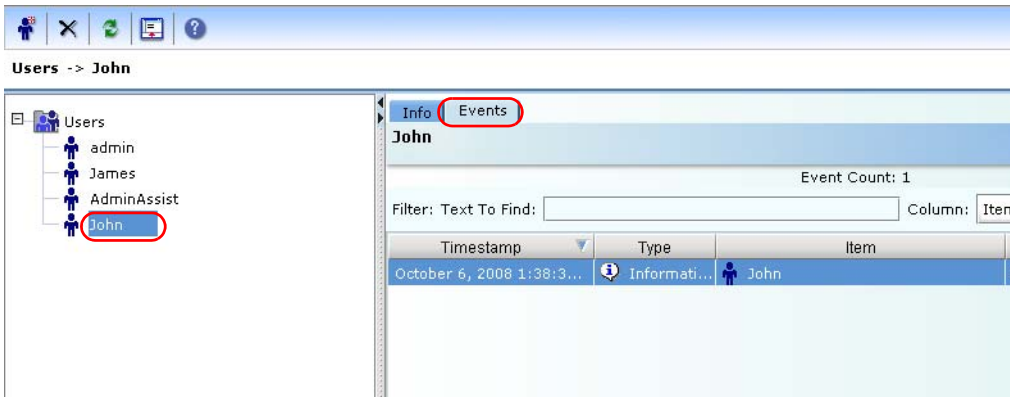
VIEWING A USER'S ACTIVITY

Step 1. Select the **User** shortcut.

Step 2. Select the user whose access you want to view.

Step 3. Click the **Events** tab.

Step 4. The events initiated by the user appear in the right pane.



CONFIGURING LDAP

In addition to local user accounts, VI-Center supports LDAP authentication (Lightweight Directory Access Protocol) via a centralized database.

Virtual Iron® supports both Microsoft Active Directory (for Windows®) and Open LDAP for Linux distributions.

About LDAP Authentication

LDAP is a protocol used to store and access information in a directory. LDAP has the advantage of being platform-independent and standards-based. Applications do not need to know what type of server is hosting the LDAP directory to communicate with it. The server can be any one of a number of commercial or open-source LDAP directory servers—even a DBMS server with an LDAP interface).

LDAP Support and Administration

To use LDAP, you need to provide a set of LDAP criteria and enable the LDAP protocol on VI-Center. Only personnel with **admin** privileges are allowed to log in to the VI-Center or make changes to the LDAP configuration.

Note: To use LDAP over SSL, you must import the LDAP SSL certificate into the java keystore of the VI-Center.

When LDAP is enabled, the user accounts on the local server are disabled. However, local account information remains on the management server and can be used again if LDAP is disabled.

LDAP Component Information

LDAP directories store data hierarchically, similar to DNS trees, or Unix directories. Though LDAP implementations may differ slightly, they preserve a common set of components that are used in specific ways. The components include the following:

Component Name	Abbreviation	Definition
Distinguished Name	dn	The top level of the LDAP directory tree is the base DN.
Common Name	cn	When using LDAP to authenticate users of Virtual Iron®, the common name refers to a user's full name.

Component Name	Abbreviation	Definition
Organization	o	The organization component.
Domain Component	dc	The domain component.
Organizational Unit	ou	Organizational units that further subdivide information in a dc.

Configuring Virtual Iron To Authenticate with LDAP

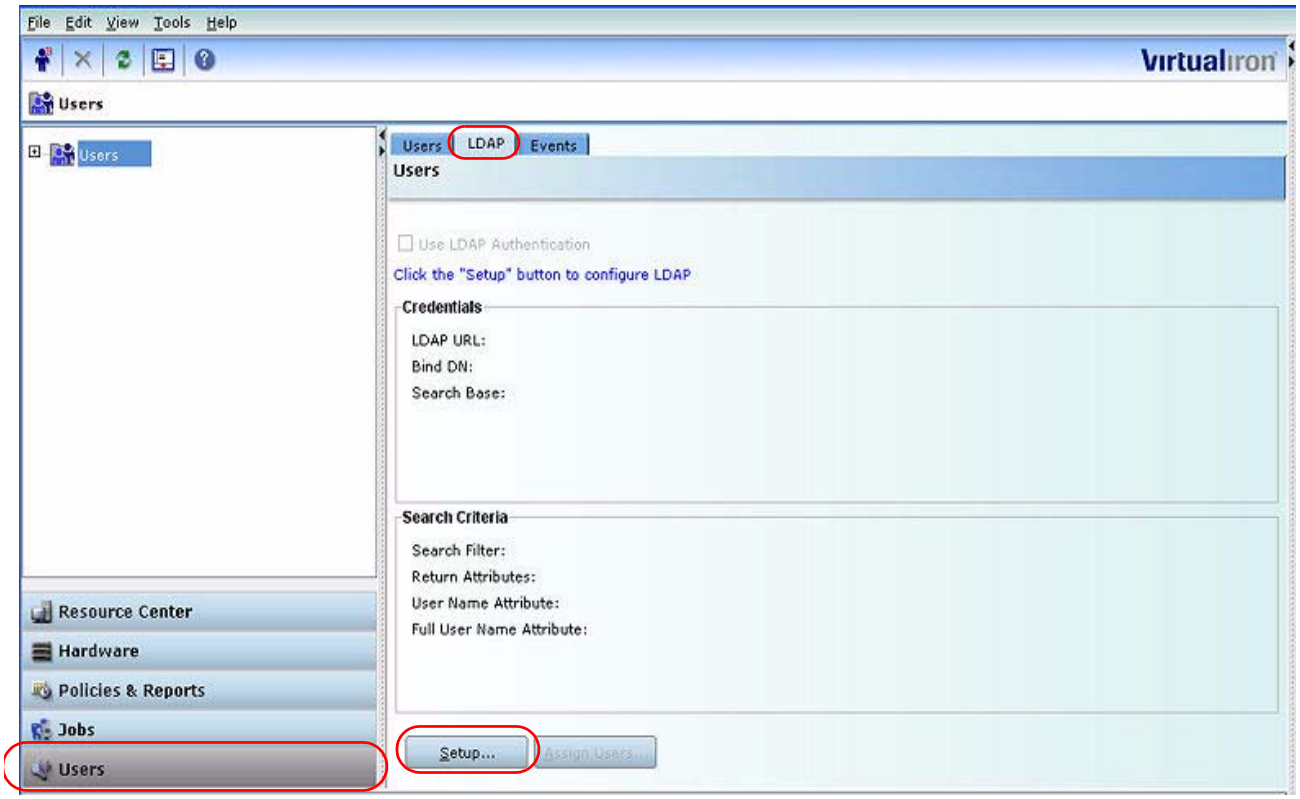
LDAP authentication requires enabling VI-Center to access user information stored on an LDAP server and enabling the LDAP protocol.

You need to know which LDAP implementation is in use at your site. The implementation determines the proper syntax to use to pass LDAP credentials and search criteria to the LDAP server. For information on the LDAP components to pass and the proper syntax, contact your LDAP system administrator.

To configure LDAP authentication for the VI-Center:

Step 1. Click **Users** on the application toolbar. Select the **LDAP** tab. The screen shown in Figure 141 appears.

Figure 141. LDAP Authentication Tab

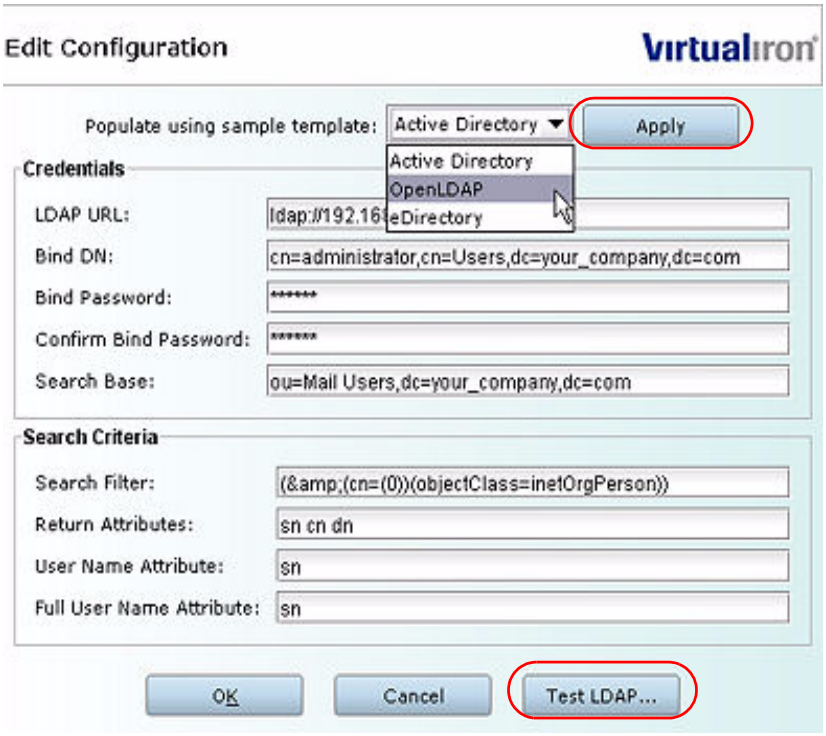


Step 2. The LDAP tab has two panes, which are blank initially. Once you have set up LDAP (Step 3), these panes are populated with the credentials and search criteria you specified.

- **Credentials**—Records the URL of the LDAP server, the server's distinguished name (DN), and the LDAP search base within that DN. The search base defines the specific location in the LDAP directory from which your LDAP search will begin.
- **Search Criteria**—Provides the criteria used to match against the user data stored in the LDAP search base. VI-Center applies the criteria you enter to filter the data. When it connects to the LDAP server, VI-Center uses these criteria to identify a set of users. Use the **Assign Users...** dialog to add some or all of them to the list of those that can manage within the Virtual Iron® framework.

Step 3. Before you can enable LDAP, you need to add or edit LDAP Credentials and Search criteria. To do this, click **Setup...** The dialog shown in Figure 142 is displayed. In this example, LDAP information has been added to the template.

Figure 142. Entering LDAP Credentials and Search Criteria

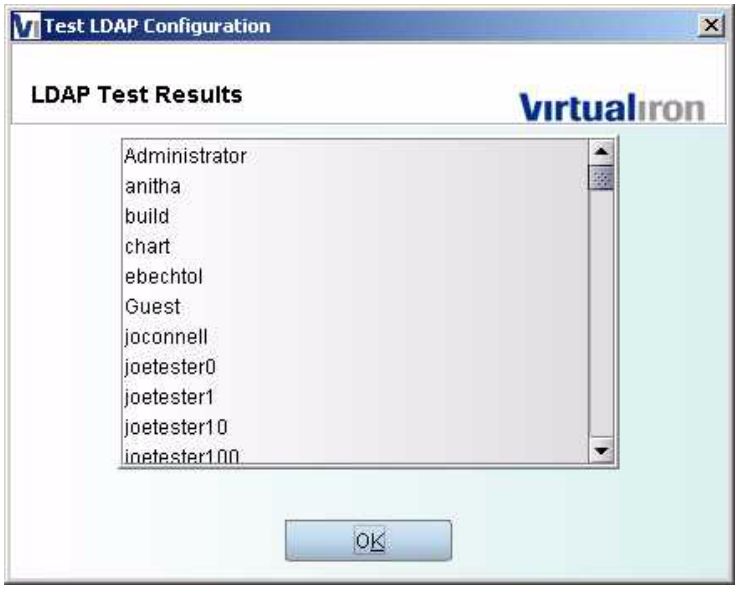


Step 4. Select a sample template to modify:

- **Active Directory**—An implementation of LDAP Directory Services for use in Microsoft Windows environments.
- **OpenLDAP**—A free, open source implementation of LDAP. Platform independent. Several common Linux distributions include OpenLDAP.
- **eDirectory**—Supports Windows 2000 and Windows 2003, SUSE Linux Enterprise Server, Red Hat Enterprise Linux, among other operating systems.

Step 5. Edit LDAP credentials and search criteria. Click **Test LDAP** to validate the data. VI-Center connects with the LDAP server and uses the search criteria you provided to return a list of users. Figure 143 shows a sample of the test results window. Click **OK** to accept the configuration.

Figure 143. Adding LDAP User Data to the VI-Center Database



Following are examples of valid parameters for the implementation of LDAP in Active Directory, and OpenLDAP.

Sample LDAP Data, Active Directory

Credentials

URL:ldap://10.1.20.3/

DN: cn=Adminstrator,cn=Users,dc=qadev,dc=local

DN Password: *password*

LDAP Search Base: cn=Users,dc=qadev,dc=local

Search Criteria

Search Filter: (& sAMAccountName={0}(objectClass=User))

LDAP User Name: userPrincipalName sAMAccountName name

LDAP Full User Name: sAMAccountName

Sample LDAP Data, OpenLDAP

Credentials

URL: ldap://123.45.67.23

DN: cn=admin,cn=Users,dc=qatest,dc=com

DN Password: *password*

LDAP Search Base: ou=users,dc=qadev,dc=local

Search Criteria

Search Filter: (& (cn={0})(objectClass=inetOrgPerson))

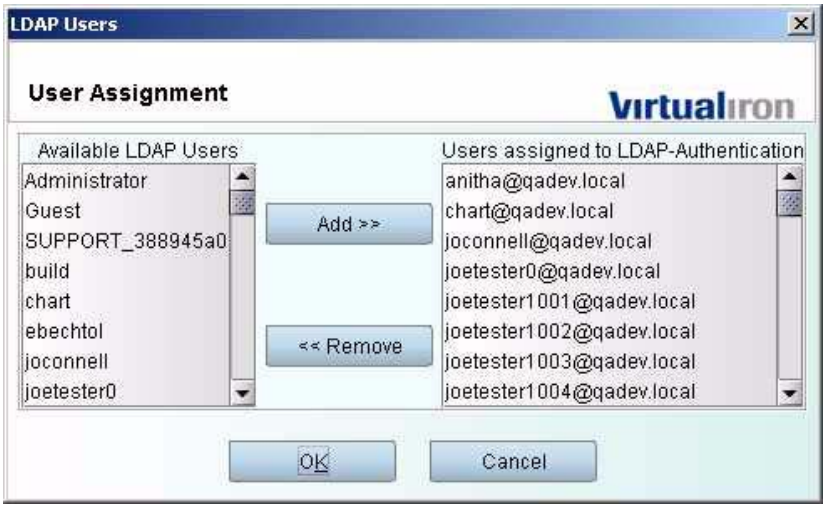
LDAP User Name: cn uid

LDAP Full User Name: cn

Step 6. After the LDAP credentials have been validated, you are ready to assign LDAP users. Click **Assign Users...** The dialog box that appears contains all of the users VI-Center has found on the LDAP server. A sample is shown in Figure 144.

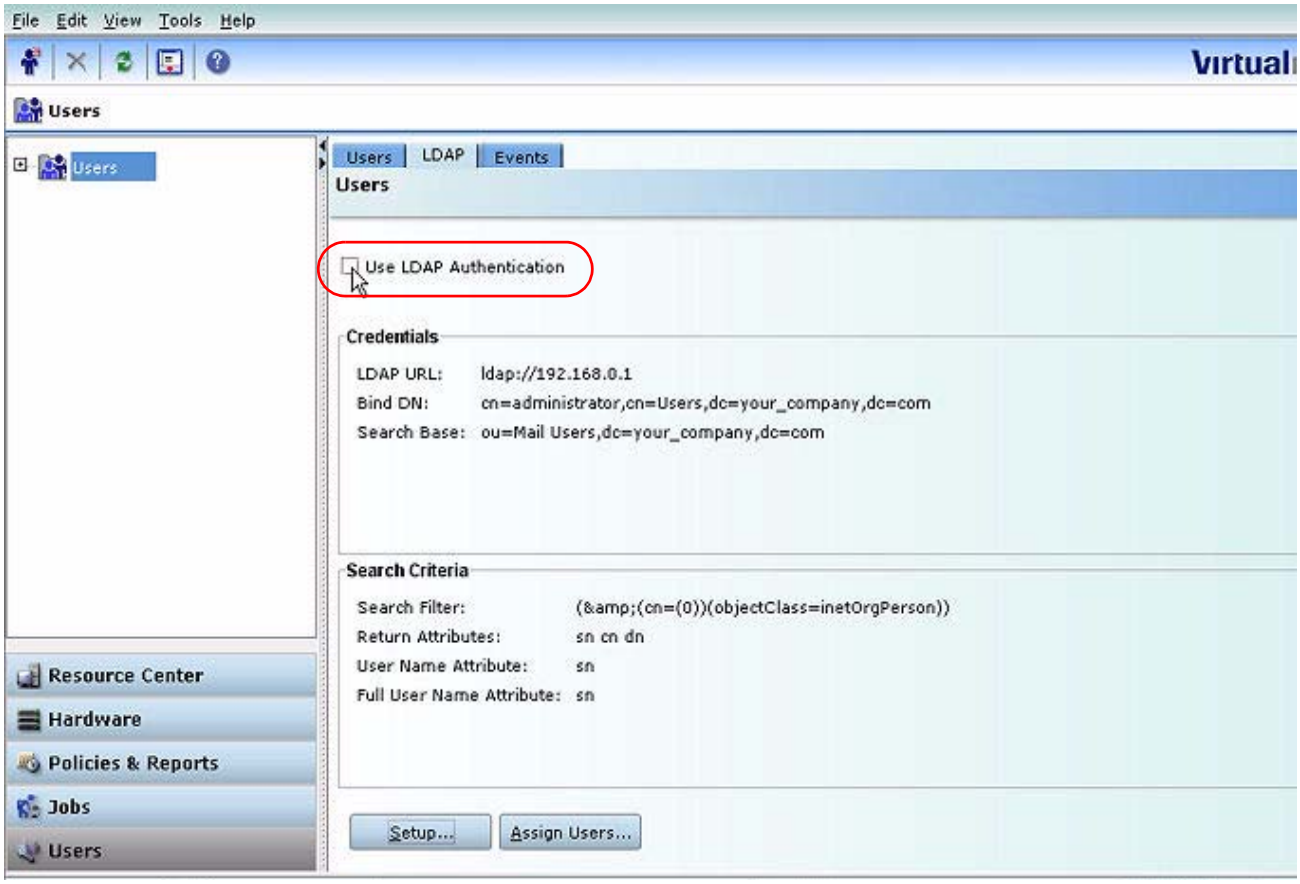
To assign one or more of these users to the list stored on the management server, use the **Add>>** and **<<Remove** keys to move users from the left to the right pane. Click **OK**.

Figure 144. Adding LDAP User Data to the VI-Center Database



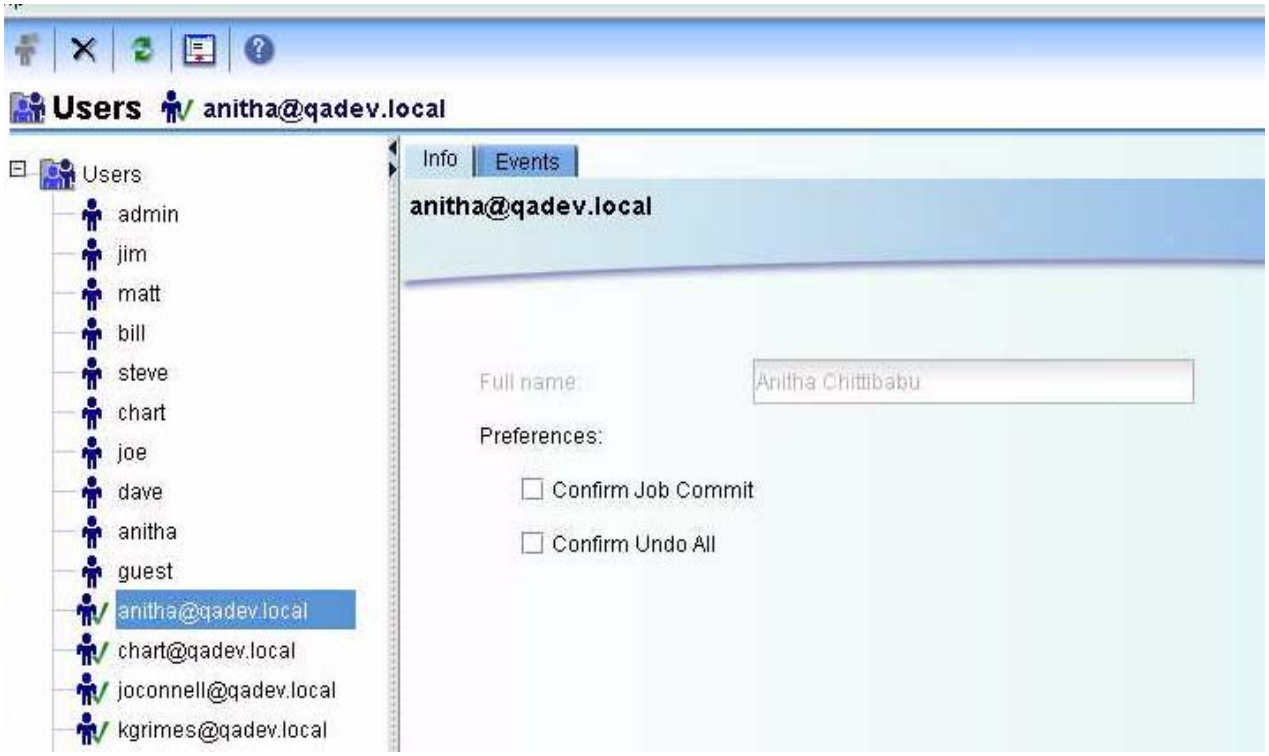
Step 7. Click **Enable LDAP** as shown in Figure 145.

Figure 145. Enable LDAP



Step 8. The LDAP users you have assigned appear on the management UI. A green check mark next to the User icons identifies users authenticated with LDAP, as shown in Figure 146. The user names that appear in the navigation tree is data retrieved via LDAP based on the User Name attribute. The Full Name information is retrieved via LDAP based on the Full User Name Attribute.

Figure 146. LDAP Users Added to the Virtual Iron Database



Changing the LDAP Configuration

Only personnel with Admin privileges can make changes to the LDAP configuration.

You cannot edit LDAP search criteria while LDAP is enabled. To make changes to the criteria, uncheck the **Enable LDAP** check box. Then click **Setup...** and make whatever changes are required. Test the changes and check **Enable LDAP** to re-enable the protocol.

Note that while LDAP is disabled, local users can connect to the VI-Center and manage resources.

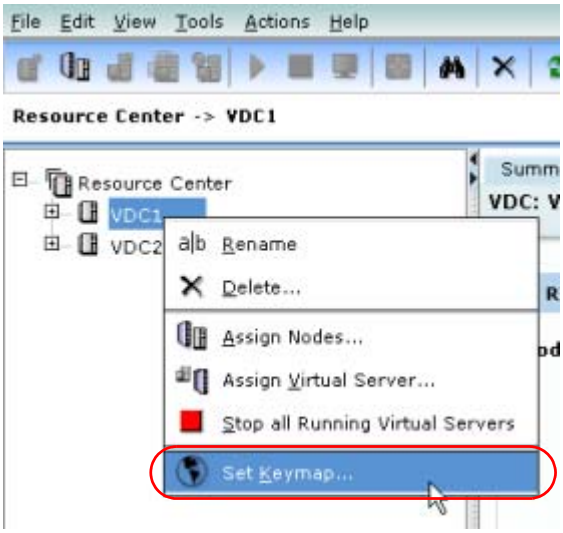
CONFIGURING NON-ENGLISH KEYBOARDS

You can configure all of your networks to a single language keymap, or individual Virtual Data Centers and virtual servers to separate language maps.

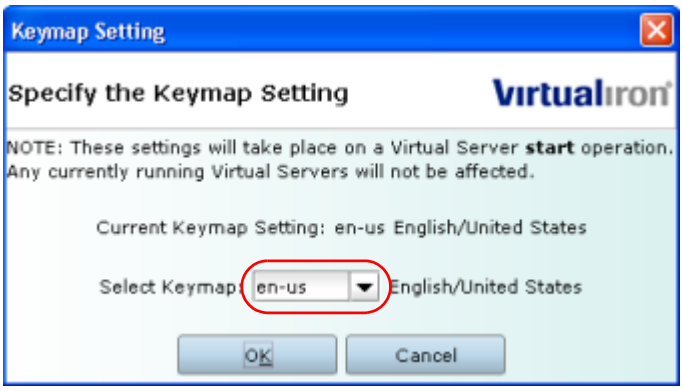
Set a Language Keymap

Step 1. In the Resource Center, right-click on Resource Center, a VDC, or a virtual server. The language code is a hierarchical setting affecting all entries in the tree below, so a setting on a VDC, for example, affects all virtual servers in that VDC.

Step 2. From the menu that appears, select Set Keymap.



Step 3. In the Keymap Setting dialog which appears.



Step 4. Select a language keymap setting. The table below lists each of the codes in the dropdown menu and which language they correspond to:

Supported Key Map Codes			
Argentina	ar	Danish	da
German	de	Swiss-German	de-ch
British-English	en-gb	American-English	en-us
Spanish	es	Estonian	et
Finnish	fi	Faroese	fo
French	fr	Beligan-French	fr-be
Canadian-French	fr-ca	Swiss-French	fr-ch
Croatian	hr	Hungarian	hu
Icelandic	is	Italian	it
Japanese	ja	Lituanian	lt
Latvian	lv	Macedonian	mk
Dutch	nl	Belgian-Dutch	nl-be
Norwegian	no	Polish	pl
Portuguese	pt	Brazillian-Portuguese	pt-br
Russian	ru	Slovenian	sl
Swedish	sv	Thai	th
Turkish	tr		

Step 5. Click OK.

PERFORMANCE STATISTICS

VI-Center provides performance and activity statistics on nodes and virtual servers.

Node statistics are available at all times; statistics on virtual servers are available only if VStools has been installed on the virtual server being monitored. See Installing VS Tools on Virtual Servers for information.

VI-Center collects and presents statistics for these areas:

- Resources & Activity for the Resource Center
- Last 5 Errors
- System-Wide Node Performance
- System-Wide Virtual Server Performance

- License Usage
- Active Policies
- User Connections

Each of these data categories are organized in a dashboard in the Resource Center's **Summary** screen.

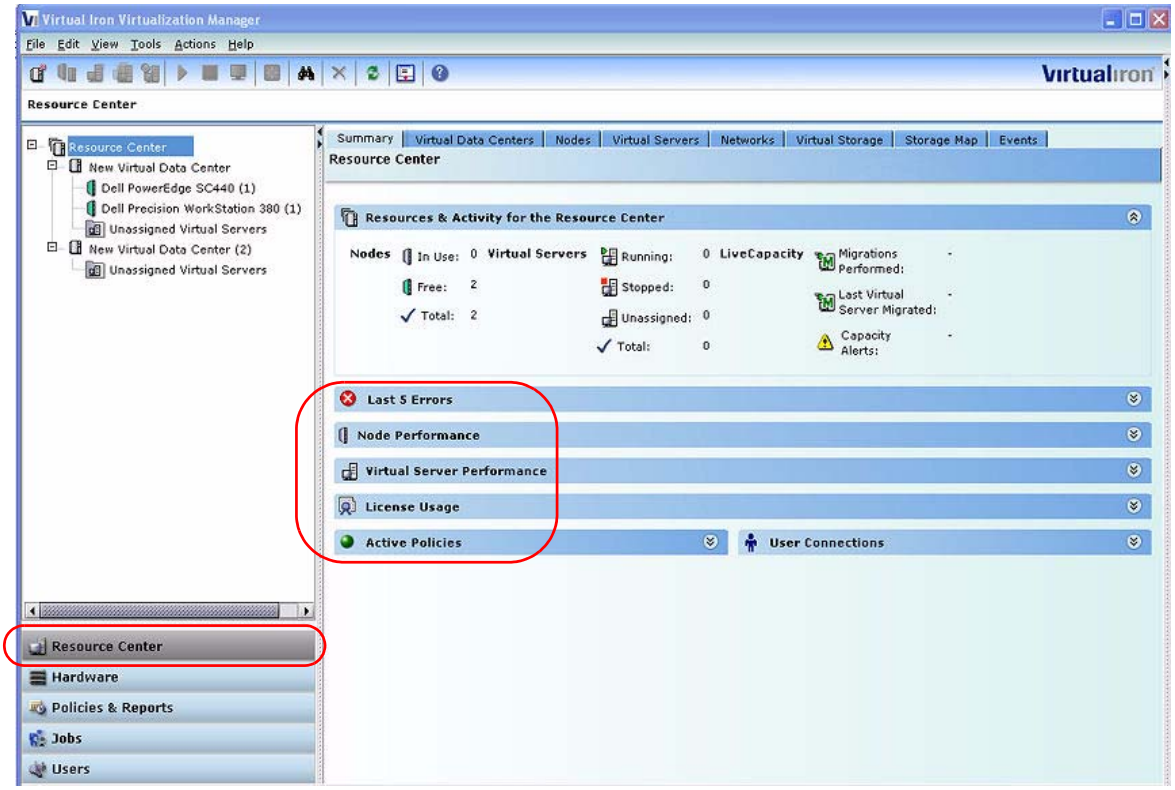
Accessing Performance Statistics

To view performance statistics in VI-Center, do the following:

Step 1. In the **Resource Center** view, select **Resource Center** in the navigation tree. The Resource Center window opens with the **Summary** tab active.

Step 2. Click one or more of the performance statistics categories displayed in the dashboard. See Figure 147.

Figure 147. Resource Center Activity Screen, showing dashboard options



RESOURCES & ACTIVITY FOR THE RESOURCE CENTER

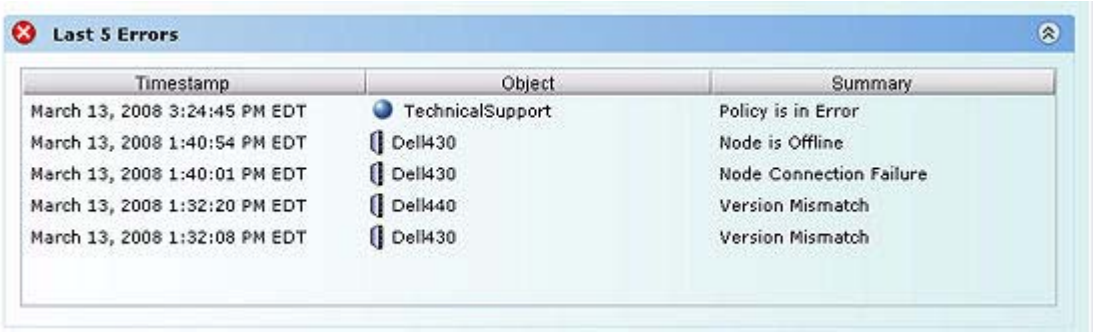
Figure 148 shows a close-up of the initial screen with Resource Center level data for Nodes, Virtual Servers, and LiveCapacity.

Figure 148. Resource and Activity Data

LAST 5 ERRORS

To view the last five errors associated with the Resource Center, select Resource Center in the navigation tree. In the Summary screen, click the **Last 5 Errors** tab. Error data is displayed with a timestamp of the occurrence, the object, and a brief summary of the issue.

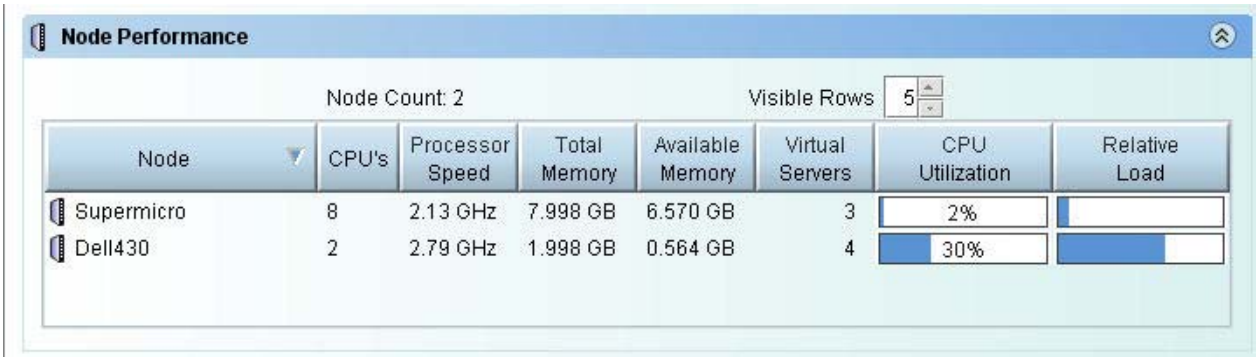
Figure 149. Last 5 Errors Detail



SYSTEM-WIDE NODE PERFORMANCE

To check the performance of all nodes in a resource center, select **Resource Center** in the navigation tree. In the Summary screen, click the **Node Performance** tab. An example of the data is shown in Node Performance Detail.

Figure 150. Node Performance Detail



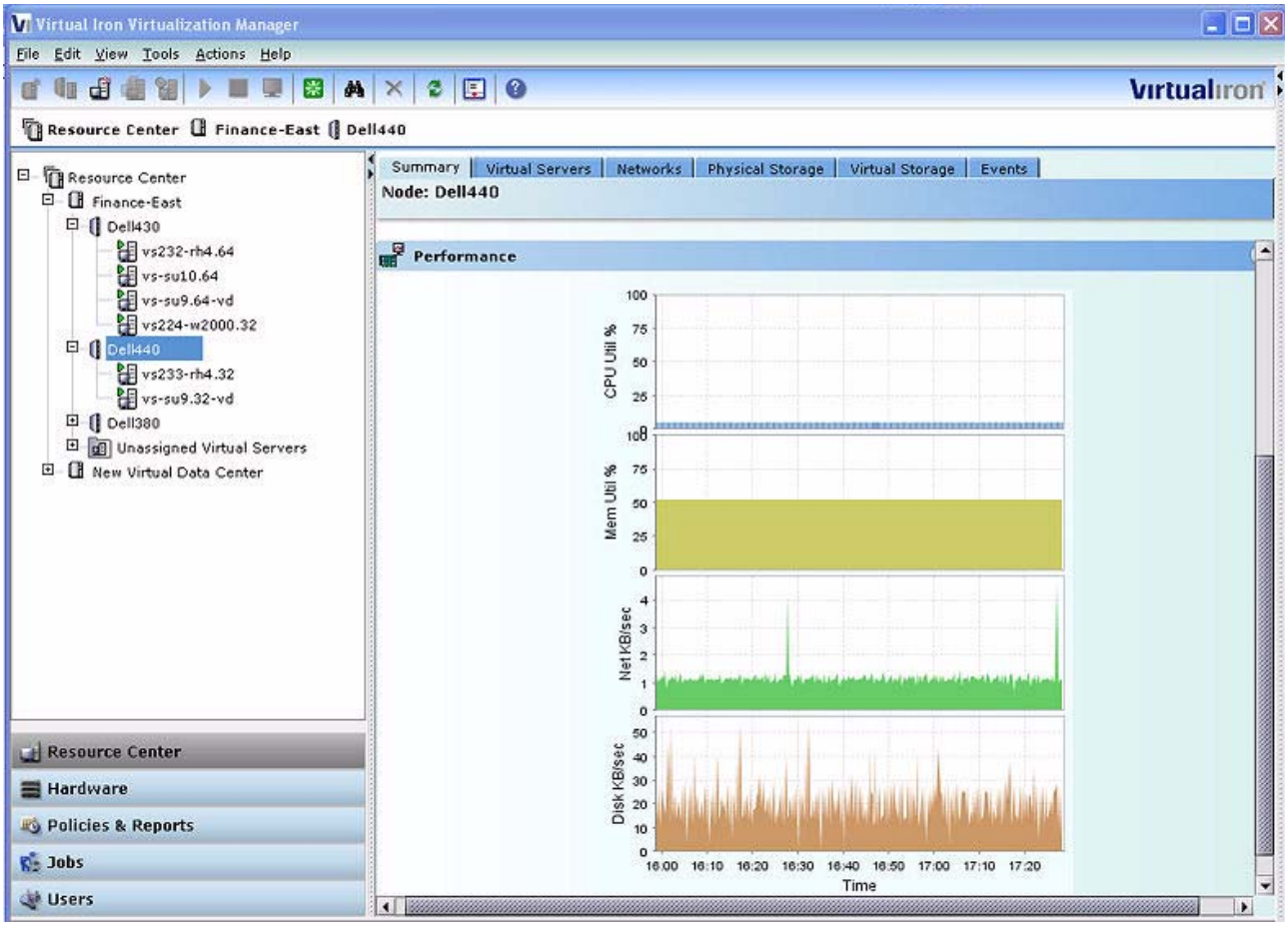
Note that you can set the number of rows of data displayed in the Node Performance pane. Click any of the column headings to switch the order of the displayed data from highest to lowest or vice versa. The **CPU Utilization** and **Relative Load** columns are a visual representation in terms of percentage of use.

Relative Load is calculated by computing a weighted average of the CPU, memory, network, and SAN load on each node, and then normalizing these node scores on a scale of 0 (the least busy node) to 100 (the mode busy node). Relative Load usually correlates to CPU utilization, but if two nodes have an equal CPU utilization, and one has much less free memory, that node will have a higher relative load value.

INDIVIDUAL NODE PERFORMANCE

To see the performance of a *specific* node, in the **Resource Center** view, click the node icon in the navigation tree, and then click **Performance** in the Summary screen. A graphical representation of the node's disk, network, memory, and CPU usage are displayed in 10-minute increments. See Figure 151.

Figure 151. Node Statistics

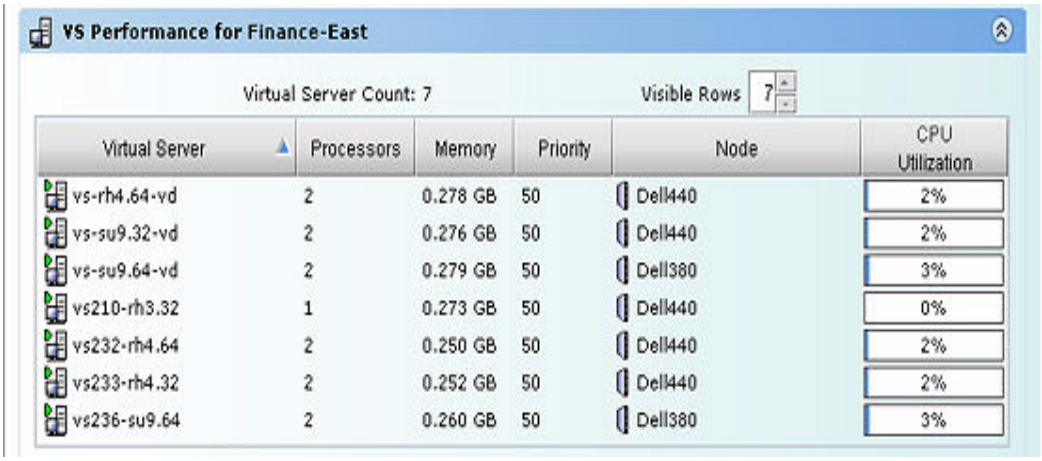


SYSTEM-WIDE VIRTUAL SERVER PERFORMANCE

Virtual Server statistics are available only if VSTools is enabled for the guest operating system booted by a virtual server. In addition to using the Summary screen to view all virtual server statistics, you can click a specific virtual server icon in the navigation tree to see detailed data.

Note that you can set the number of rows of data displayed in the Virtual Server Performance pane. Click any of the column headings to switch the order of the displayed data from highest to lowest or vice versa. The **CPU Utilization** column is a visual representation in terms of percentage of use. See Figure 152

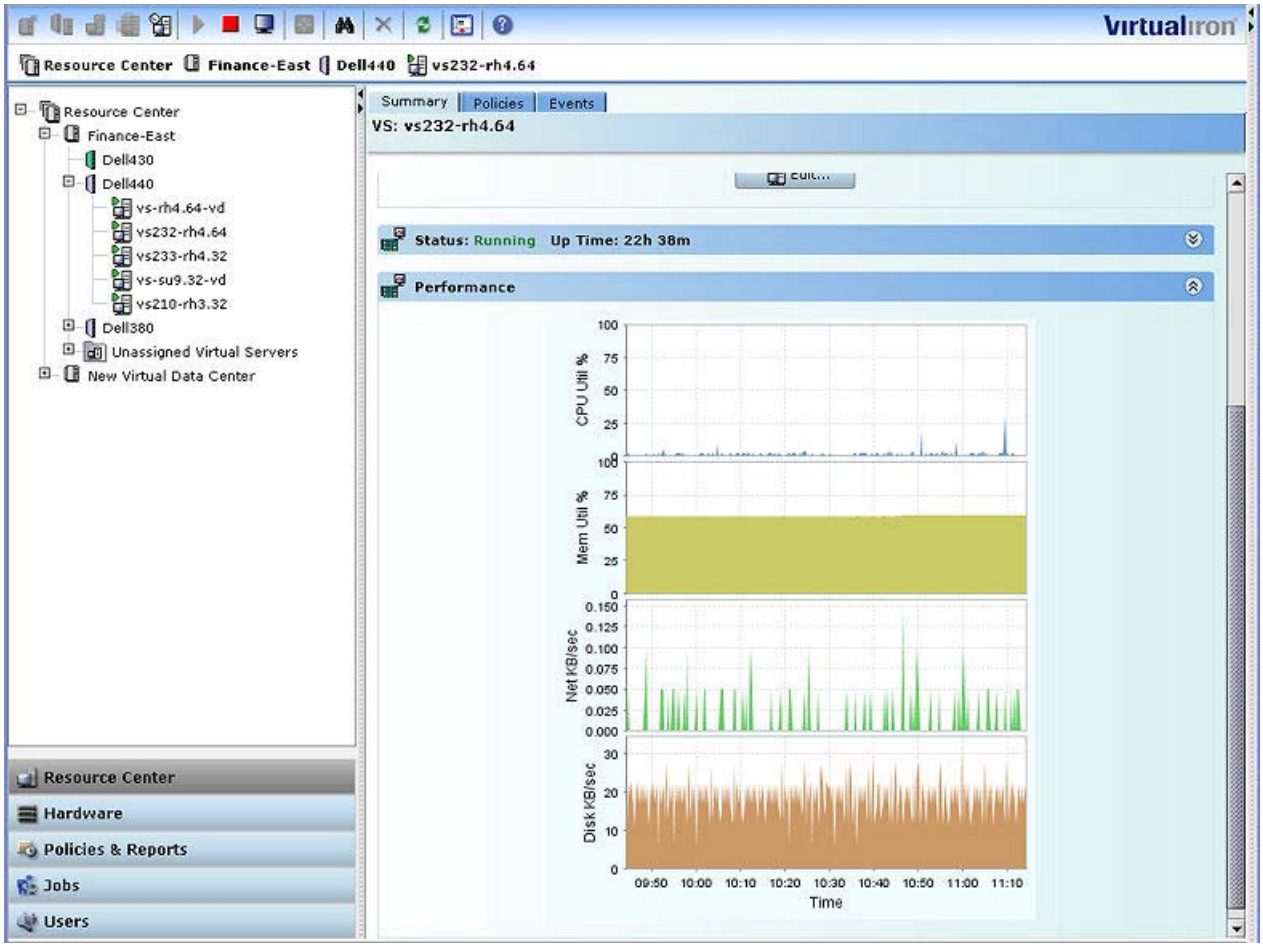
Figure 152. Virtual Server Performance Detail



INDIVIDUAL VIRTUAL SERVER PERFORMANCE

To see the performance of a *specific* virtual server, click the virtual server icon in the navigation tree, and then click **Performance** in the Summary screen. A graphical representation of the virtual server's disk, network, memory, and CPU usage are displayed in 10-minute increments. See Figure 153.

Figure 153. Virtual Server Statistics

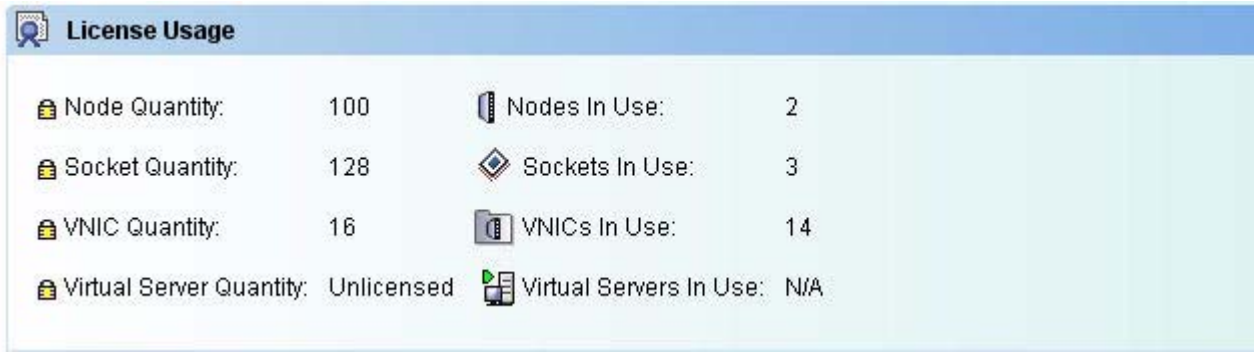


LICENSE USAGE

The License Usage pane shows how many resources are being used in relation to the total available for use.

To check license usage, in the Resource Center view, click **Resource Center** and the **License Usage** tab in the dashboard. See Figure 154 for an example of the type of data displayed in the License Usage pane.

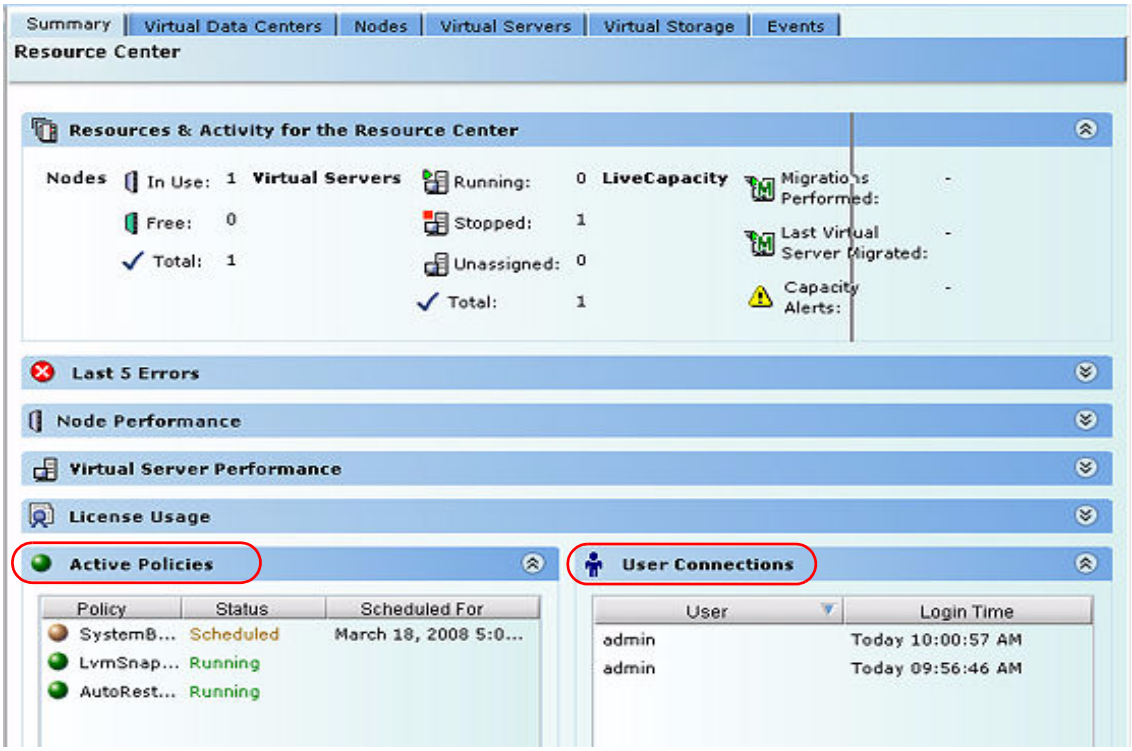
Figure 154. License Usage Detail



ACTIVE POLICIES

Use the Active Policies pane to track which policies are scheduled and which are running. See Figure 155.

Figure 155. Active Policies Detail



USER CONNECTIONS

The User Connections pane shows which users are connected and at what time they logged on. See Figure 155.

STARTING THE VI-CENTER

The instructions that follow explain how to start the Virtual Iron® VI-Center on Linux or Windows®. These instructions do not apply to the Single Server Edition, which does not require a hosting OS.

Starting the VI-Center, Linux®

After installing Virtual Iron® start the VI-Center. On the management node, type:

/etc/init.d/vivmgr

You are presented with **start** and **stop** options. Choose start.sh to start the server.

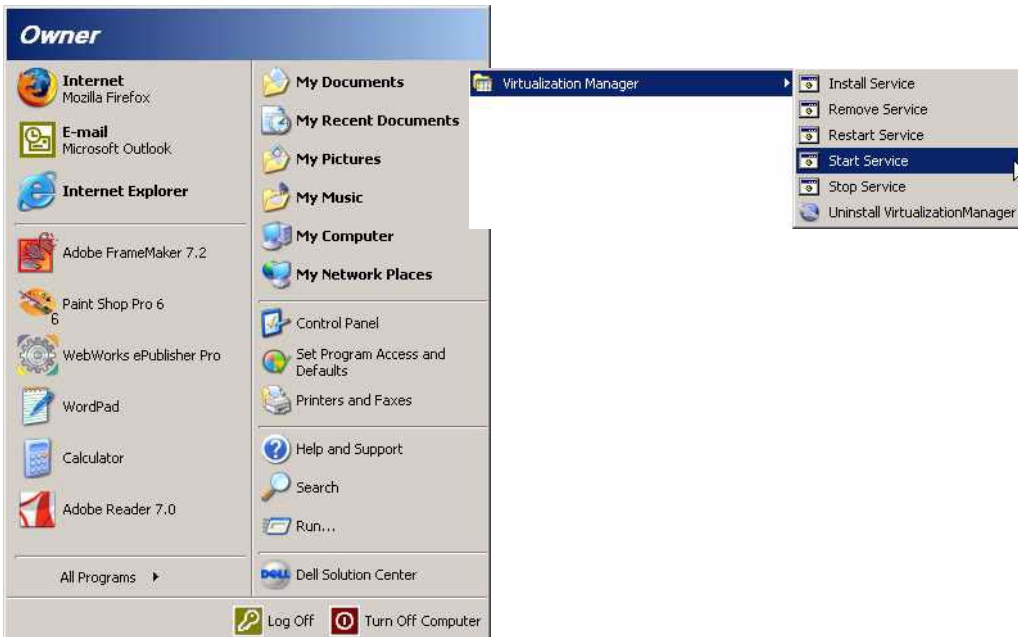
Note: You can also start the VI-Center by rebooting the management node after installation.

Starting the VI-Center, Windows®

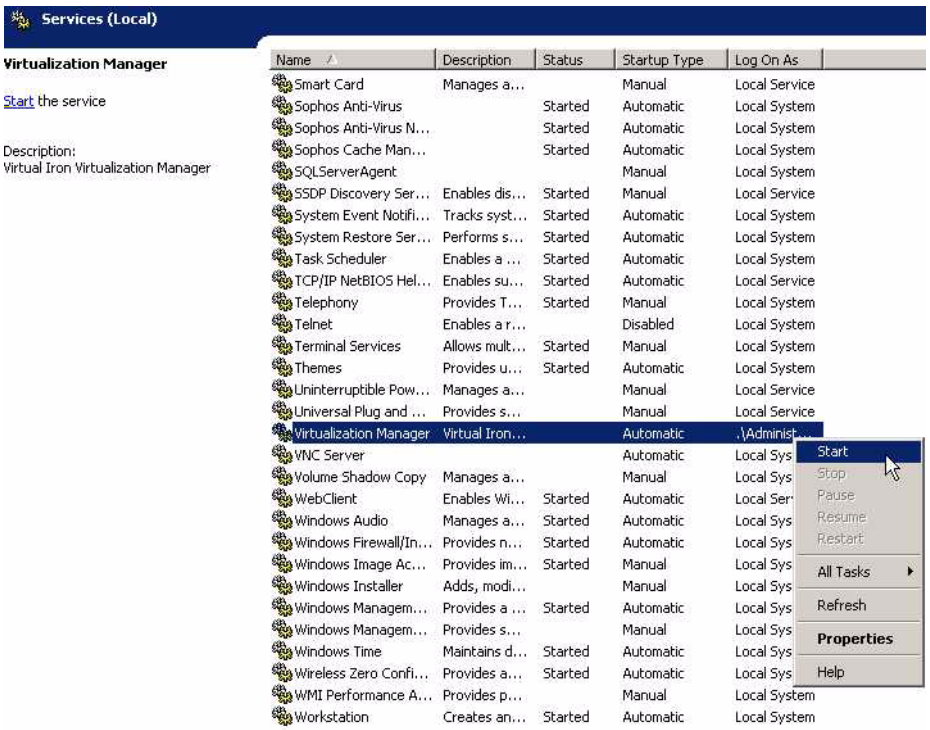
After completing an installation on Windows:

Step 1. Install and start the VI-Center as a service. Choose **All Programs -> VI-Center ->Install Service.** You are prompted for a password. Enter the password of the system Administrator or Owner (in the case of Windows® XP).

Choose **Programs -> VI-Center ->Start Service**



Step 2. Navigate to **Control Panel ->Administrative Tools-> Services.** VI-Center is listed as a service. Start the service as shown here.



PERFORMING BACKUP AND RESTORE OPERATIONS

The VI-Center database can be backed up on the system hosting the VI-Center. Backed-up data includes the state of all virtual objects.

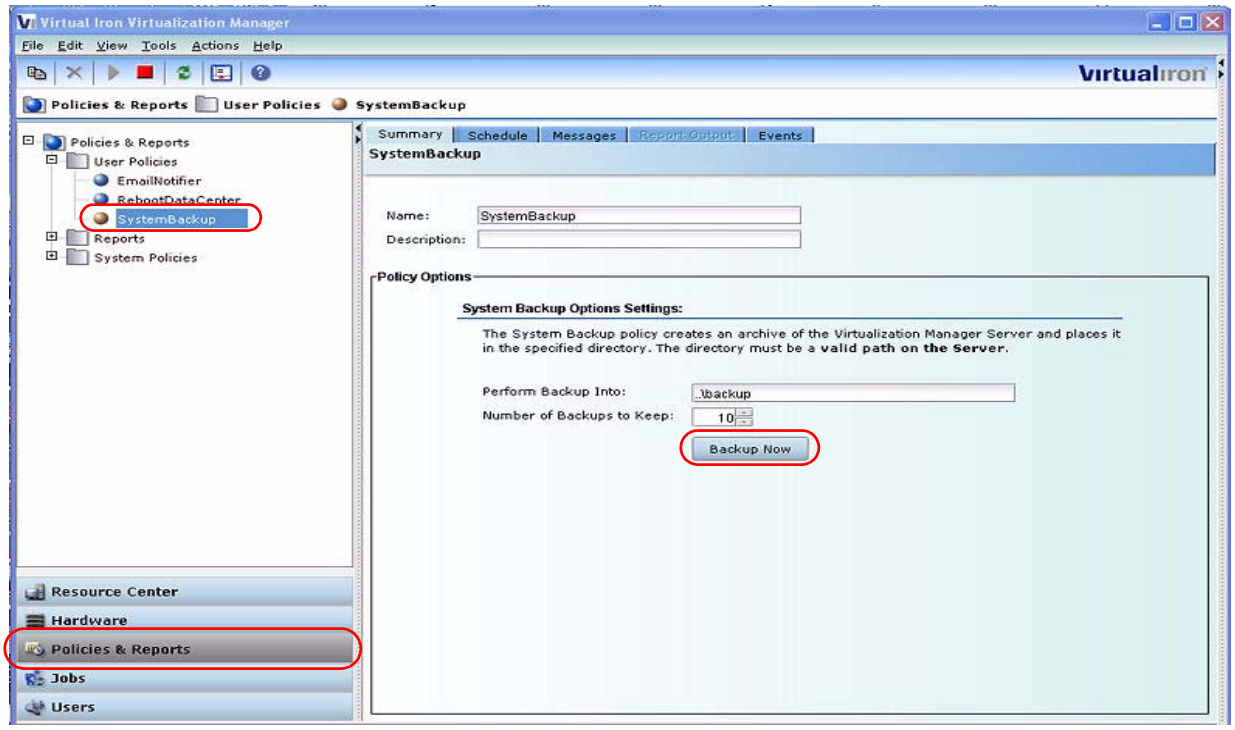
Backing up the Configuration Database

Perform backup operations by running a backup policy from the user interface:

Step 1. Cancel all current jobs, close all virtual console sessions, and close all user sessions.

Step 2. Click **Policies and Reports** in the Applications Shortcuts. Then select **SystemBackup** as shown.

Figure 156. Running a Backup Policy



Step 3. To run a backup policy immediately, select SystemBackup and click **Backup Now** as shown in Figure 156. To configure the system for scheduled back ups, see Policies and Reports.

Restoring the Configuration Database

To restore a saved configuration desk, run the restore script. This script shuts down the Virtual Iron VI-Center, untars and runs the backup file you specify, and restarts the VI-Center. The script is in the installation directory on the VI-Center host.

To run the script, change directory to the installation directory. Then use this command.

LINUX:

```
<root@ms-host># /opt/VirtualIron/restore.sh
backup/backup.<date>.tar
```

WINDOWS:

```
C:\Program Files\VirtualIron\restore.bat backup\backup. <date>.tar
```

CHANGING THE VI-CENTER IP ADDRESS

It may sometimes become necessary to rearchitect the network or move the VI-Center to a different subnet after installation.

Follow these steps to change the VI-Center IP address:

Step 1. Stop the VI-Center.

Step 2. Change the IP address of the dedicated network on the VI-Center system via the host operating system.

Step 3. Copy the file:

VirtualizationManager\etc\dhcpd.conf_default

to

VirtualizationManager\etc\dhcpd.conf

Step 4. Copy the file:

VirtualizationManager\etc\dhcpd.leases_default

to

VirtualizationManager\etc\dhcpd.leases

Step 5. Start the VI-Center and reboot all nodes.

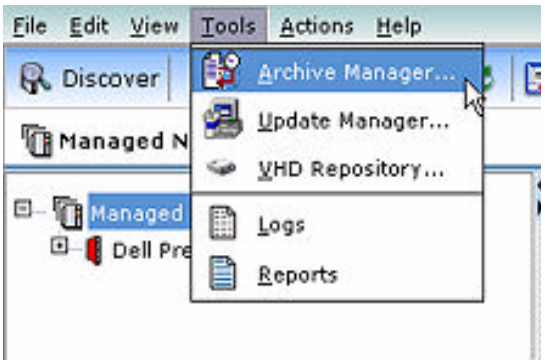
CONFIGURING THE ARCHIVE MANAGER

The archive manager is a background process that runs continuously. The archive manager moves all jobs and associated events that are older than a specified date to a secondary location in the VI-Center database. This reduces the size of the working set of jobs and events stored in the VI-Center's primary database.

To configure the archive manager, proceed as follows:

Step 1. Choose **Archive Manager** from the **Tools** pull down menu. This displays the window shown in Figure 157.

Figure 157. Tools Menu, Archive Manager Selected



By default, the archive manager runs every day at 2 am. The operation keeps 500 most recent jobs and associated events, and 10,000 most recent non-job events. Such events would include hardware failures and environmental events. The operation deletes all jobs, events, and statistics older than 90 days.

Step 2. You can edit the defaults, as shown in Figure 158. You can run the archive manager at any time, but it is best to run it when activity on the VI-Center is light.

Figure 158. Archive Manager Defaults

ASSURING VI-CENTER HIGH AVAILABILITY

As you deploy Virtual Iron in production environments, you may want to plan for failure scenarios. Use the following procedure to assure that the VI-Center, which controls virtual infrastructure, is readily available.

This assures that if the VI-Center is unavailable because of a hardware or software failure, the virtual infrastructure continues to run; there is no interruption of service for any of the virtual machines in your environment.

	Symptom	Recovery	Result
Cable or switch	Node appears to be down; loss of control	Replace faulty cables or switches; multi-pathing not available in management network	Virtual servers continue to run
Virtualization services	Node appears to be down	Cycle node power	Virtual servers must be restarted
Physical server	Node appears to be down	Use VI-Center to migrate virtual servers to spare physical hardware	Virtual servers must be restarted
VI-Center physical server	Cannot access VI-Center	Fail over to passive server	Virtual servers continue to run
VI-Center file system	VI-Center error	Restore object from backup	Virtual servers continue to run
VI-Center software	Cannot access VI-Center	Restart VI-Center	Virtual servers continue to run

High Availability Considerations

It is recommended that the VI-Center database is backed up on a nightly basis. This assures that the database can be restored in the event of a disk failure.

A network power controller and network monitoring software can fully automate VI-Center failover. Network monitoring software monitors port 80 or 443 to check the status of VI-Center. Alternatively, a heartbeat script can be written using the command */etc/init.d/vivmgr status*.

The active server can be powered off and the passive server powered on manually, or automatically, with a network power controller. Once this server boots, the VI-Center is back online without any affect on the availability of any virtual server.

If the management server fails while objects in the Resource Center are being modified, when the failover management server restarts, these objects may be locked. To remove the locks, abort any pending jobs. Operations in progress may be completed but errors could appear.

No statistics are collected while the VI-Center is down. This resets the interval that policies wait to perform actions based on resource utilization.

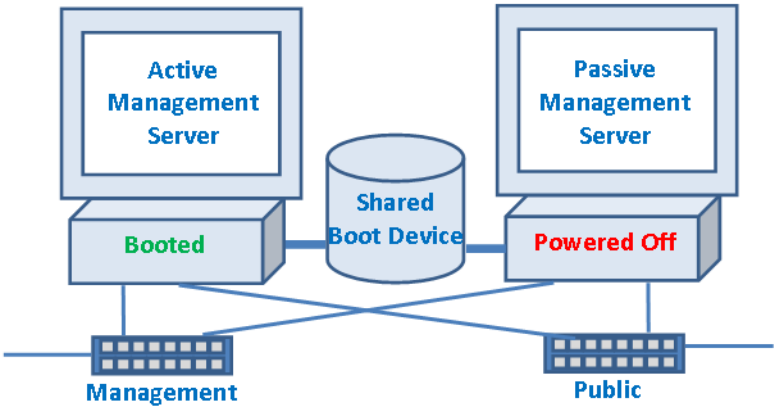
HIGH AVAILABILITY ARCHITECTURE

The VI-Center is connected using a private management network to virtualized nodes.

We recommend the following architecture for the best results (see Figure 159):

- Deploy clustered VI-Center servers to avoid hardware failures.
- Backup your environment regularly.
- Make sure the server is on an Un-interruptible power supply (UPS) to prevent issues when there are power outages.
- Use FibreChannel or ISCSI network storage for virtual server disks for the highest availability and simplest deployment.

Figure 159. High Availability Server Configuration

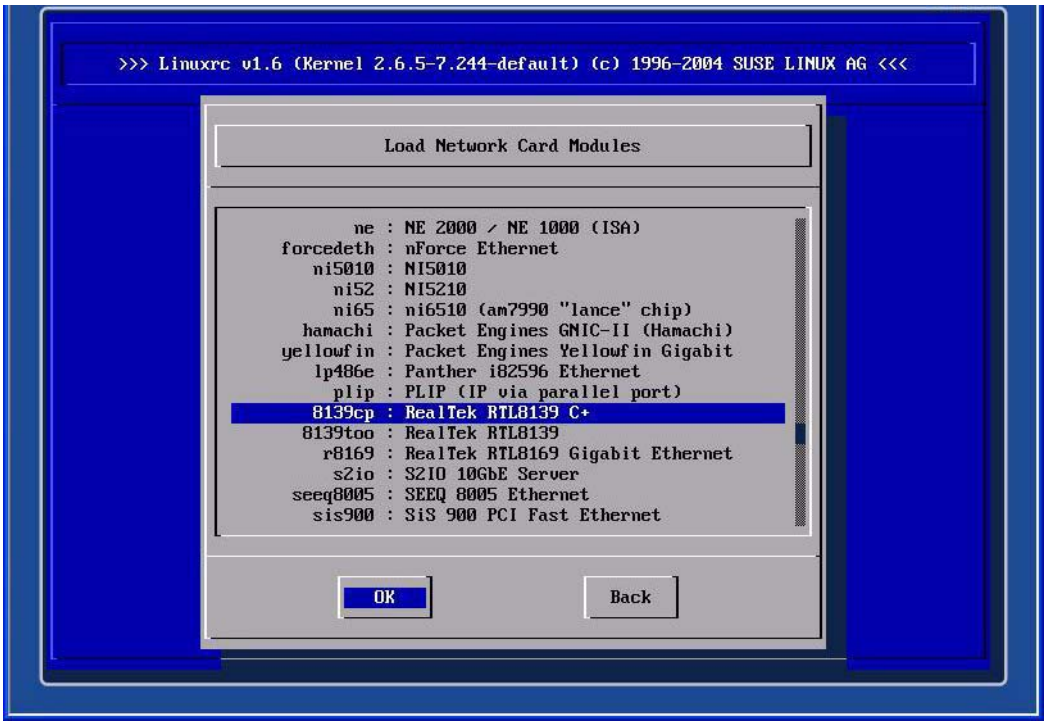


FAILOVER CONFIGURATION

To decrease the time VI-Center is offline, Virtual Iron recommends using Active/Passive clustering technology. The following steps describe how to configure your environment:

Step 1. Configure two identical servers. Ensure they have the same hardware. Refer to Figure 160.

Figure 160. SLES Install Driver Window



Step 2. Install a supported VI-Center server operating system—Windows 2003, Red Hat 4, or Novell SLES 9.

Configure the servers to boot from the same SAN or iSCSI LUN. We recommend that the LUN is mirrored using hardware RAID. Do not boot the servers simultaneously; only one server can be active at a time.

Step 3. Follow the steps in the *Administrator's Guide* to install the VI-Center server on the Active server.

Step 4. Go to one of these directories:

/opt/VirtualIron/VirtualizationManager/etc or

Program Files\VirtualIron\VirtualizationManager\etc

Step 5. Open the web.properties file and find the line:

VirtualIron.eth.public = 00:11:43:dc:68:6f

Add the MAC from the public network NIC on the Passive server to the end, for example:

VirtualIron.eth.public = 00:11:43:dc:68:6f 00:90:96:a6:e3:6f

Step 6. Open the tftpd.properties file and find the line:

VirtualIron.eth.private = 00:11:43:dc:68:70

Add the MAC from the public network NIC on the Passive server to the end, for example:

VirtualIron.eth. private = 00:11:43:dc:68:6f 00:90:96:a6:e3:6f

Step 7. Open the dhcpd.properties file and find the line:

VirtualIron.eth.private = 00:11:43:dc:68:70

Add the MAC from the public network NIC on the Passive server to the end, for example:

VirtualIron.eth. private = 00:11:43:dc:68:6f 00:90:96:a6:e3:6f

Step 8. Open the action.properties file and find the line:

VirtualIron.eth.private = 00:11:43:dc:68:70

Add the MAC from the public network NIC on the Passive server to the end, for example:

VirtualIron.eth. private = 00:11:43:dc:68:6f 00:90:96:a6:e3:6f

Step 9. Open the tunnel.properties file and find the line:

VirtualIron.eth.private = 00:11:43:dc:68:70

Add the MAC from the public network NIC on the Passive server to the end, for example:

VirtualIron.eth. private = 00:11:43:dc:68:6f 00:90:96:a6:e3:6f

A network power controller and network monitoring software can fully automate VI-Center failover. Network monitoring software can monitor port 80 or 443 to determine if the VI-Center is healthy.

When the VI-Center experiences a hardware or software failure, either

automatically using a network power controller, or manually, the active server can be powered off and the passive server powered on. Once this server boots, the VI-Center will be back online without impacting the availability of any virtual server.

No statistics will be collected during the period the VI-Center is down. This will reset the interval that policies wait to perform actions based on resource utilization. However, all virtual servers will continue to run, even when the VI-Center is offline.

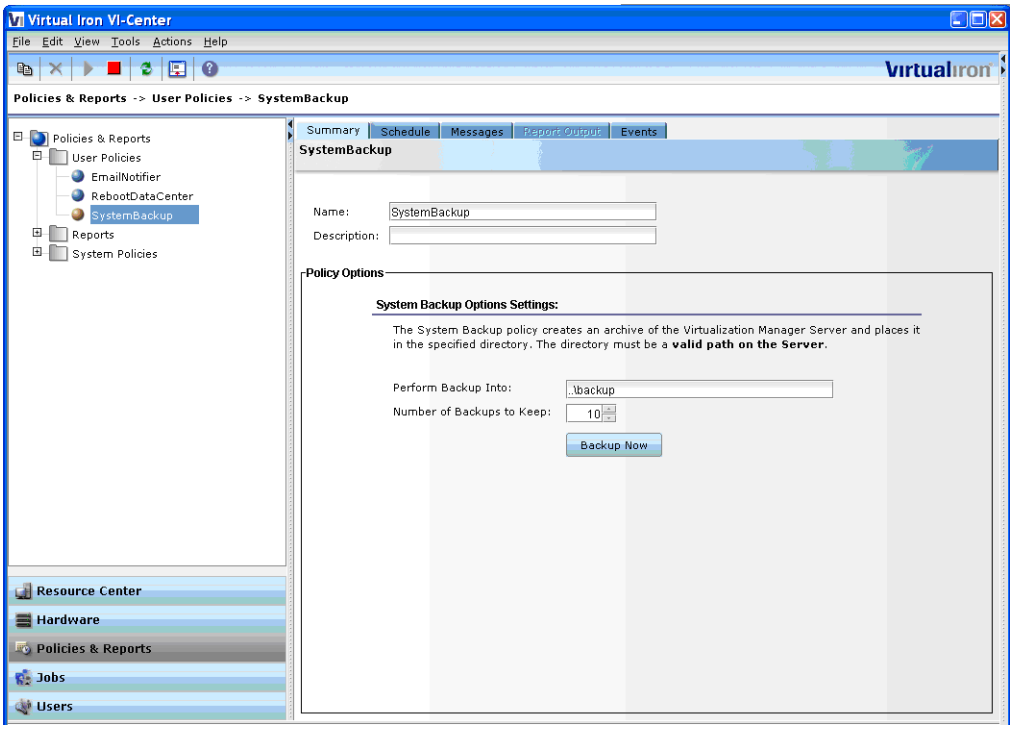
BACKUP/RESTORE

VI-Center needs to be deployed and running on a platform that is capable of maintaining critical applications. Although Virtual Servers continue to run even when the VI-Center is not, the VI-Center should be configured as an always-on product.

As with any database-based product, database corruption can occur if there is a loss of power or a management server connected to a storage subsystem configured with write-caching is improperly shut down. This could affect the most current statistics collection, configuration changes, and log file updates. To be fully functional again may require restoring the database with a backup version. As a result, some critical data may be lost. It is a best practice to operate the VI-Center with a UPS (un-interruptible power supply) and to run regularly scheduled backups.

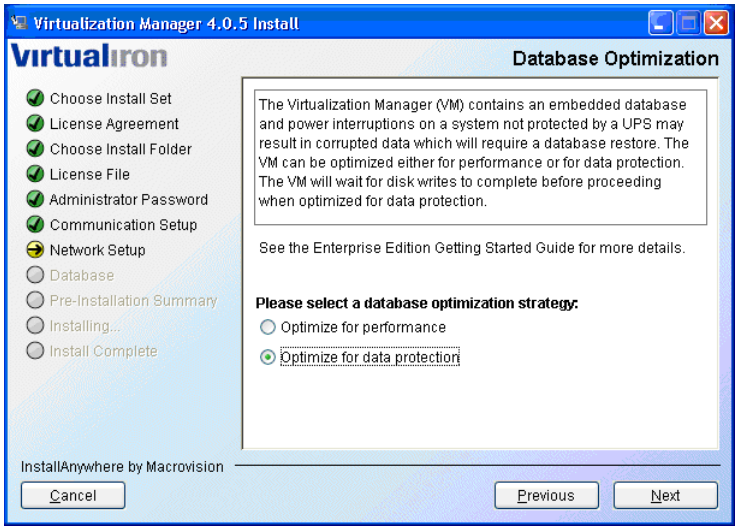
In the VI-Center Policies & Reports section, check to make sure the System Backup policy is running. This will create a backup of the database on a frequency you can determine through the schedule. Don't forget to move the backups off the server on a nightly basis or point the System Backup policy to a shared NFS or CIFS share that gets backed up as shown below. This allows

the database to be restored in the event of a disk failure.



FAULT-TOLERANT STORAGE

If your system is not protected by a UPS, there is a risk of database corruption in the event of a power interruption. This would require restoring the database and could result in lost data. Select **Optimize for data protection** during VI-Center installation to reduce this risk. This causes VI-Center to wait until the data is completely written to the disk before proceeding. To ensure that performance is not adversely affected, Virtual Iron recommends disks capable of operating at a minimum of 7200 RPM.



If you run the Enterprise Edition of VI-Center on a Windows system, it is considered a best practice to disable write-caching on the drives used by the VI-Center. Disabling write-caching helps to avoid file problems that can sometimes result if the system loses power suddenly while running.

To disable disk write-caching

Step 1. Right-click My Computer, and then click Properties.

Step 2. Click the Hardware tab.

Step 3. Click Device Manager.

Step 4. Click the plus sign (+) next to the Disk Drives branch to expand it.

Step 5. Right-click the drive on which you want to enable or disable disk write caching, and then click Properties.

Step 6. Click the Disk Policies tab.

Step 7. Click to clear the Write Cache Enabled check box.

Step 8. Click OK.

UNINSTALLING VI-CENTER

Following are procedures for uninstalling Virtual Iron® from Linux and Windows®.

Uninstalling from Linux

To uninstall VI-Center from Linux, enter this command:

```
/opt/VirtualIron/Uninstall_VirtualizationManager
```

Uninstalling from Windows

Follow these steps to uninstall VI-Center.

Step 1. As the Administrative User who installed VI-Center, navigate to **Start > Programs > VI-Center > Stop Service**. A command window is displayed as the service is being stopped. The window closes when the service is stopped.

Step 2. Select **Start > Programs > VI-Center > Remove Service**.

Step 3. Select **Start > Programs > VI-Center > Uninstall VI-Center**. A Virtual Iron dialog window is displayed. Click **Uninstall** to uninstall the VI-Center. Click **Done**.

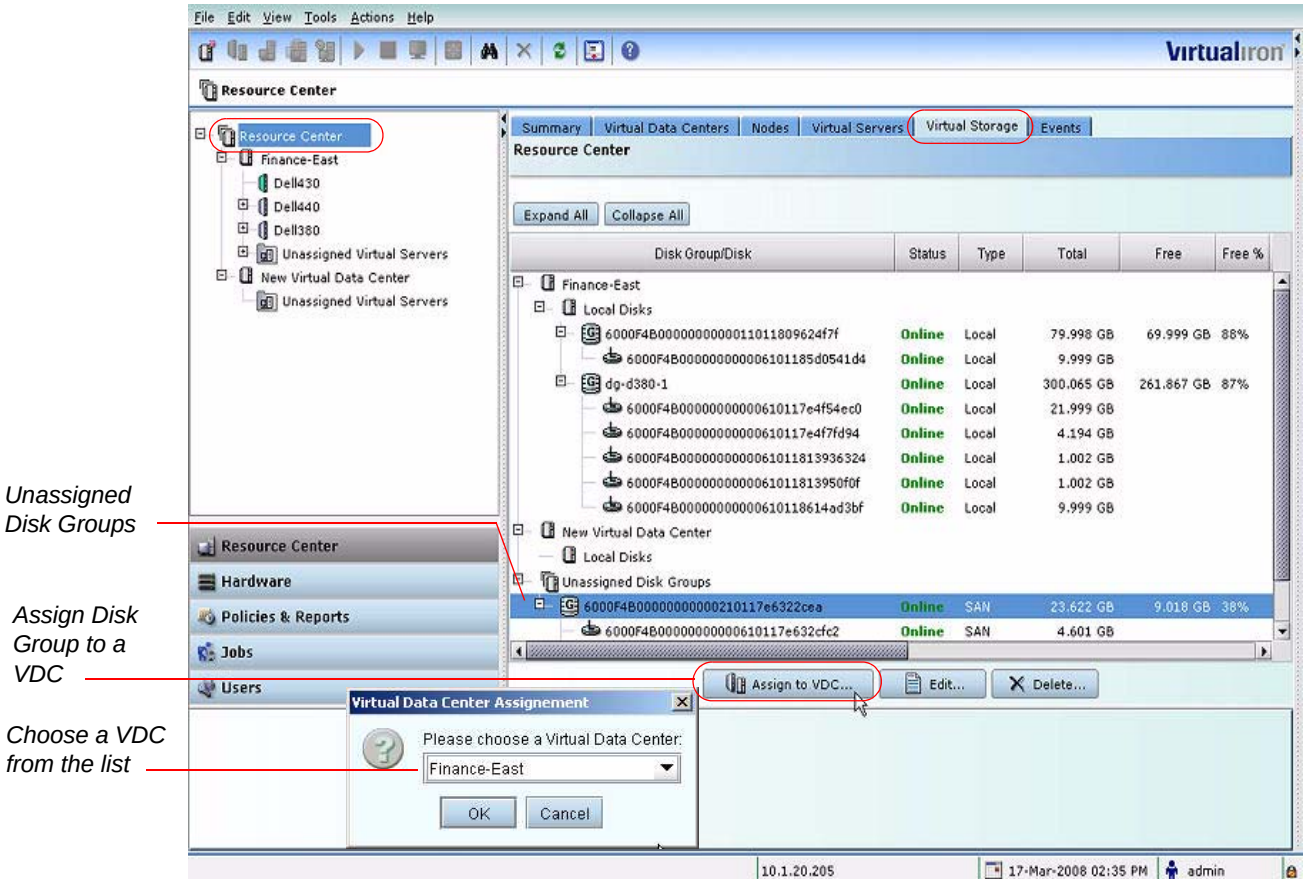
Step 4. Navigate to Program Files. Select the Virtual Iron folder, and delete it to complete the Uninstall process.

REASSIGNING UNASSIGNED DGS

If you need to upgrade to the next version of Virtual Iron®, it is recommended that you perform a system upgrade, rather than reinstall the software. Occasionally, it may be necessary to reinstall the software.

If you reinstall the product, the associations between disk groups created previously and the VDCs configured in the system's database are lost. The information associated with the disk groups still exists on the SAN. However, although VI-Center can discover this information during the discovery phase, it can not determine which VDC(s) to associate with these orphan disk groups. They appear at the Resource Center level in the **Virtual Storage** tab. An example is shown in Figure 161.

Figure 161. Unassigned DGs



For orphaned disk groups to be of use, they must be reassigned to VDCs.

Step 1. To re-assign VDCs, in the Resource Center view, select **Resource Center** in the navigation tree.

Step 2. Click the **Virtual Storage** tab and expand the Disk Group/Disk navigation tree so you can select each unassigned disk group. See Figure 161.

Step 3. Click **Assign to VDC**, and choose the VDC from the pull down list in the Virtual Data Center Assignment pop-up. Click **OK**.

Step 4. Perform this procedure for each unassigned disk group.

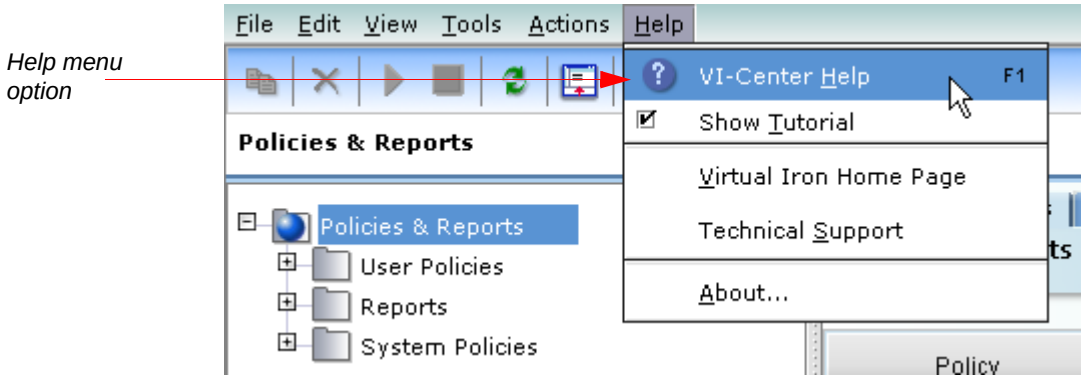
ACCESSING ONLINE HELP

To access online Help:

Step 1. Perform one of the following actions.

- Select **Help** from the Help menu pull-down, as shown in Figure 162.

Figure 162. Help Pull-down Menu



- Click on the Help icon in the application toolbar, as shown in Figure 163.

Figure 163. Help Icon

Step 2. The HTML-based Help system opens in a separate browser window. A sample window is shown in Figure 164. The left pane contains tabs for Contents, Index, and Search. Help content is displayed by default. Use the tabs as needed to search Help based on text strings or indexed entries.

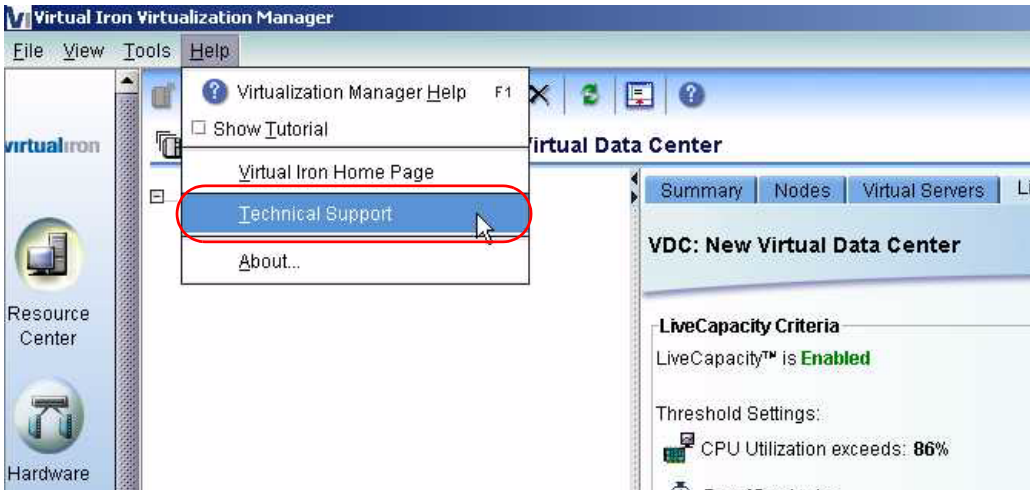
Figure 164. Sample Help Window

ACCESSING TECHNICAL SUPPORT

To access technical support:

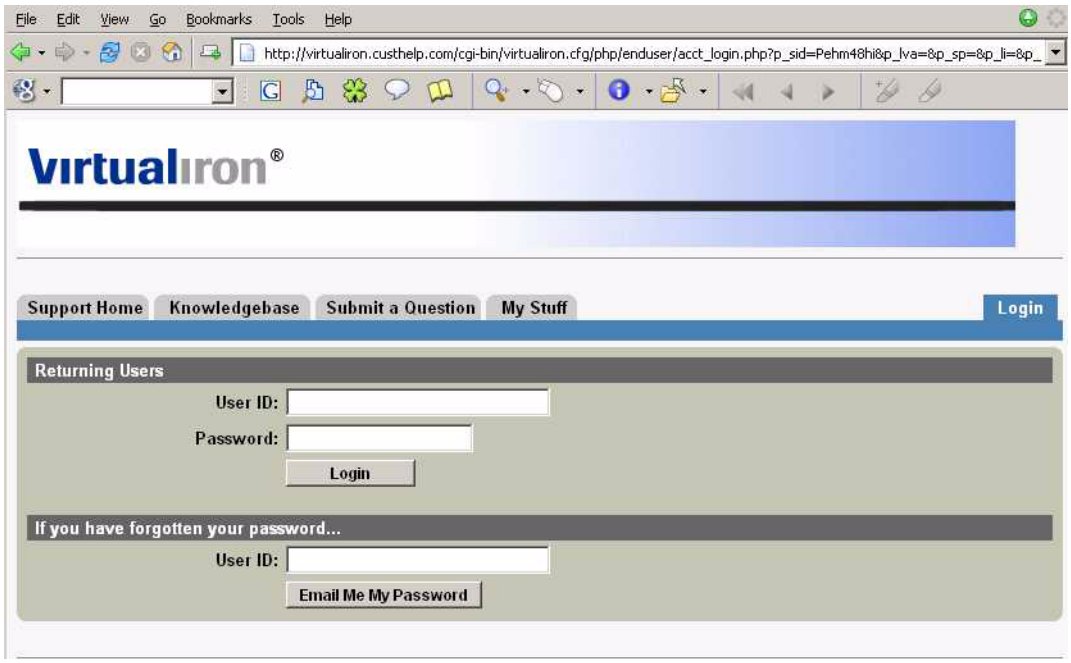
Step 1. Select **Technical Support** from the Help pull down menu.

Figure 165. Accessing Technical Support



Step 2. This connects you to the Virtual Iron® Technical Support database. A sample of the connection screen is shown in Figure 166.

Figure 166. Virtual Iron® Technical Support Home Page



Use the tabs on the Support home page to access and search the Virtual Iron knowledge base, submit a question, or connect to your own area of the support site. To login, enter your User ID and Password in the fields provided, and click **Login**.

VS TOOLS SILENT INSTALL

The following procedure automatically installs VS Tools for Windows XP and Windows 2003.

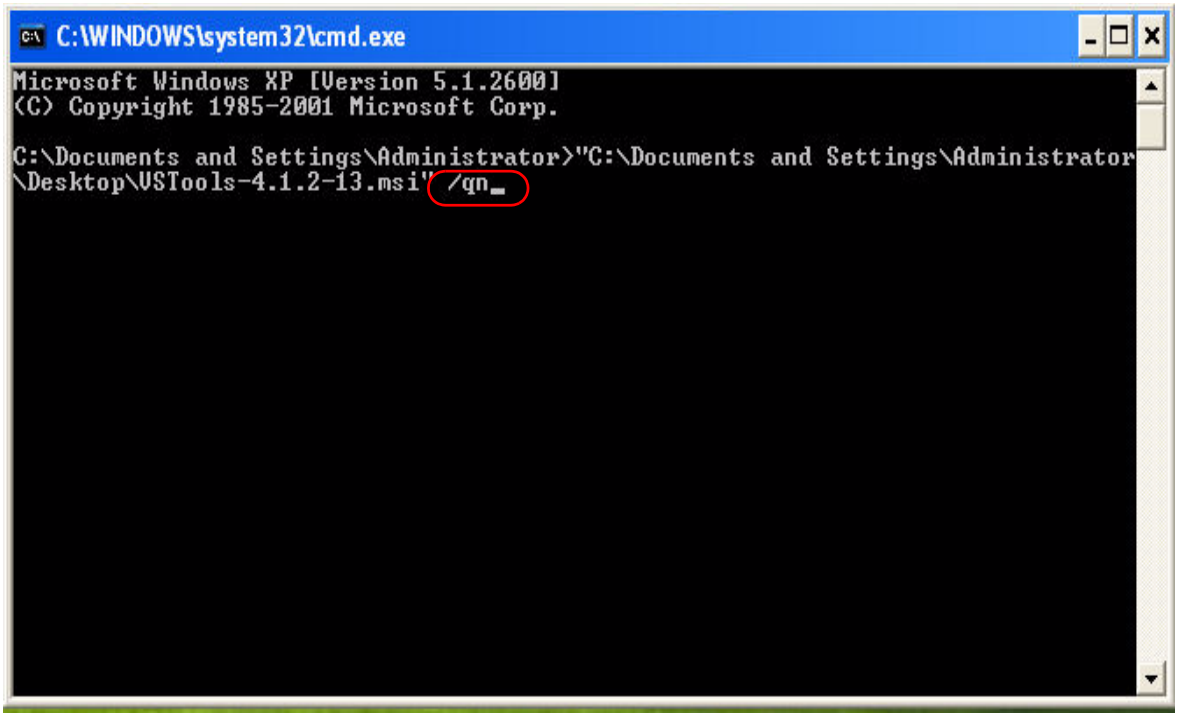
Step 1. In Windows **Start** menu, select **Run**.

Step 2. In the **Run** window, type **cmd**. Press **Enter**.

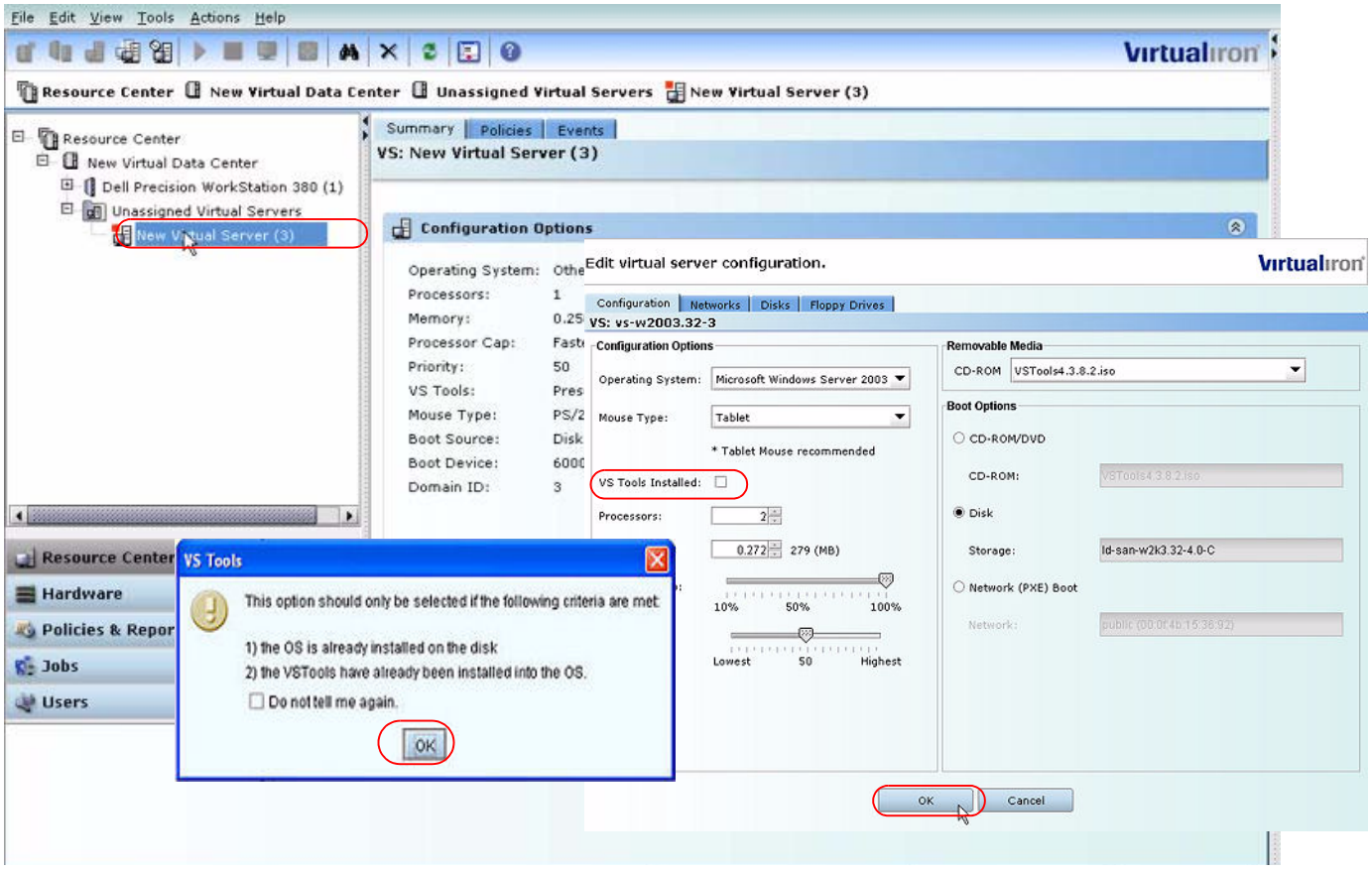
Step 3. In the command console, click the **VSTools-4.x.x.x-xx.msi** icon and drag it into the console window.

Step 4. The command string is automatically entered. Press the space bar.

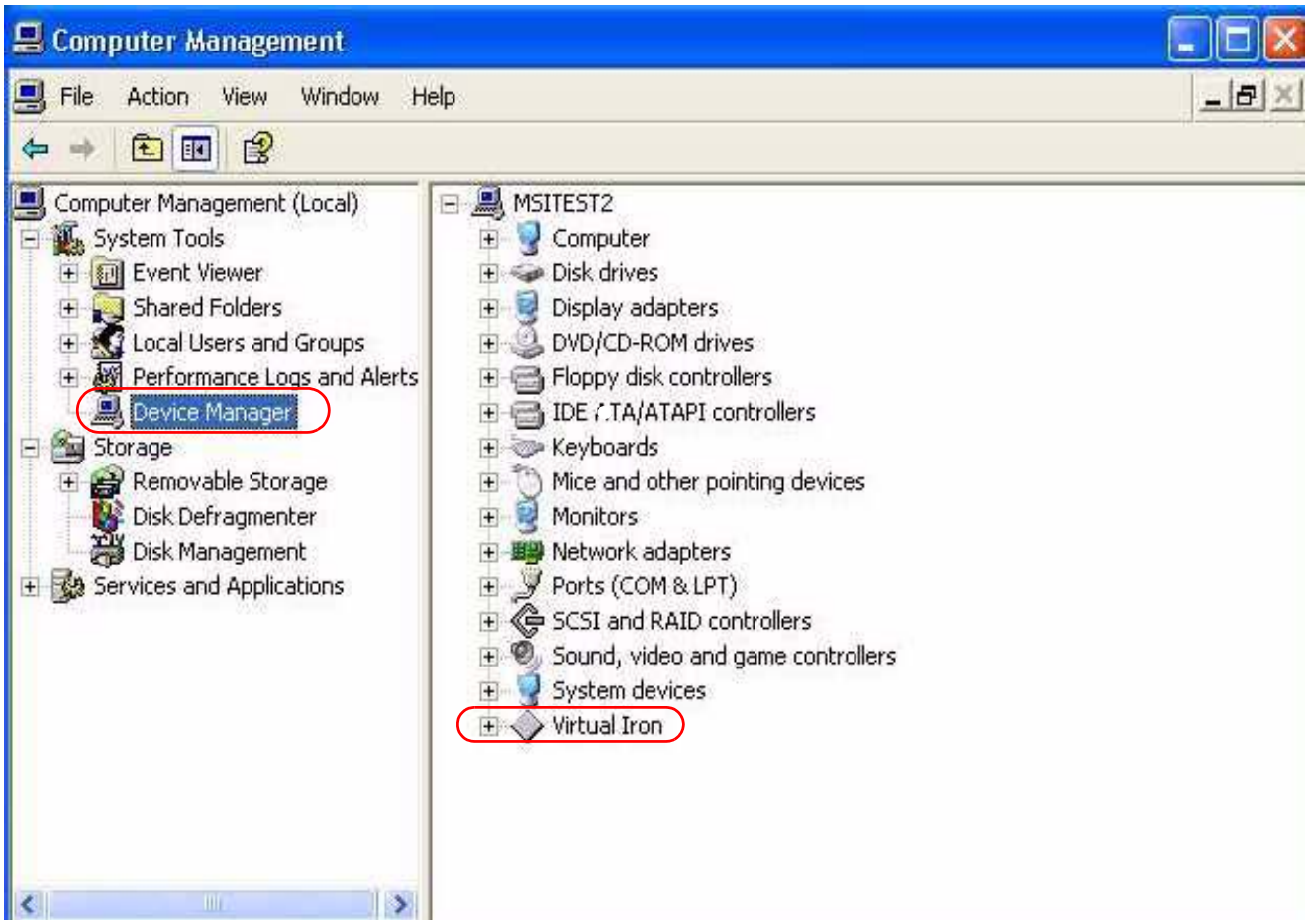
Step 5. In the console window, type **/qn**, as shown**. P**ress **Enter**. ‘I



Step 6. In VI-Center, perform a **Hard Reset** on the virtual server. Open the VS Configuration window, and check **VS Tools installed**. Click **OK**.



Step 7. This completes installation of the Virtual Iron® drivers, which appear under **Device Manager**.



INDEX

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

Index