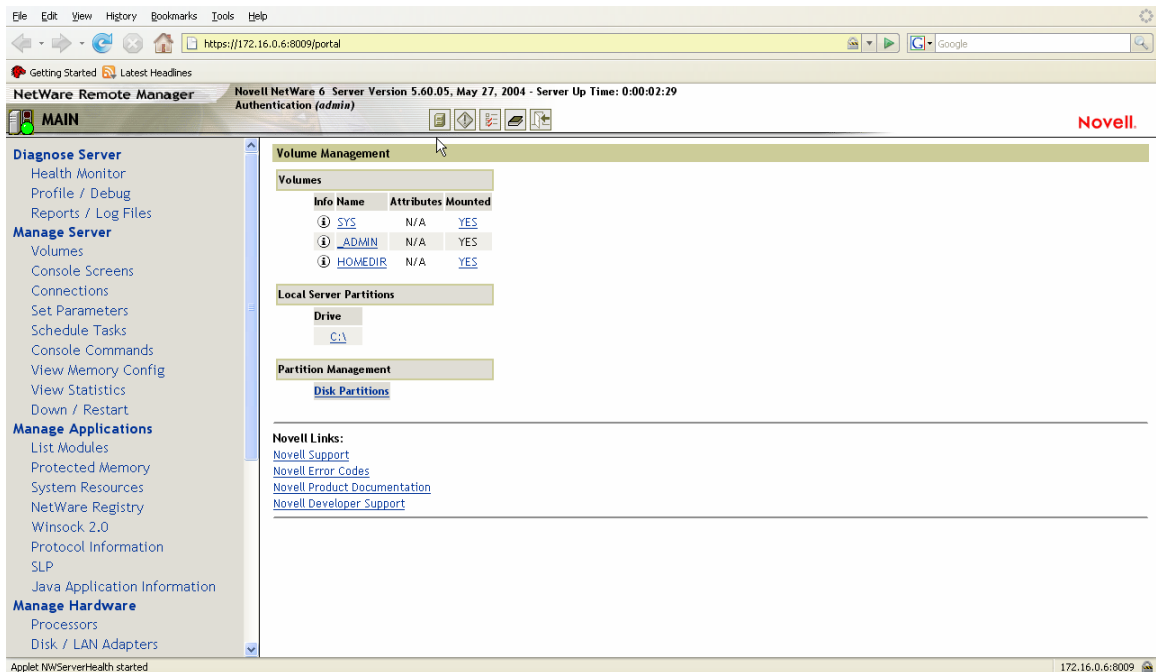


## Introduction to Novell Network Security

Like any other network operating system currently deployed in the business world today Novell Netware must be secured properly to maintain the confidentiality integrity and availability of the networks and users that the OS maintains. However certain things must be taken into account when dealing with Novell Netware, first and foremost it is a combination of Linux and Windows design principles, so there for we must take a Windows and Linux approach when securing the OS from potential attack. Secondly although it is not widely used today it is still vulnerable to attack.

As with most network operating procedures there are two types of Netware administration, the first being on console work and the second being remote management of the server, with Novell's heavy integration with Apache 2 and Console1 Novell Netware makes a ideal operating system choice for the administrator that travels. Administrators can make partitions and volumes and even execute remote console commands from there web browser. However with this level of integration also comes a point of vulnerability, Apache 2 has numerous vulnerabilities associated with it, and there for your administration website can be compromised



The screenshot displays the Novell NetWare Remote Manager web interface. The browser address bar shows the URL `https://172.16.0.6:8009/portal`. The page title is "NetWare Remote Manager" and the status bar indicates "Novell NetWare 6 Server Version 5.60.05, May 27, 2004 - Server Up Time: 0:00:02:29". The interface is divided into a left-hand navigation menu and a main content area.

The left-hand navigation menu includes the following sections:

- Diagnose Server**
  - Health Monitor
  - Profile / Debug
  - Reports / Log Files
- Manage Server**
  - Volumes
  - Console Screens
  - Connections
  - Set Parameters
  - Schedule Tasks
  - Console Commands
  - View Memory Config
  - View Statistics
  - Down / Restart
- Manage Applications**
  - List Modules
  - Protected Memory
  - System Resources
  - NetWare Registry
  - Winsock 2.0
  - Protocol Information
  - SLP
  - Java Application Information
- Manage Hardware**
  - Processors
  - Disk / LAN Adapters

The main content area is titled "Volume Management" and contains the following sections:

- Volumes**

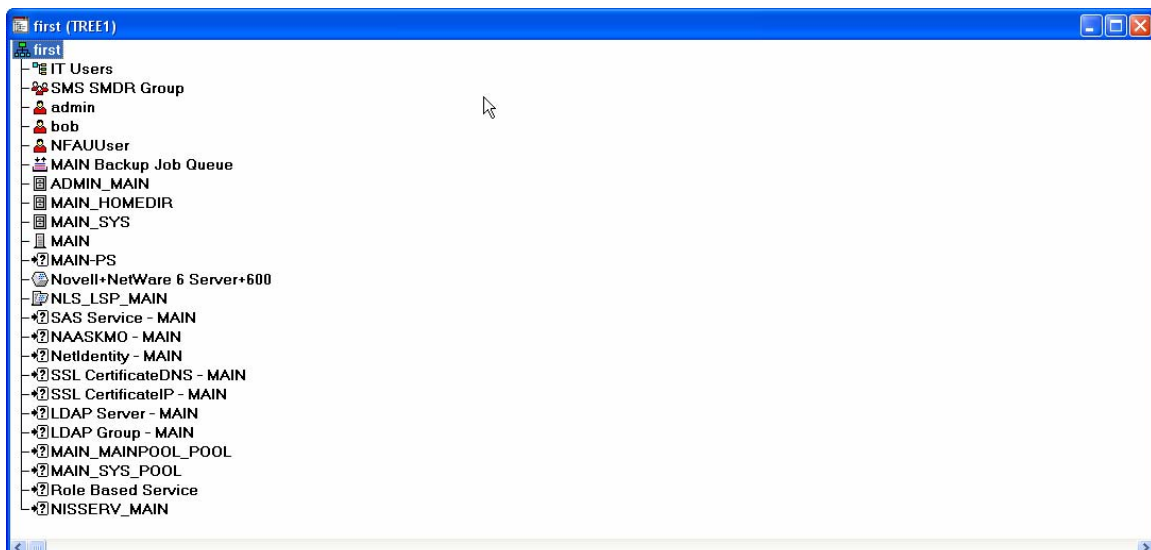
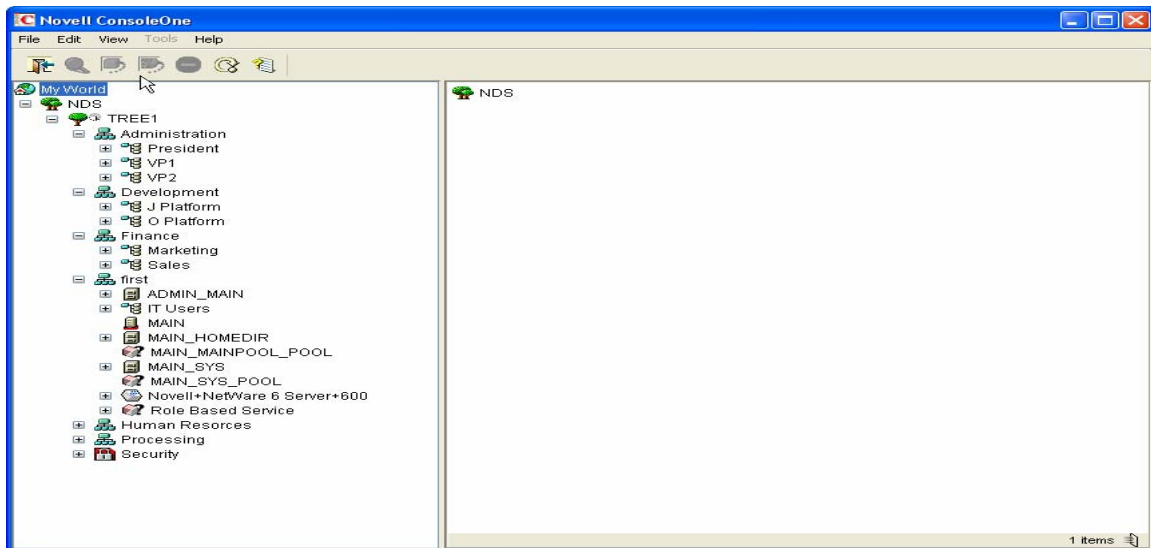
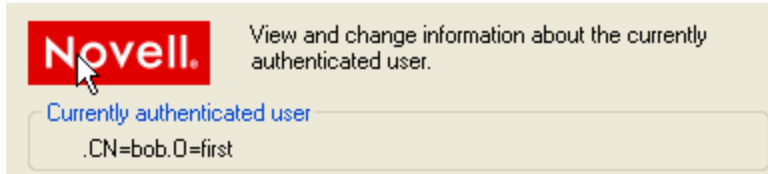
Info Name	Attributes	Mounted
<a href="#">SYS</a>	N/A	<a href="#">YES</a>
<a href="#">_ADMIN</a>	N/A	<a href="#">YES</a>
<a href="#">HOMEDIR</a>	N/A	<a href="#">YES</a>
- Local Server Partitions**
  - Drive**
    - [C:\](#)
- Partition Management**
  - [Disk Partitions](#)

At the bottom of the main content area, there are "Novell Links" with the following links:

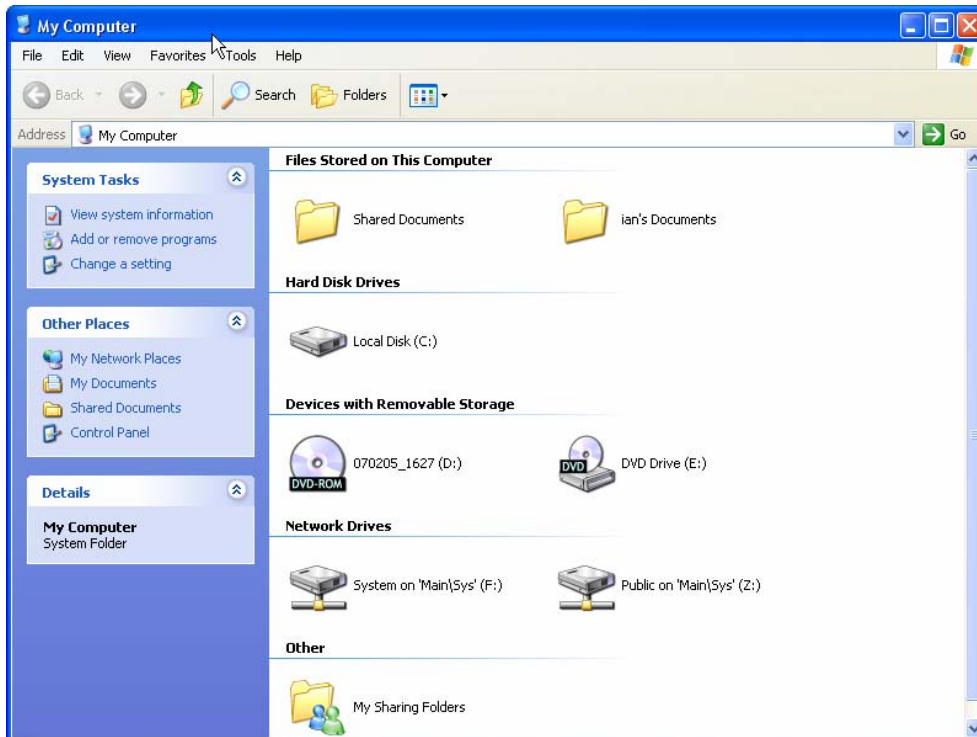
- [Novell Support](#)
- [Novell Error Codes](#)
- [Novell Product Documentation](#)
- [Novell Developer Support](#)

The status bar at the bottom of the browser window shows "Applet NWServerHealth started" on the left and "172.16.0.6:8009" on the right.

One other major remote administration tool that can be used is the Novell Netware Console1 and Novell Netware Administrator (commonly referred to as NWADMIN) however as with imanager both these applications can be used by any user that is authenticated to the server. For security reasons it is recommended that the administrators remove access to these two programs either by Group or Registry policy, or by removing access to the server shares that the programs reside on. The bellow screenshots illustrate how a limited user can access console 1 and NWADMIN without a administrator password



Additionally all users that authenticate to the server will automatically have two volumes mapped to network drives on there windows desktops, the SYS volume and its sub folder PUBLIC. With default access rights the users can remove critical system files such as imanager.nlm (the executable file that triggers Imanager and lets administrators perform tasks on the server), the default shares may be also used to transfer documents anonymously over the server.



In order to counteract the inherent security problems with Novell Netware the administrator should accomplish the following tasks:

- Remove Default shares in Novell Netware Administrator or prevent access to system volumes
- Remove Access to console1 and NWADMIN via a effective group policy or registry policy
- Insure Proper Apache 2 Security with SSL is enabled in Apache 2 Manager
- Limit size of SYS volume upon creation (4 GB should be plenty)
- Deploy GroupWise and other systems to separately created IT Volume that only IT users have access to (console has root access to everything by default)

Physical Security of the Novell console cannot be taken lightly and with All the remote management software that Novell has bundled with the newest editions of Netware (5.1, 6 and 6.5) it is becoming increasingly easy for administrators to spend very little time actually working on the console. Therefore the option of placing the server in a high security area with minimized access is available and should be taken advantage of