Integrating and Managing HP ProLiant Servers in the Enterprise

CSG18406LG0405

Integrating and Managing HP ProLiant Servers in the Enterprise

CSG18406LG0405

HP Training

Lab guide

invent

Printed in USA

Integrating and Managing HP ProLiant Servers in the Enterprise
Lab Guide
May 2004

HP Restricted

Contents

Module 1 — Lab: Heterogeneous server deployment and integration

Module 2 — Lab: Enterprise management

Module 3 — Lab: Security

Module 4 — Lab: Performance management

Appendices

Module 5 — Lab: High availability and clusters

Module 6 — Lab: Business continuity planning and disaster recovery

Heterogeneous server deployment and integration

Lab 1

Objectives

After completing this lab, you should be able to:

- Use the HP ProLiant Essential Rapid Deployment Pack (RDP) to perform pre-deployment configuration tasks
- Deploy a scripted Microsoft Windows 2000 installation job to a Preboot eXecution Environment (PXE) enabled server
- Deploy servers using imaging
- Configure a Samba server by editing the smb.conf file using a text editor
- Deploy a Windows disk image

Requirements

To complete this lab, you will need:

- A Windows 2000 Advanced Server with RDP 1.50
- A Linux image on the RDP server with the following software installed:
    - Red Hat Enterprise Linux 3.0
    - Samba
    - Xwindows
    - gedit
- An unconfigured ProLiant server

Introduction

RC Engineering has acquired new HP ProLiant servers that need to be configured for a multiplatform environment. The company wants to set up one as a Linux server to share information with the other servers.

In this lab, you will deploy a Windows 2000 scripted installation to an unconfigured system. You will then deploy a previously created Linux image to the server to demonstrate the versatility of RDP and the use of Samba. At the end of the lab, you will redeploy Windows to the ProLiant target to prepare for the next set of labs.

Exercise 1 — RDP pre-deployment configuration

Before you can install an operating system or application software on a server, you must configure the hardware. RDP provides the tools and scripts to automate server hardware configuration. Before you use RDP, make the following configuration modifications so that your deployment server will function optimally:

1. Configure PXE to process new computers automatically.
2. Synchronize the console name with the operating system name.
3. Change the primary lookup key to the serial number.
4. Preconfigure the Deployment Agent and the web agent for Windows.

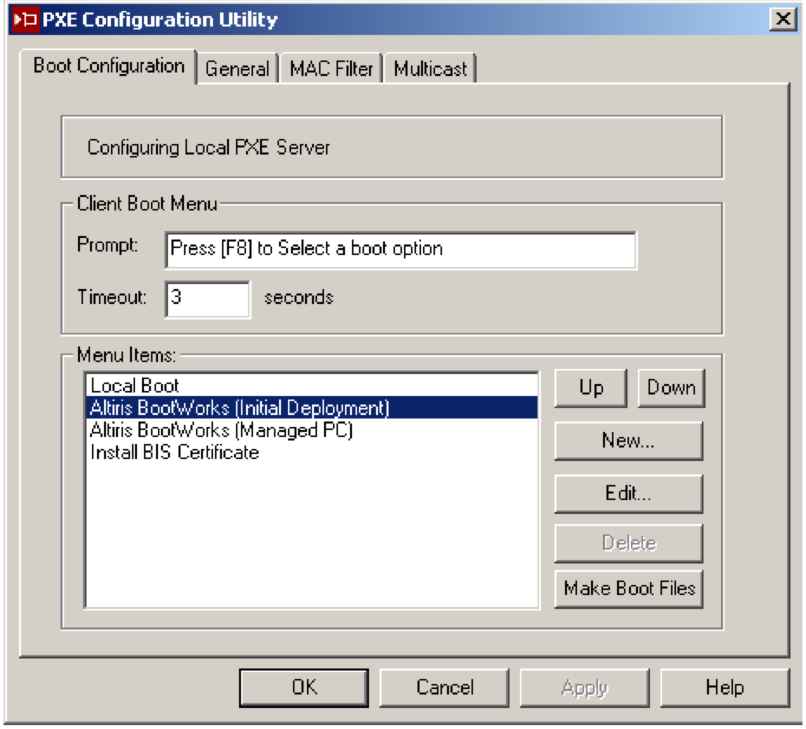
Configuring PXE to process new computers automatically

By default, the correct menu choice for your environment is automatically selected in the PXE Server menu, but an initial deployment requires you to press the *Enter* key to confirm the choice. This process prevents destructive events from running on a computer because the Deployment Server was unaware of the computer. The default action for servers is to wait for the Deployment Server console administrator to assign the computer a task. Therefore, it is not necessary to warn you about potentially data destructive operations.

To configure the PXE server to choose the Initial Deployment menu item automatically and continue without user interaction, follow these steps:

1. Click *Start* → *Programs* → *Altiris* → *PXE Services* → *PXE Configuration Utility.*

2. Select *Altiris BootWorks (Initial Deployment)*. Click *Edit* to display the Menu Item Properties screen.



Configuring Local PXE Server

Client Boot Menu

Prompt: Press [F8] to Select a boot option

Timeout: 3 seconds

Menu Items:

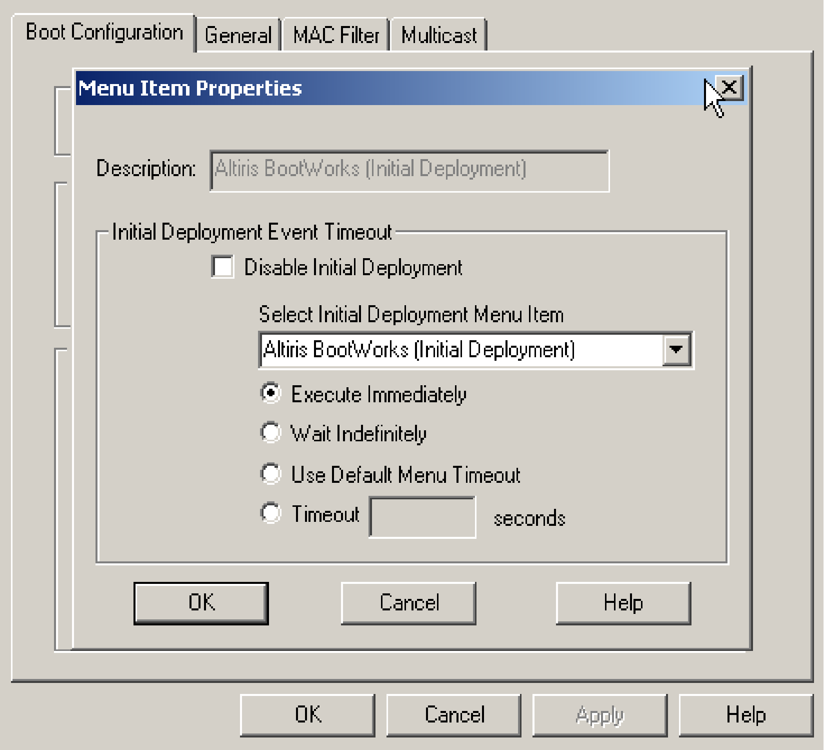
Local Boot
Altiris BootWorks (Initial Deployment)
Altiris BootWorks (Managed PC)
Install BIS Certificate

!

Important

Do **not** rearrange the order of the menu items. Changing the menu item order can cause your target servers to fail to boot to local hard drives.

3. Select the *Execute Immediately* option to eliminate wait time and click *OK* to close both windows. Initial Deployment will now run automatically for every server not in the database.



Description: Altiris BootWorks (Initial Deployment)

Initial Deployment Event Timeout

☐ Disable Initial Deployment

Select Initial Deployment Menu Item: Altiris BootWorks (Initial Deployment)

● Execute Immediately

○ Wait Indefinitely

○ Use Default Menu Timeout

○ Timeout ______ seconds

Synchronizing the console and Windows names and changing the primary lookup key

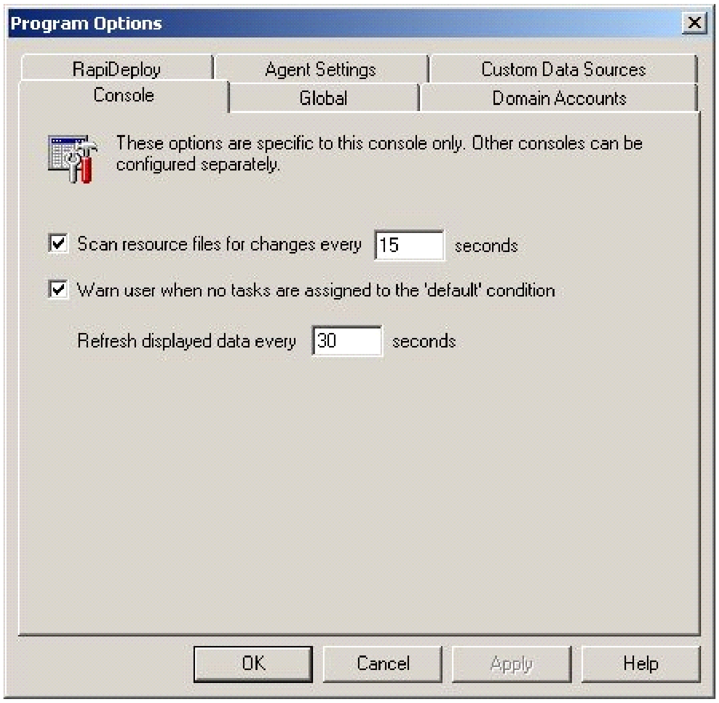
Deployment Server uses the memory access control (MAC) address of the NIC as the primary lookup key, which is its primary means of identifying computers. Therefore, changing the NIC in a computer causes Deployment Server to treat this address as a new computer. By associating MAC address with the serial number, you need to know only the serial number, not the MAC address, when you import new computers.

To modify the settings, follow these steps:

1. Double-click the *Deployment Server console* icon on the desktop. Close the Getting Started screen.

> **Note**
> If you want to prevent the Getting Started screen from displaying every time the Deployment Server console is started, select the *Don't ask me again* box.

2. At the Deployment Server console screen, select *Tools* → *Options*.
3. The Program Options screen displays. Click the *Global* tab.



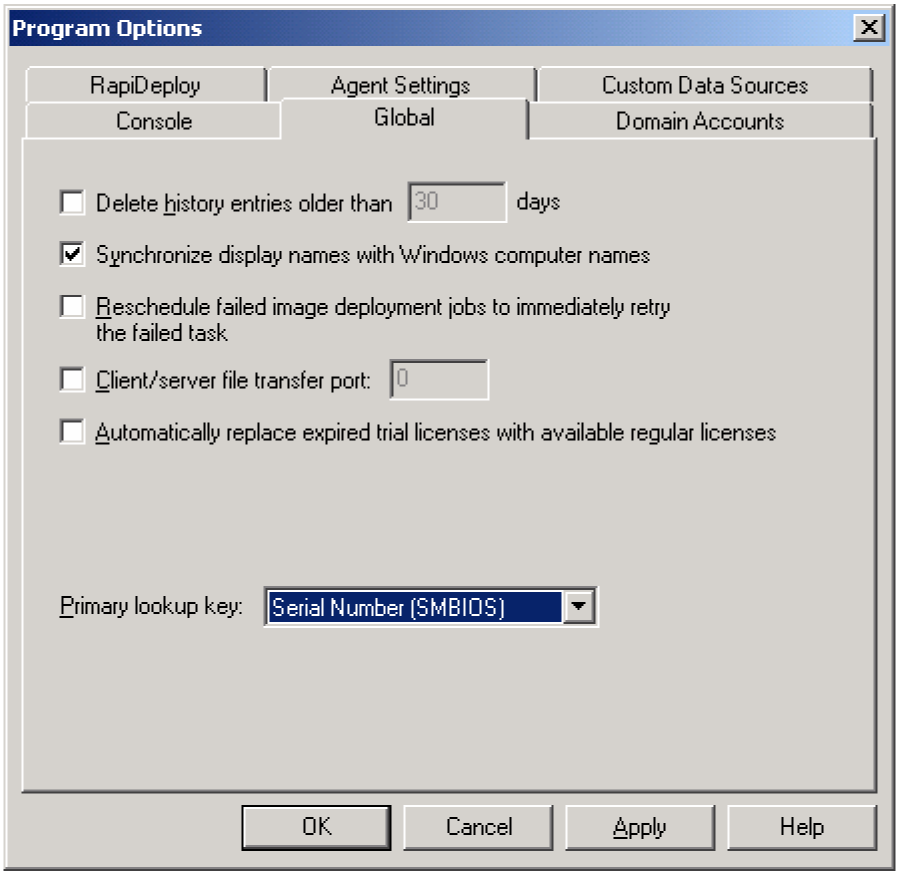
These options are specific to this console only. Other consoles can be configured separately.

☑ Scan resource files for changes every 15 seconds

☑ Warn user when no tasks are assigned to the 'default' condition

Refresh displayed data every 30 seconds

4. Select the box next to *Synchronize display names with Windows computer names*. Change the primary lookup key to *Serial Number (SMBIOS)* and click *OK*.



☐ Delete history entries older than 30 days

☑ Synchronize display names with Windows computer names

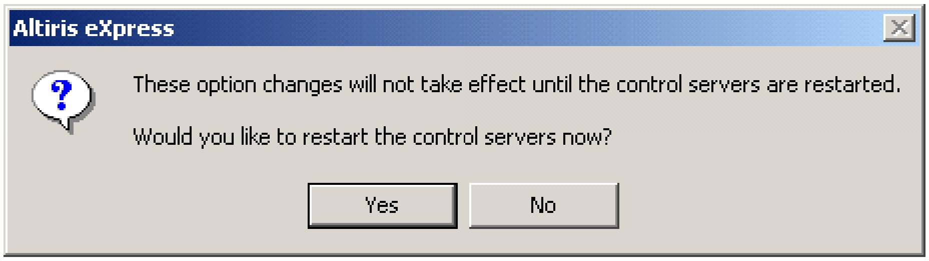
☐ Reschedule failed image deployment jobs to immediately retry the failed task

☐ Client/server file transfer port: 0

☐ Automatically replace expired trial licenses with available regular licenses

Primary lookup key: Serial Number (SMBIOS)

5. When prompted to restart the control servers, click *Yes*.



These option changes will not take effect until the control servers are restarted.

Would you like to restart the control servers now?

Preconfiguring the Deployment Agent for Windows

The provided Windows scripted install jobs use the aclient.inp file in the Deployment Server root directory for agent settings. These settings are independent of the Remote Client Installer settings that are established from *Tools → Options → Agent Settings*.

In this part of the exercise, you will:

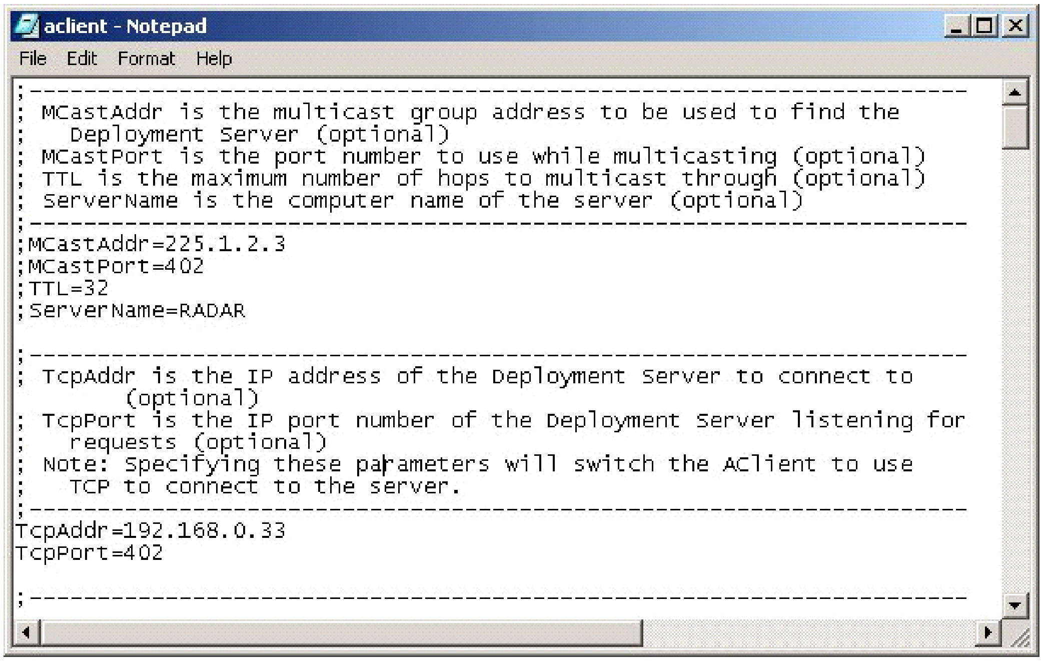
- Modify the aclient.imp config file
- Set the IP address of the deployment server

To configure the Deployment Agent for Windows, follow these steps:

1. From a text editor, open the *aclient.inp* file in the Deployment Server root directory.

Note

By default, the Deployment Server root directory is *\program files\altiris\express\Deployment Server*.



```
;-----------------------------------------------------------------------
; MCastAddr is the multicast group address to be used to find the
;   Deployment Server (optional)
; MCastPort is the port number to use while multicasting (optional)
; TTL is the maximum number of hops to multicast through (optional)
; ServerName is the computer name of the server (optional)
;-----------------------------------------------------------------------
;MCastAddr=225.1.2.3
;MCastPort=402
;TTL=32
;ServerName=RADAR

;-----------------------------------------------------------------------
; TcpAddr is the IP address of the Deployment Server to connect to
;       (optional)
; TcpPort is the IP port number of the Deployment Server listening for
;   requests (optional)
; Note: Specifying these parameters will switch the AClient to use
;   TCP to connect to the server.
;-----------------------------------------------------------------------
TcpAddr=192.168.0.33
TcpPort=402

;-----------------------------------------------------------------------
```

2. Verify that the static IP address listed in the TcpAddr= line is the IP address of your deployment server.

3. To ensure that jobs do not fail if the server must be restarted, select the option to force applications to close when the server needs to restart by changing the line:

   ```
   ; ForceReboot=No
   ```

   to

   ```
   ForceReboot=Yes
   ```

4. If boot diskettes are used instead of PXE and a configuration task is issued to a computer when no diskette is in the diskette drive, a prompt instructs you to insert a diskette. If this occurs when you are not logged in to the server, you must log in and close the prompt before the job can continue. By selecting to never be prompted for a boot diskette, the server restarts to the normal operating system if a boot diskette is not inserted in the server when required.

   Modify the BootWorks disk prompting behavior by changing the line:

   ```
   ; BootDiskMessageUsage=4
   ```

   to

   ```
   BootDiskMessageUsage=0
   ```

4. Select the option to synchronize the target server time with the Deployment Server time by changing the line:

   ```
   ; SyncTimeWithServer=No
   ```

   to

   ```
   SyncTimeWithServer=Yes
   ```

5. Save the file and close the text editor.

Preconfiguring the web agent for Windows

Several utilities in a ProLiant Support Pack (PSP) use the web agent, which enables you to manage a server locally and remotely through a web browser. Smart Components are modules within the PSP. The web agent requires you to configure a password in the Smart Components before installation. Without the password, these other utilities install but do not function correctly and are not accessible.

> **!** **Important**
> The PSPs must reside on writeable media so that you can configure the Smart Components in the PSP before PSP deployment. You cannot configure the PSPs from the CD-ROM drive.

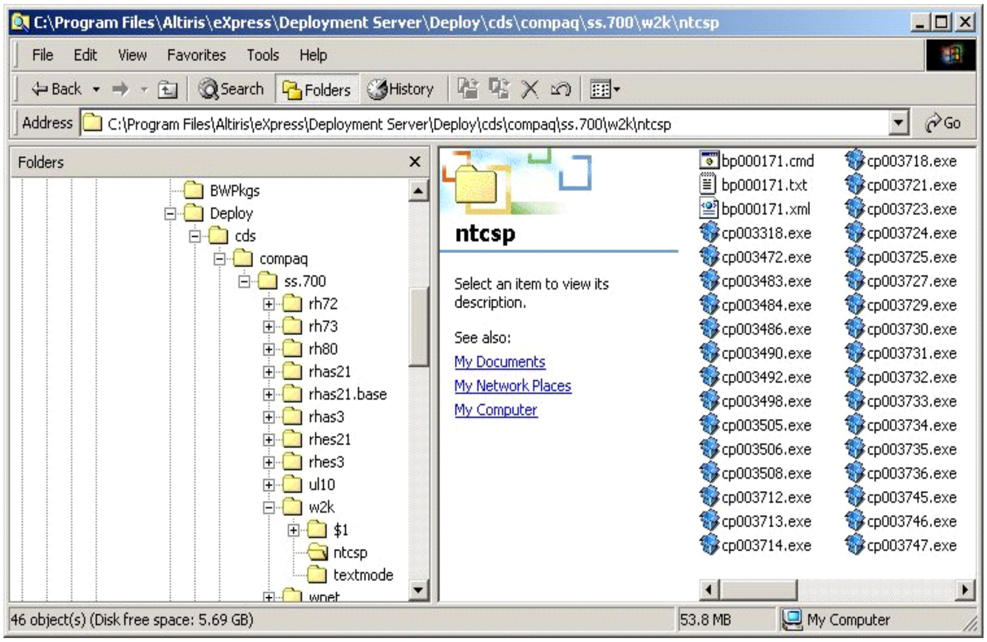
You only need to configure the Smart Components in the PSP one time; you do not need to configure the components each time they are deployed. After you configure the PSP, it is ready for deployment.

To configure the web agent (and other Smart Components) in the PSP for deployment, follow these steps:

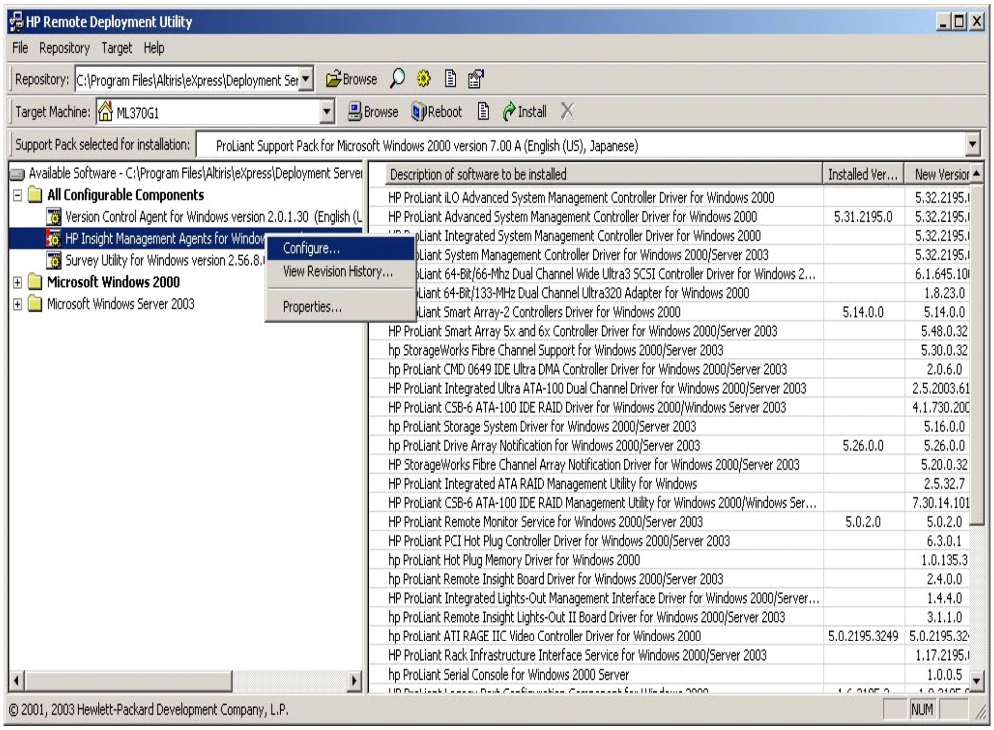
1. Open Microsoft Windows Explorer and browse to the following directory:

   C:\ProgramFiles\Altiris\eXpress\DeploymentServer\Deploy\cds\compaq\ss.xxx\w2k\ntcsp

   where *xxx* is the version of SmartStart you are using.



2. Locate and double-click *setup.exe*.
3. Click *OK* on the HP Remote Deployment Utility screen.
4. Expand the *All Configurable Components* directory in the tree in the left pane. Right-click *HP Insight Management Agents for Windows*. From the pop-up menu, select *Configure*. The item configuration screen displays.


HP Remote Deployment Utility
File Repository Target Help
Browse
Browse Reboot Install
Available Software - C:\Program Files\Altiris\eXpress\Deployment Server
All Configurable Components
Version Control Agent for Windows version 2.0.1.30 (English (L
HP Insight Management Agents for Window
Survey Utility for Windows version 2.56.8.(
Microsoft Windows 2000
Microsoft Windows Server 2003
Configure...
View Revision History...
Properties...
NUM

Repository: C:\Program Files\Altiris\eXpress\Deployment Ser

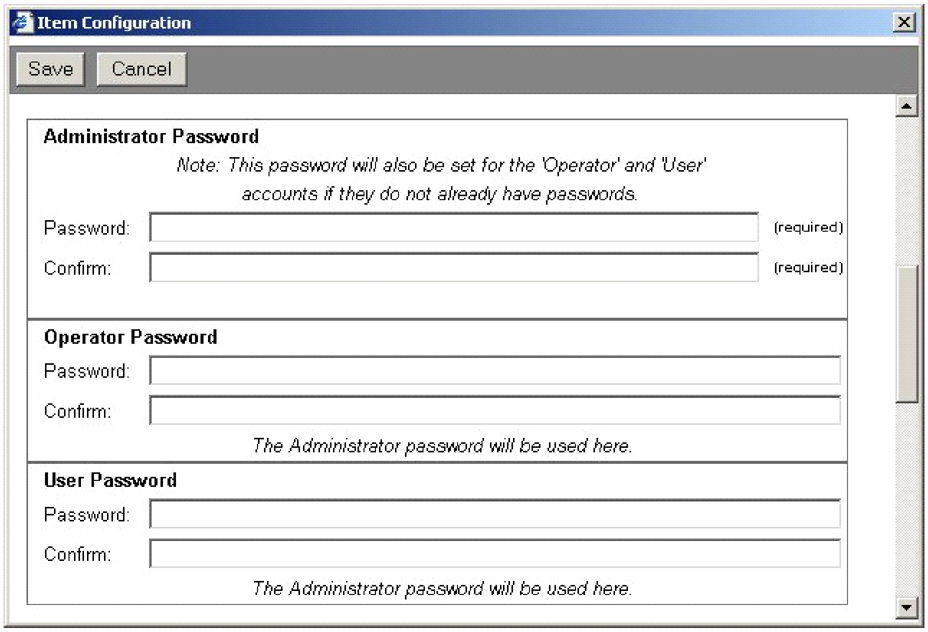
Target Machine: ML370G1

Support Pack selected for installation: ProLiant Support Pack for Microsoft Windows 2000 version 7.00 A (English (US), Japanese)

Description of software to be installed	Installed Ver...	New Versior
HP ProLiant iLO Advanced System Management Controller Driver for Windows 2000		5.32.2195.
HP ProLiant Advanced System Management Controller Driver for Windows 2000	5.31.2195.0	5.32.2195.
oLiant Integrated System Management Controller Driver for Windows 2000		5.32.2195.
oLiant System Management Controller Driver for Windows 2000/Server 2003		5.32.2195.
oLiant 64-Bit/66-Mhz Dual Channel Wide Ultra3 SCSI Controller Driver for Windows 2...		6.1.645.10
oLiant 64-Bit/133-MHz Dual Channel Ultra320 Adapter for Windows 2000		1.8.23.0
oLiant Smart Array-2 Controllers Driver for Windows 2000	5.14.0.0	5.14.0.0
HP ProLiant Smart Array 5x and 6x Controller Driver for Windows 2000/Server 2003		5.48.0.32
hp StorageWorks Fibre Channel Support for Windows 2000/Server 2003		5.30.0.32
hp ProLiant CMD 0649 IDE Ultra DMA Controller Driver for Windows 2000/Server 2003		2.0.6.0
HP ProLiant Integrated Ultra ATA-100 Dual Channel Driver for Windows 2000/Server 2003		2.5.2003.61
HP ProLiant CSB-6 ATA-100 IDE RAID Driver for Windows 2000/Windows Server 2003		4.1.730.20
hp ProLiant Storage System Driver for Windows 2000/Server 2003		5.16.0.0
hp ProLiant Drive Array Notification for Windows 2000/Server 2003	5.26.0.0	5.26.0.0
HP StorageWorks Fibre Channel Array Notification Driver for Windows 2000/Server 2003		5.20.0.32
HP ProLiant Integrated ATA RAID Management Utility for Windows		2.5.32.7
HP ProLiant CSB-6 ATA-100 IDE RAID Management Utility for Windows 2000/Windows Ser...		7.30.14.101
HP ProLiant Remote Monitor Service for Windows 2000/Server 2003	5.0.2.0	5.0.2.0
HP ProLiant PCI Hot Plug Controller Driver for Windows 2000/Server 2003		6.3.0.1
hp ProLiant Hot Plug Memory Driver for Windows 2000		1.0.135.3
hp ProLiant Remote Insight Board Driver for Windows 2000/Server 2003		2.4.0.0
HP ProLiant Integrated Lights-Out Management Interface Driver for Windows 2000/Server...		1.4.4.0
hp ProLiant Remote Insight Lights-Out II Board Driver for Windows 2000/Server 2003		3.1.1.0
hp ProLiant ATI RAGE IIC Video Controller Driver for Windows 2000	5.0.2195.3249	5.0.2195.32
HP ProLiant Rack Infrastructure Interface Service for Windows 2000/Server 2003		1.17.2195.
hp ProLiant Serial Console for Windows 2000 Server		1.0.0.5

© 2001, 2003 Hewlett-Packard Development Company, L.P.

5. Scroll down to modify the Administrator password. Enter *password* in the Password field and *password* in the Confirm field.



Administrator Password

Note: This password will also be set for the 'Operator' and 'User' accounts if they do not already have passwords.

Password: (required)

Confirm: (required)

Operator Password

Password:

Confirm:

The Administrator password will be used here.

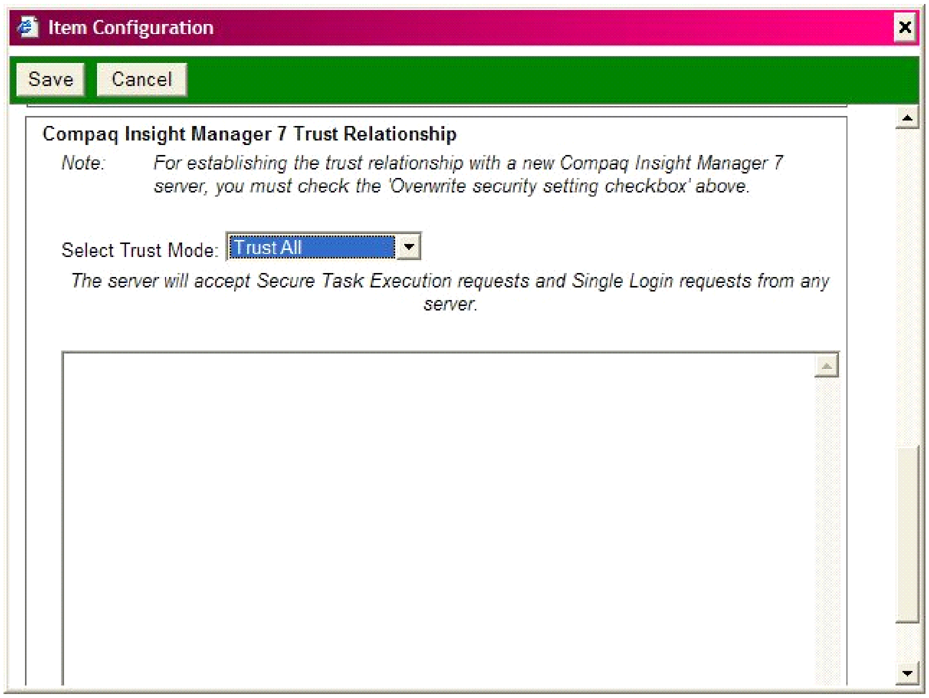
User Password

Password:

Confirm:

The Administrator password will be used here.

6. Scroll down to the Insight Manager 7 Trust Relationship section, select *Trust All* from the Select Trust Mode drop-down menu, and click *Save*. The web agent is now configured.



Compaq Insight Manager 7 Trust Relationship

Note: For establishing the trust relationship with a new Compaq Insight Manager 7 server, you must check the 'Overwrite security setting checkbox' above.

Select Trust Mode: Trust All

The server will accept Secure Task Execution requests and Single Login requests from any server.

7. Close the HP Remote Deployment Utility screen.

Exercise 2 — Deploying a scripted Windows 2000 installation job to a PXE-enabled server

Customizing the unattended installation file

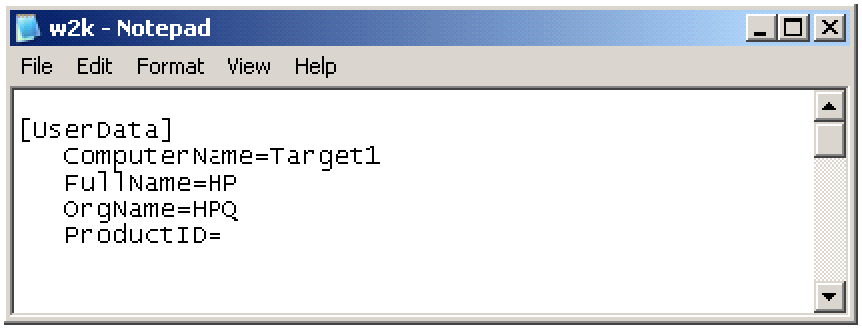
The first step in deploying a scripted installation is to ensure that the configuration is customized to your environment. To modify the unattend.txt file for your environment, follow these steps:

1. Open Microsoft Windows Explorer on the Deployment Server and browse to the C:\Program Files\Altiris\eXpress\Deployment Server\Deploy\configs directory. Locate the w2k.txt file and open it using a text editor. This is the unattend.txt file used during the scripted installation.
2. In the [UserData] section, change the ComputerName setting to:

   `ComputerName=Targetx` (where *x* is your group number)
3. Add the line:

   `ProductID=XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`

   Replace *`XXXXX-XXXXX-XXXXX-XXXXX-XXXXX`* with the Microsoft Product Key for your copy of Microsoft Windows. This should be provided by your instructor.



```
[UserData]
   ComputerName=Target1
   FullName=HP
   OrgName=HPQ
   ProductID=
```

Note

If you are using the Select Edition of Microsoft Windows (for Microsoft Select Customers only), omit the entire ProductID= line.

4. Save the file. You will use this file during the scripted installation.

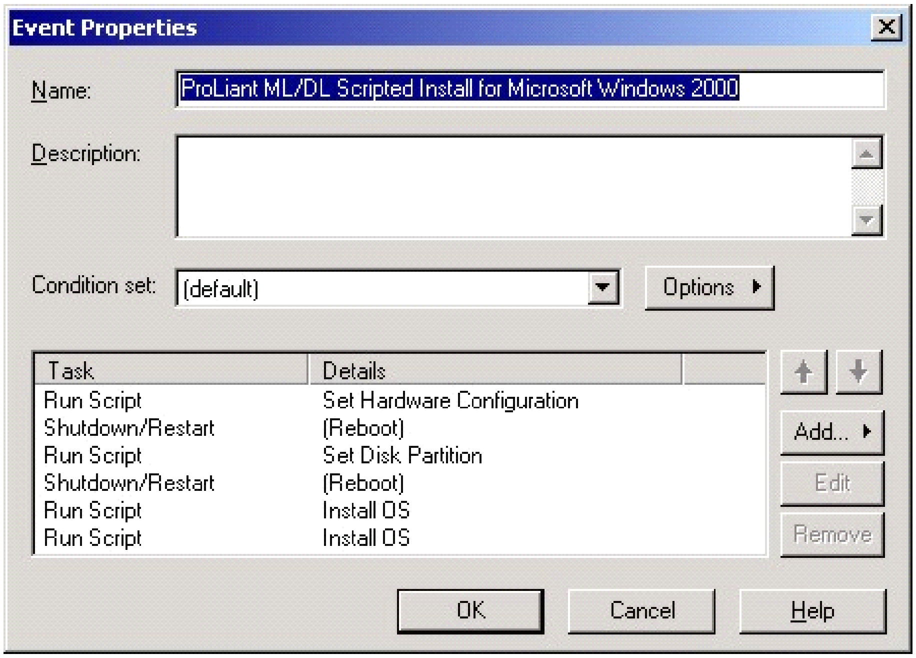
Windows 2000 scripted installation job

To perform an unattended Windows 2000 scripted installation, follow these steps:

1. From the Deployment Server console Jobs pane, expand the Microsoft Windows 2000 Scripted Install Jobs folder. Open the *ProLiant ML/DL Scripted Install for Microsoft Windows 2000* job by double-clicking the job name.

Note

If you are using ProLiant BL10e servers, open the *ProLiant BL10e Scripted Install for Windows 2000* job.



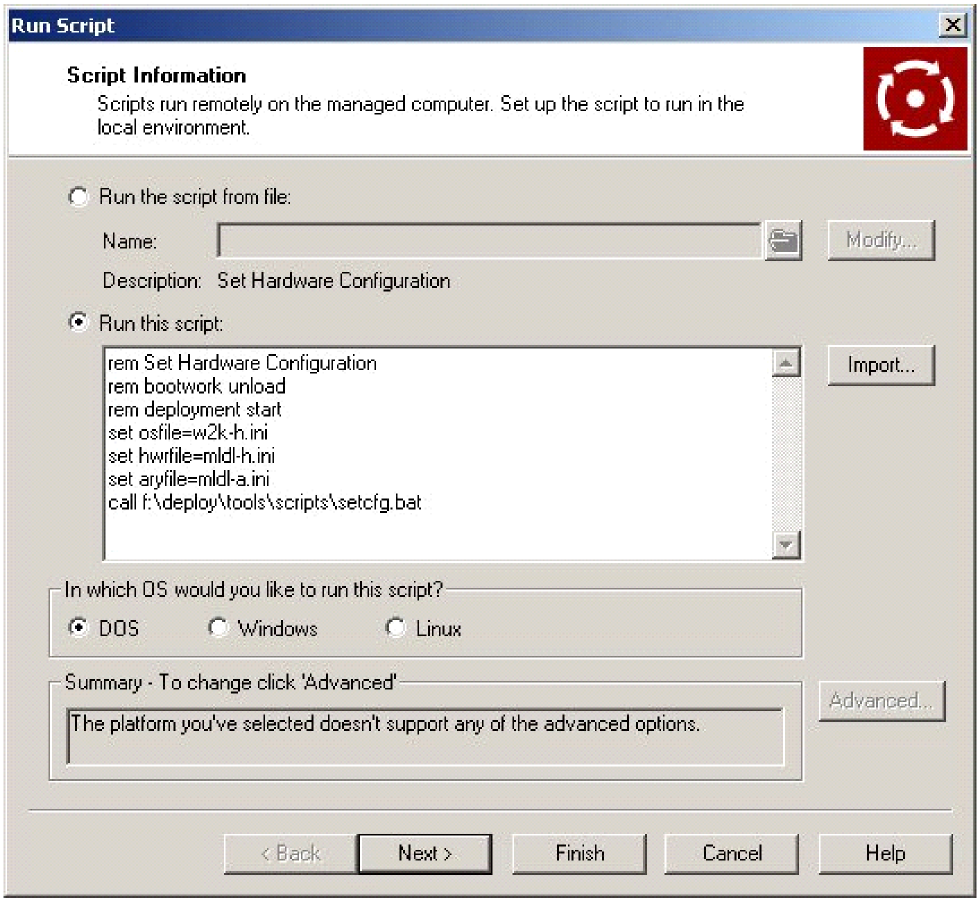
Name: ProLiant ML/DL Scripted Install for Microsoft Windows 2000

Description:

Condition set: (default)

Task	Details
Run Script	Set Hardware Configuration
Shutdown/Restart	(Reboot)
Run Script	Set Disk Partition
Shutdown/Restart	(Reboot)
Run Script	Install OS
Run Script	Install OS

2. View details of the tasks by clicking the individual tasks within the job. Note how the DOS environment variables are used to specify the configuration files used during the job.



Run Script

Script Information

Scripts run remotely on the managed computer. Set up the script to run in the local environment.

○ Run the script from file:

Name:

Description: Set Hardware Configuration

● Run this script:

```
rem Set Hardware Configuration
rem bootwork unload
rem deployment start
set osfile=w2k-h.ini
set hwrfile=mldl-h.ini
set aryfile=mldl-a.ini
call f:\deploy\tools\scripts\setcfg.bat
```

In which OS would you like to run this script?

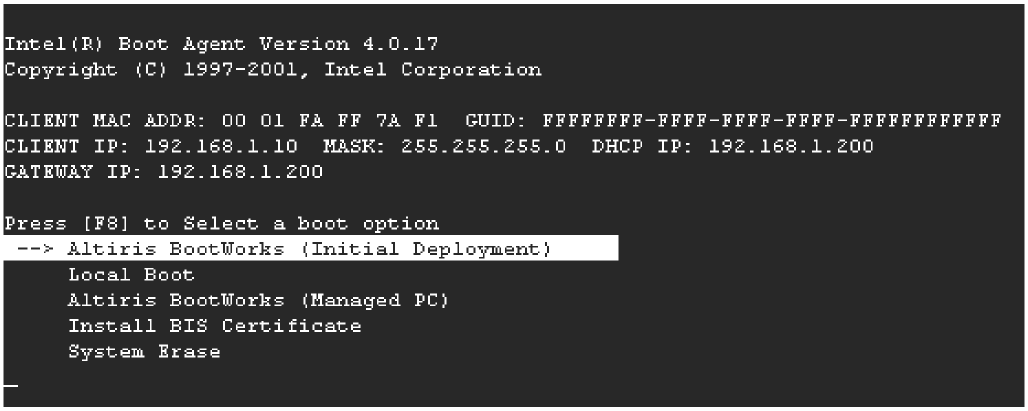
● DOS ○ Windows ○ Linux

Summary - To change click 'Advanced'

The platform you've selected doesn't support any of the advanced options.

3. After you have finished browsing, click *Cancel* to return to the Deployment Server console.

4. To begin the deployment, power on the target server. At the PXE Boot Selection menu, *Altiris BootWorks (Initial Deployment)* should be selected. The deployment should run automatically.



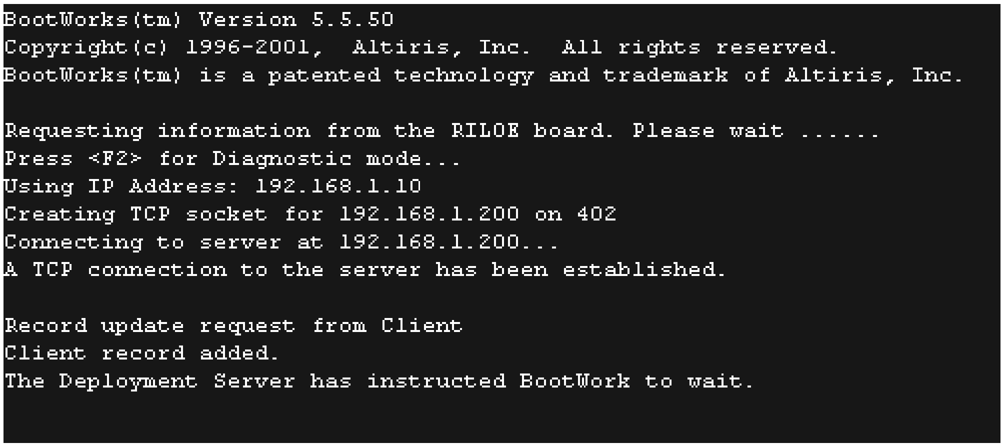
```
Intel(R) Boot Agent Version 4.0.17
Copyright (C) 1997-2001, Intel Corporation

CLIENT MAC ADDR: 00 01 FA FF 7A F1  GUID: FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
CLIENT IP: 192.168.1.10  MASK: 255.255.255.0  DHCP IP: 192.168.1.200
GATEWAY IP: 192.168.1.200

Press [F8] to Select a boot option
 --> Altiris BootWorks (Initial Deployment)
     Local Boot
     Altiris BootWorks (Managed PC)
     Install BIS Certificate
     System Erase
_
```

Note

If you are installing on a ProLiant BL10e server, you will **not** see the preceding screen in the Integrated Administrator Remote Console session. The ProLiant BL10e has limited remote console capabilities. After the system loads an operating system, including a DOS-based PXE boot image, the Integrated Administrator Remote Console session is no longer updated.

The Initial Deployment job adds the target server to the New Computers group in the Deployment Server console. The target server displays in the Deployment Server console with the Waiting State icon:

5. After the target server registers with the Deployment Server, the BootWorks agent instructs the target server to wait. The target server does not perform any other action until a job is assigned to it from the Deployment Server console.

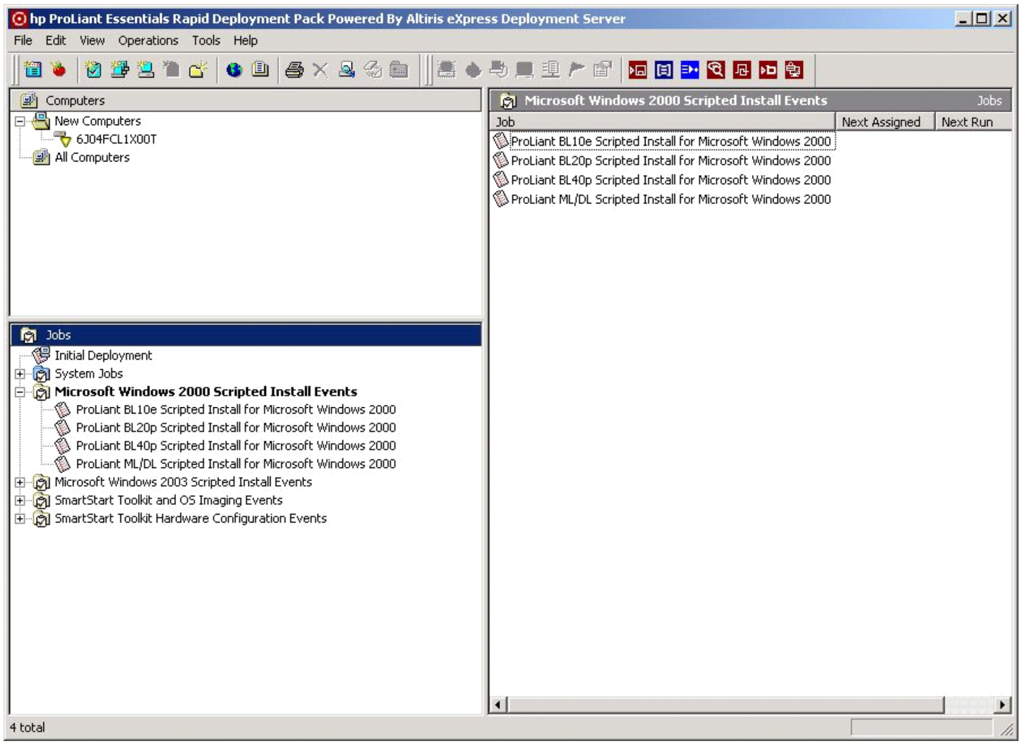


```
BootWorks(tm) Version 5.5.50
Copyright(c) 1996-2001,  Altiris, Inc.  All rights reserved.
BootWorks(tm) is a patented technology and trademark of Altiris, Inc.

Requesting information from the RILOE board. Please wait ......
Press <F2> for Diagnostic mode...
Using IP Address: 192.168.1.10
Creating TCP socket for 192.168.1.200 on 402
Connecting to server at 192.168.1.200...
A TCP connection to the server has been established.

Record update request from Client
Client record added.
The Deployment Server has instructed BootWork to wait.
```

Note

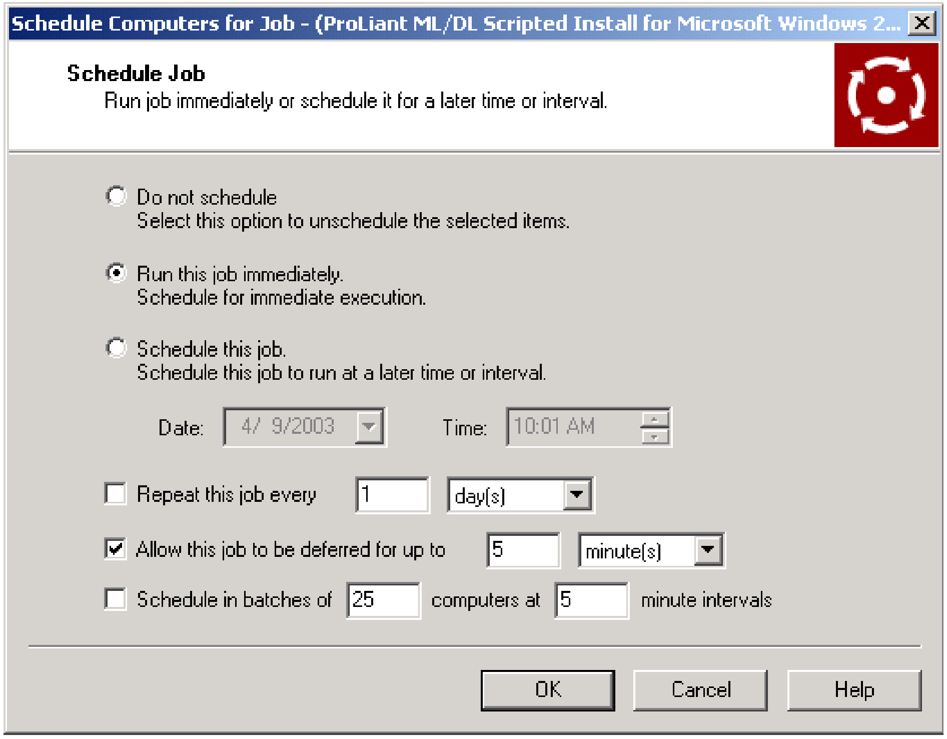
This screen is not visible through a remote console connection to a ProLiant BL10e server. If the Diagnostic Adapter is attached to a ProLiant BL10e, you can view the screen locally.

6. In the Deployment Server console, drag and drop the appropriate Microsoft Windows 2000 Scripted Install job on to the target server.


hp ProLiant Essentials Rapid Deployment Pack Powered By Altiris eXpress Deployment Server
File
Edit
View
Operations
Tools
Help
Computers
New Computers
6J04FCL1X00T
All Computers
Jobs
Initial Deployment
System Jobs
Microsoft Windows 2000 Scripted Install Events
ProLiant BL10e Scripted Install for Microsoft Windows 2000
ProLiant BL20p Scripted Install for Microsoft Windows 2000
ProLiant BL40p Scripted Install for Microsoft Windows 2000
ProLiant ML/DL Scripted Install for Microsoft Windows 2000
Microsoft Windows 2003 Scripted Install Events
SmartStart Toolkit and OS Imaging Events
SmartStart Toolkit Hardware Configuration Events
Microsoft Windows 2000 Scripted Install Events
Jobs
4 total

Job	Next Assigned	Next Run
ProLiant BL10e Scripted Install for Microsoft Windows 2000		
ProLiant BL20p Scripted Install for Microsoft Windows 2000		
ProLiant BL40p Scripted Install for Microsoft Windows 2000		
ProLiant ML/DL Scripted Install for Microsoft Windows 2000		

7. In the Schedule Computers for Job screen, select *Run this job immediately* and click *OK* to start the scripted installation on your target server.



Schedule Computers for Job - (ProLiant ML/DL Scripted Install for Microsoft Windows 2...

Schedule Job

Run job immediately or schedule it for a later time or interval.

○ Do not schedule
Select this option to unschedule the selected items.

● Run this job immediately.
Schedule for immediate execution.

○ Schedule this job.
Schedule this job to run at a later time or interval.

Date: 4/ 9/2003 Time: 10:01 AM

☐ Repeat this job every 1 day(s)

☑ Allow this job to be deferred for up to 5 minute(s)

☐ Schedule in batches of 25 computers at 5 minute intervals

8. In the confirmation dialog box, click *Yes* to perform the scripted install.

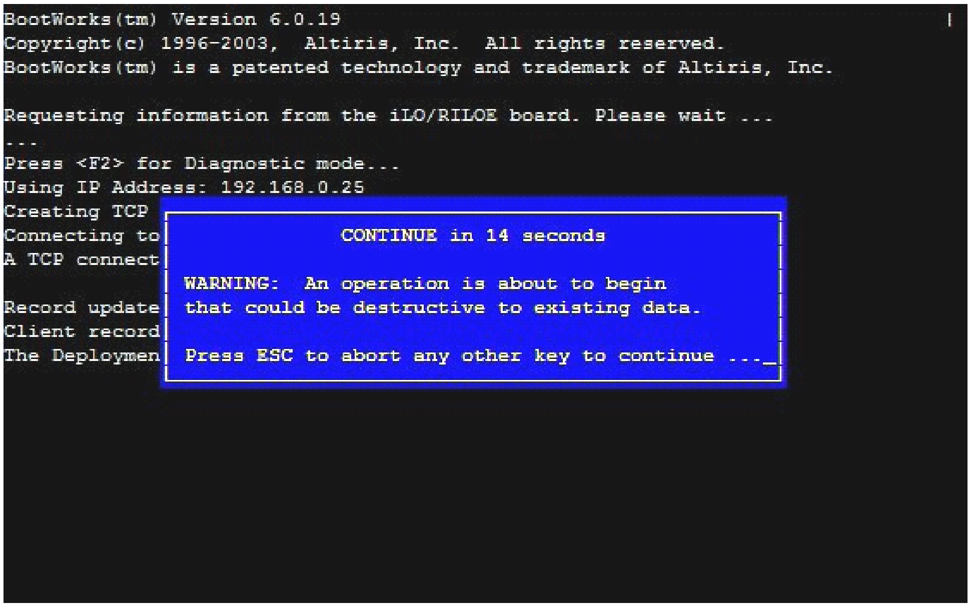
Note

To bypass this step in the future, select the *Don't prompt me again* box.

9. When a warning message displays on the target server, let the timer count down or press any key (**except** *ESC*) to continue with the installation.

Note

This screen is not visible through a remote console connection to a ProLiant BL10e server unless the Diagnostic Adapter is attached to it.



```
BootWorks(tm) Version 6.0.19
Copyright(c) 1996-2003,  Altiris, Inc.  All rights reserved.
BootWorks(tm) is a patented technology and trademark of Altiris, Inc.

Requesting information from the iLO/RILOE board. Please wait ...
...
Press <F2> for Diagnostic mode...
Using IP Address: 192.168.0.25
Creating TCP
Connecting to             CONTINUE in 14 seconds
A TCP connect
              WARNING:  An operation is about to begin
Record update that could be destructive to existing data.
Client record
The Deploymen Press ESC to abort any other key to continue ..._
```

The scripted installation of Windows 2000 continues unattended and takes approximately 30 to 45 minutes to complete.

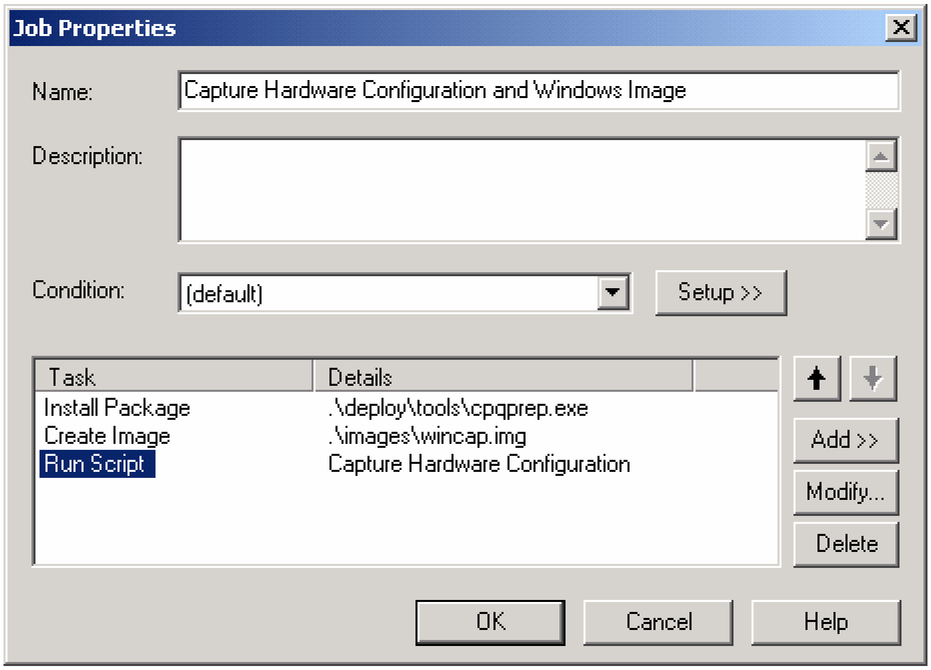
Exercise 3 — Deploying servers using imaging

After you have completed a scripted installation of Windows 2000 and deployed the latest service pack, your server is ready to be deployed. As part of the scripted installation process, the Deployment Agent for Windows was added to the server. This server now becomes your reference server for future deployments.

Capturing a hardware configuration and disk image

To capture a disk image from your reference server, follow these steps:

1. In the Jobs pane of the Deployment Server console, expand the *SmartStart Toolkit and OS Imaging Jobs* folder.
2. Double-click the *Capture Hardware Configuration and Windows Image* job.
3. In the Job Properties screen, double-click the *Run Script* task. The Run Script screen displays.



Name: Capture Hardware Configuration and Windows Image

Description:

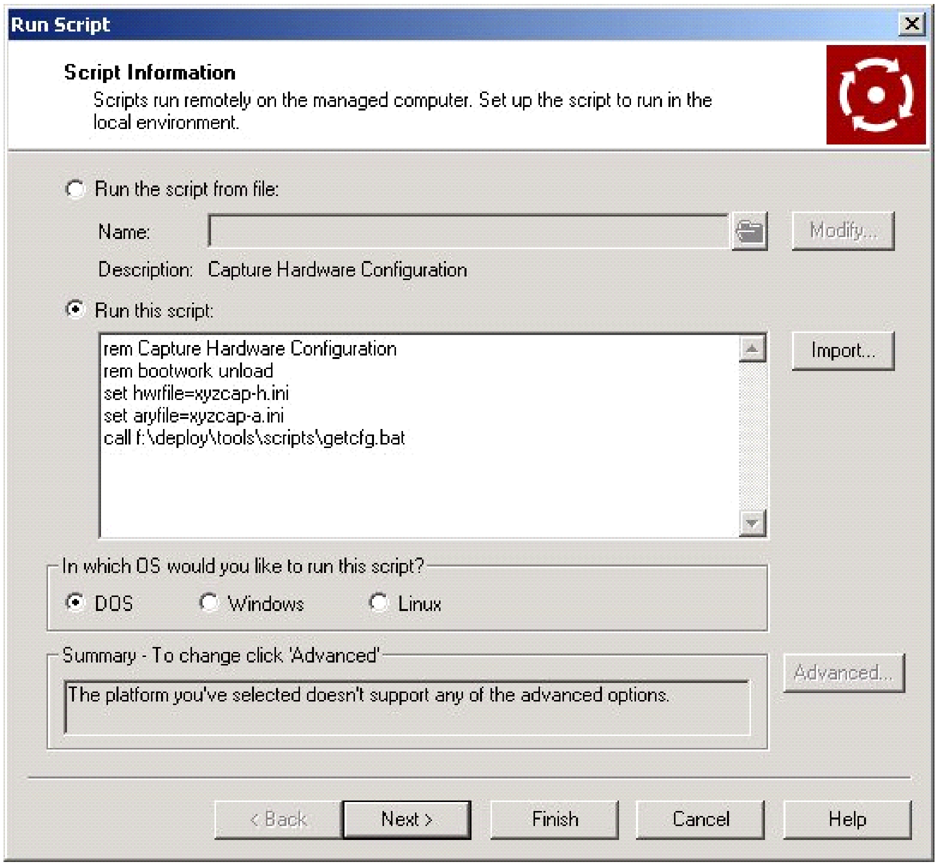
Condition: (default)

Task	Details
Install Package	.\deploy\tools\cpqprep.exe
Create Image	.\images\wincap.img
Run Script	Capture Hardware Configuration

4. In the Run Script screen, change the default names of the hardware information and array information files that will be captured. These files will be used in the image deployment jobs in the next exercise.

   - Change the wincap-h.ini file to *xyzcap-h.ini* (where *xyz* are your initials).
   - Change the wincap-a.ini file to *xyzcap-a.ini* (where *xyz* are your initials).

   Click *Finish* to return to the Job Properties screen.



Script Information

Scripts run remotely on the managed computer. Set up the script to run in the local environment.

○ Run the script from file:

Name:

Description: Capture Hardware Configuration

● Run this script:

```
rem Capture Hardware Configuration
rem bootwork unload
set hwrfile=xyzcap-h.ini
set aryfile=xyzcap-a.ini
call f:\deploy\tools\scripts\getcfg.bat
```

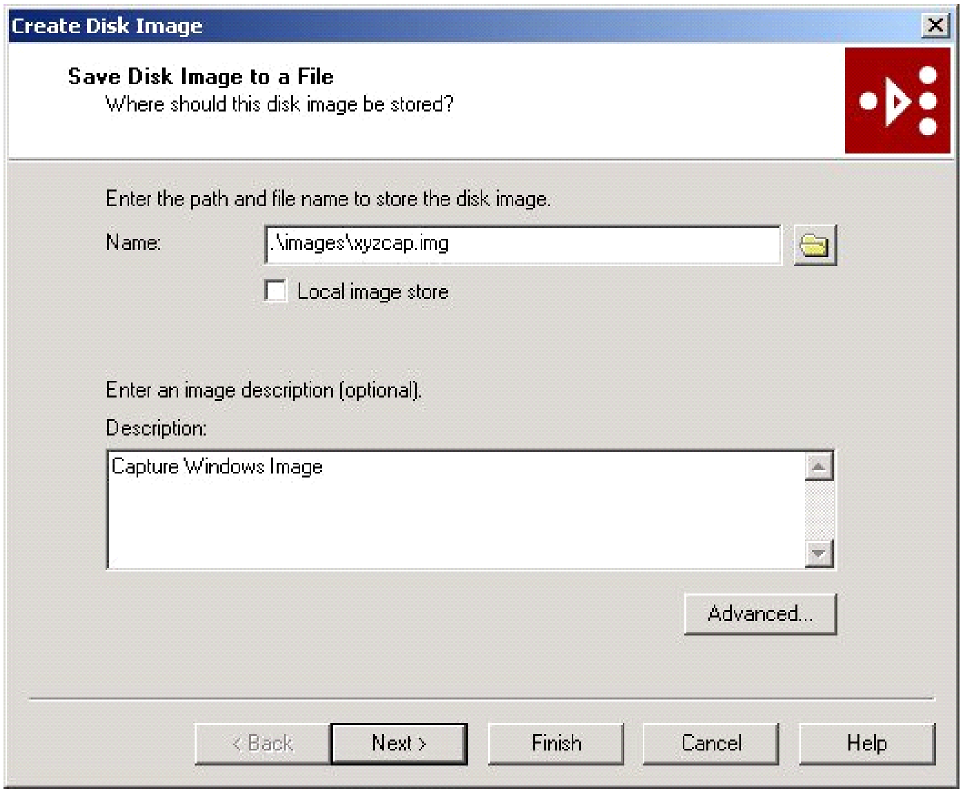
In which OS would you like to run this script?

● DOS ○ Windows ○ Linux

Summary - To change click 'Advanced'

The platform you've selected doesn't support any of the advanced options.

5. In the Job Properties screen, double-click the *Create Image* task to open the Save Disk Image to a File screen.
6. Change the default image file name *wincap.img* to *xyzcap.img* (where *xyz* are your initials). Click *Advanced* to view the optional settings for imaging.


Create Disk Image
Save Disk Image to a File
Where should this disk image be stored?
Advanced...
< Back
Next >
Finish
Cancel
Help

Enter the path and file name to store the disk image.

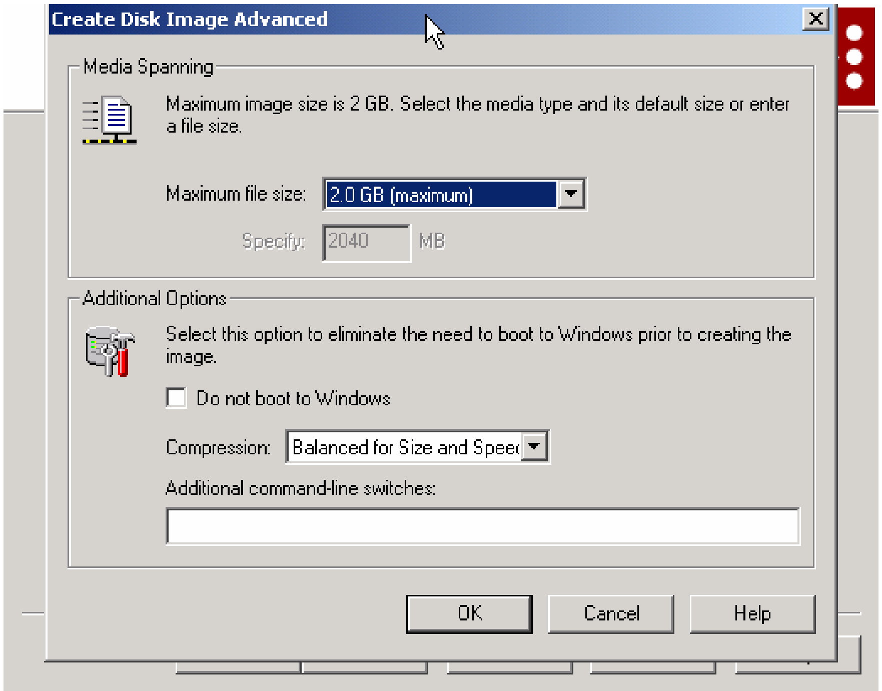
Name: .\images\xyzcap.img

☐ Local image store

Enter an image description (optional).

Description: Capture Windows Image

7. In the Create Disk Image Advanced screen, note that you can change the maximum file size and compression ratio. Click *OK* to return to the Create Disk Image screen.



Create Disk Image Advanced

Media Spanning

Maximum image size is 2 GB. Select the media type and its default size or enter a file size.

Maximum file size: 2.0 GB (maximum)

Specify: 2040 MB

Additional Options

Select this option to eliminate the need to boot to Windows prior to creating the image.

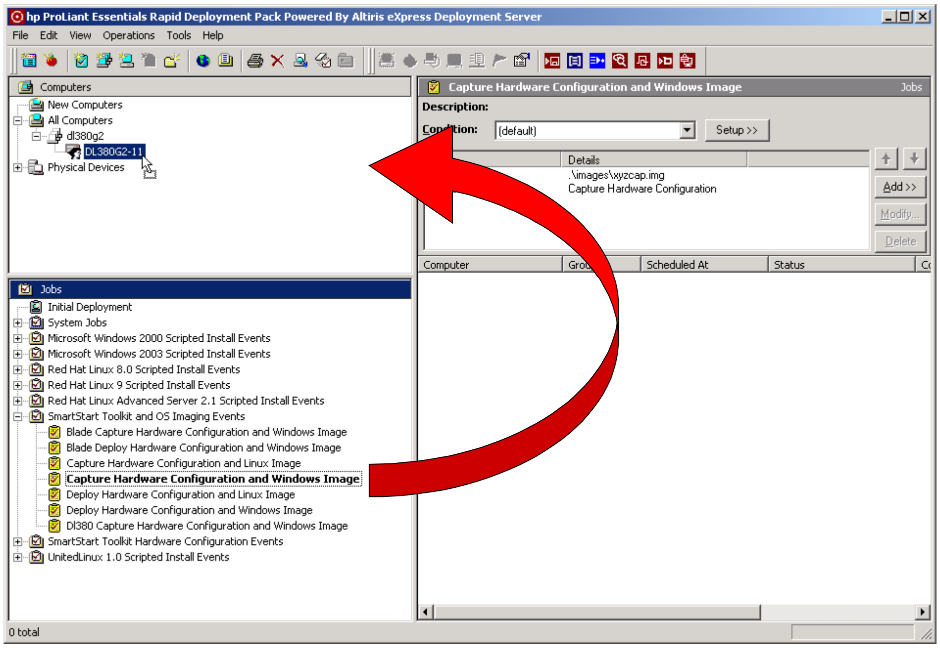
☐ Do not boot to Windows

Compression: Balanced for Size and Speec

Additional command-line switches:

8. Click *Finish* → *OK* to close the Job Properties screen.

9. In the Deployment Server console, drag and drop the modified *Capture Hardware Configuration and Windows Image* to the reference server icon in the Computers pane.

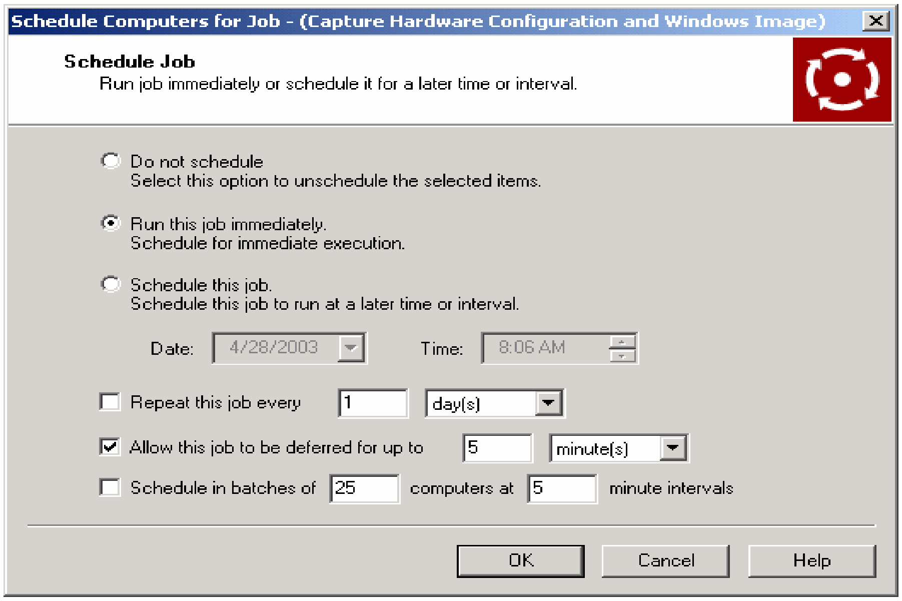

hp ProLiant Essentials Rapid Deployment Pack Powered By Altiris eXpress Deployment Server
File
Edit
View
Operations
Tools
Help
Computers
New Computers
All Computers
dl380g2
DL380G2-11
Physical Devices
Jobs
Initial Deployment
System Jobs
Microsoft Windows 2000 Scripted Install Events
Microsoft Windows 2003 Scripted Install Events
Red Hat Linux 8.0 Scripted Install Events
Red Hat Linux 9 Scripted Install Events
Red Hat Linux Advanced Server 2.1 Scripted Install Events
SmartStart Toolkit and OS Imaging Events
Blade Capture Hardware Configuration and Windows Image
Blade Deploy Hardware Configuration and Windows Image
Capture Hardware Configuration and Linux Image
Capture Hardware Configuration and Windows Image
Deploy Hardware Configuration and Linux Image
Deploy Hardware Configuration and Windows Image
Dl380 Capture Hardware Configuration and Windows Image
SmartStart Toolkit Hardware Configuration Events
UnitedLinux 1.0 Scripted Install Events
0 total
Capture Hardware Configuration and Windows Image
Jobs
Setup >>
Add >>
Modify...
Delete
Computer
Grou
Scheduled At
Status
Co

Description:

Condition: (default)

Details
.\images\xyzcap.img
Capture Hardware Configuration

10. Select *Run this job immediately* in the Schedule Computers for Job screen and click *OK*. The reference server restarts and processes the job. The PXE boot automatically selects *Managed Computer* and continues through the process.


Schedule Computers for Job - (Capture Hardware Configuration and Windows Image)
OK
Cancel
Help

Schedule Job
Run job immediately or schedule it for a later time or interval.

○ Do not schedule
Select this option to unschedule the selected items.

● Run this job immediately.
Schedule for immediate execution.

○ Schedule this job.
Schedule this job to run at a later time or interval.

Date: 4/28/2003 Time: 8:06 AM

☐ Repeat this job every 1 day(s)

☑ Allow this job to be deferred for up to 5 minute(s)

☐ Schedule in batches of 25 computers at 5 minute intervals

Deploying a Linux disk image

To deploy a Linux disk image, follow these steps:

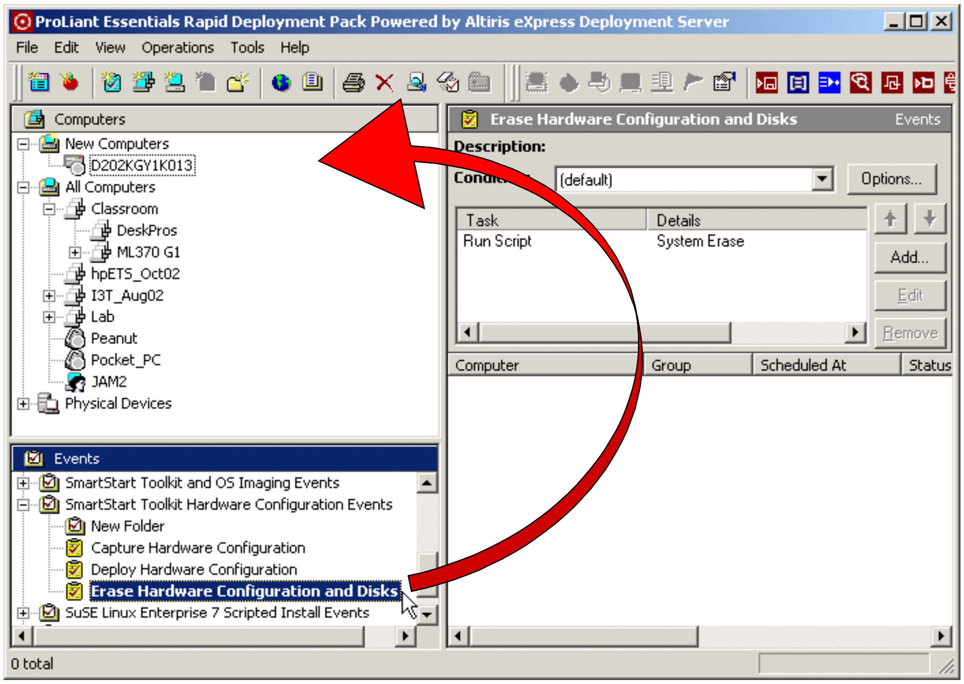
1. Erase the configuration on your target server before deploying the Linux image file by performing these steps:

Caution

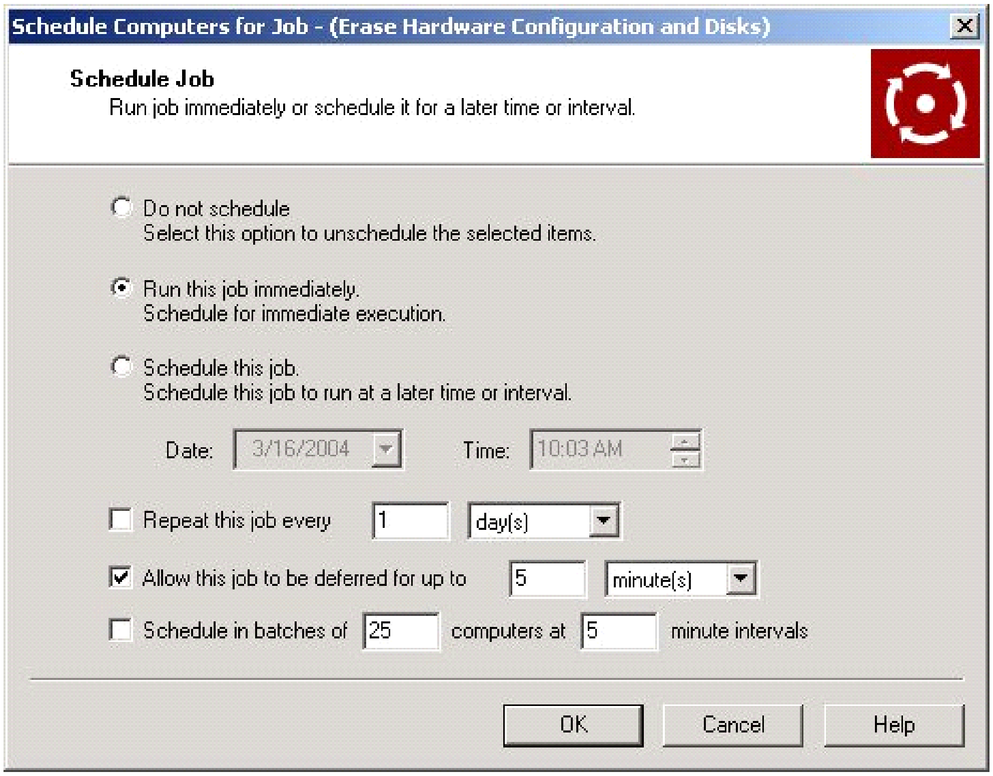
This step is data destructive. Consult with your instructor before completing this step.

   a. In the Deployment Server console, expand the *SmartStart Toolkit Hardware Configuration Jobs* folder.

   b. Drag and drop the *Erase Hardware Configuration and Disks* job to the reference server icon in the Computers pane.


ProLiant Essentials Rapid Deployment Pack Powered by Altiris eXpress Deployment Server
File Edit View Operations Tools Help
Computers
New Computers
D202KGY1K013
All Computers
Classroom
DeskPros
ML370 G1
hpETS_Oct02
I3T_Aug02
Lab
Peanut
Pocket_PC
JAM2
Physical Devices
Events
SmartStart Toolkit and OS Imaging Events
SmartStart Toolkit Hardware Configuration Events
New Folder
Capture Hardware Configuration
Deploy Hardware Configuration
Erase Hardware Configuration and Disks
SuSE Linux Enterprise 7 Scripted Install Events
0 total
Erase Hardware Configuration and Disks
Events
Description:
Condi...
(default)
Options...
Task
Details
Run Script
System Erase
Add...
Edit
Remove
Computer
Group
Scheduled At
Status

2. From the Schedule Computers for Job screen, select *Run this job immediately* and click *OK* to start the job.



Schedule Computers for Job - (Erase Hardware Configuration and Disks)

Schedule Job

Run job immediately or schedule it for a later time or interval.

○ Do not schedule
Select this option to unschedule the selected items.

● Run this job immediately.
Schedule for immediate execution.

○ Schedule this job.
Schedule this job to run at a later time or interval.

Date: 3/16/2004 Time: 10:03 AM

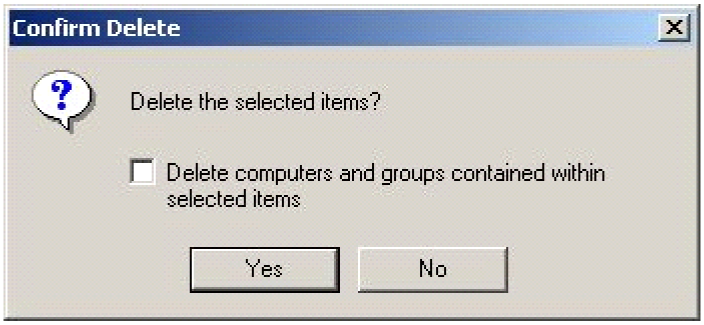
☐ Repeat this job every 1 day(s)

☑ Allow this job to be deferred for up to 5 minute(s)

☐ Schedule in batches of 25 computers at 5 minute intervals

3. After the erase job has run, delete your reference server from the Deployment Server console by right-clicking its icon and selecting *Delete*.

4. Select the *Delete computers and groups contained within the selected items* box and click *Yes*.



Confirm Delete

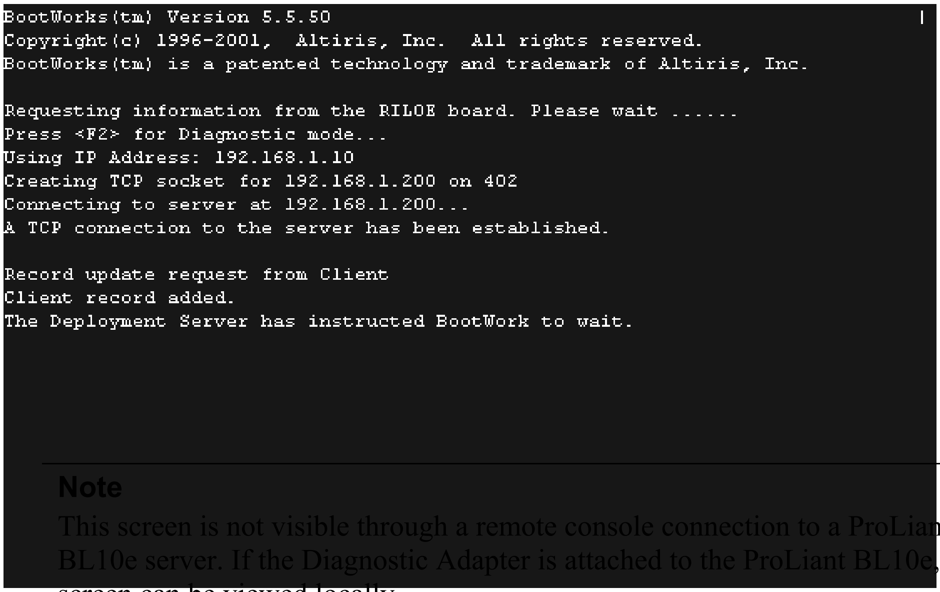
Delete the selected items?

☐ Delete computers and groups contained within selected items

5. If necessary, cycle the power on your target server. At the PXE Boot Selection menu, *Altiris BootWorks (Initial Deployment)* should be auto-selected. The Initial Deployment job is run for all new computers that are not registered in the Altiris database. This job will not perform any work, such as imaging the server. It displays the new computer in the Deployment Server console and waits for further instructions.

> **Note**
>
> This screen is not visible through a remote console connection to a ProLiant BL10e server. If the Diagnostic Adapter is attached to the ProLiant BL10e server, you can view it locally. The ProLiant BL10e has limited remote console capabilities. After the system loads any operating system, including a DOS-based PXE boot image, the Integrated Administrator Remote Console session is no longer updated.

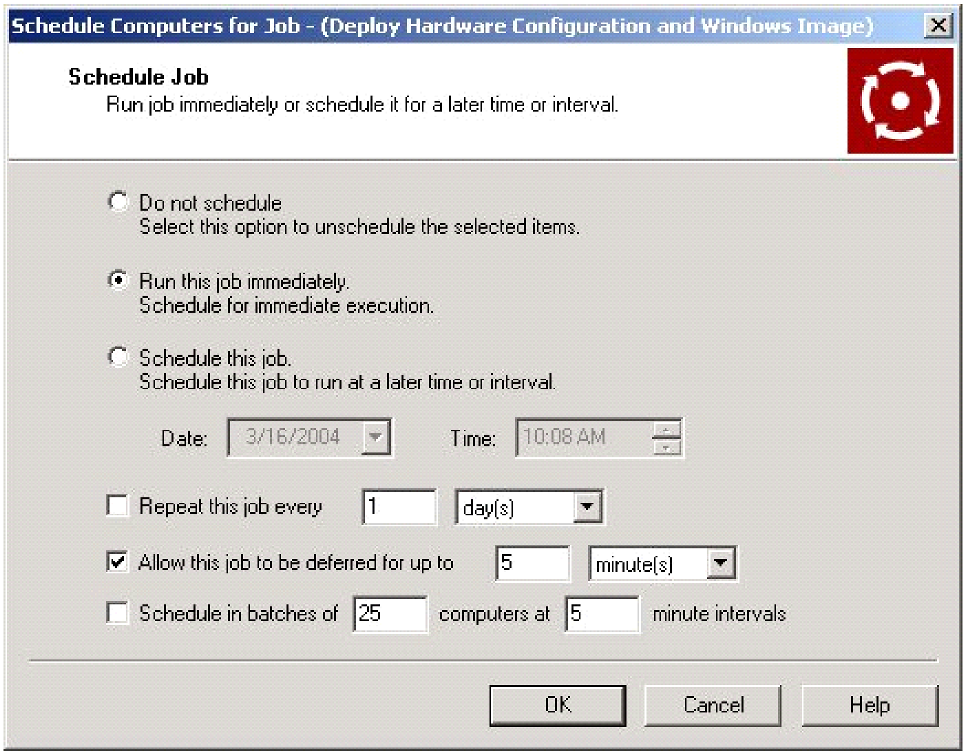
The Initial Deployment job adds the target server to the New Computers group in the Deployment Server console. The target server displays in the Deployment Server console with the Waiting State icon:



```
BootWorks(tm) Version 5.5.50
Copyright(c) 1996-2001,  Altiris, Inc.  All rights reserved.
BootWorks(tm) is a patented technology and trademark of Altiris, Inc.

Requesting information from the RILOE board. Please wait ......
Press <F2> for Diagnostic mode...
Using IP Address: 192.168.1.10
Creating TCP socket for 192.168.1.200 on 402
Connecting to server at 192.168.1.200...
A TCP connection to the server has been established.

Record update request from Client
Client record added.
The Deployment Server has instructed BootWork to wait.
```

> **Note**
>
> This screen is not visible through a remote console connection to a ProLiant BL10e server. If the Diagnostic Adapter is attached to the ProLiant BL10e, the screen can be viewed locally.

6. In the Deployment Server console, drag and drop the modified *Deploy Hardware Configuration and Linux Image* job to the target server icon in the Computers pane.
7. In the Schedule Computers for Job screen, select *Run this job immediately* and click *OK*.



Schedule Computers for Job - (Deploy Hardware Configuration and Windows Image)

Schedule Job

Run job immediately or schedule it for a later time or interval.

○ Do not schedule
Select this option to unschedule the selected items.

● Run this job immediately.
Schedule for immediate execution.

○ Schedule this job.
Schedule this job to run at a later time or interval.

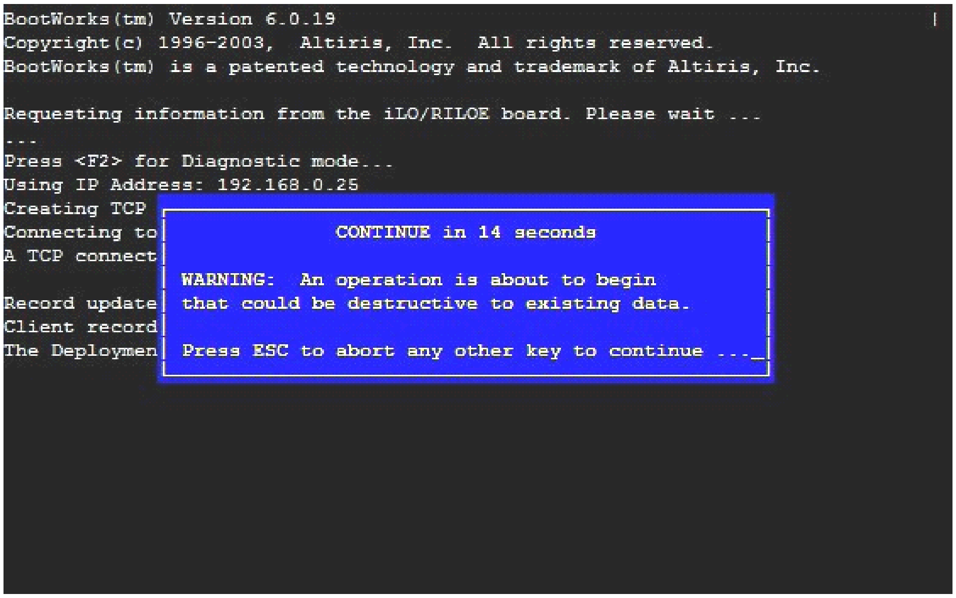
Date: 3/16/2004 Time: 10:08 AM

☐ Repeat this job every 1 day(s)

☑ Allow this job to be deferred for up to 5 minute(s)

☐ Schedule in batches of 25 computers at 5 minute intervals

8. When a warning message displays on the target server, let the timer count down or press any key (**except** *Esc*) to continue with the installation. No further interaction with the target server is required as the image deploys.



```
BootWorks(tm) Version 6.0.19                                                  |
Copyright(c) 1996-2003,  Altiris, Inc.  All rights reserved.
BootWorks(tm) is a patented technology and trademark of Altiris, Inc.

Requesting information from the iLO/RILOE board. Please wait ...
...
Press <F2> for Diagnostic mode...
Using IP Address: 192.168.0.25
Creating TCP  ┌────────────────────────────────────────────────────┐
Connecting to│              CONTINUE in 14 seconds                 │
A TCP connect│                                                     │
             │ WARNING:  An operation is about to begin            │
Record update│ that could be destructive to existing data.         │
Client record│                                                     │
The Deploymen│ Press ESC to abort any other key to continue ..._   │
             └─────────────────────────────────────────────────────┘
```

Exercise 4 — Configuring a simple file server with Samba using smb.conf

In this exercise, you will set up a basic Samba server that contains the following components:

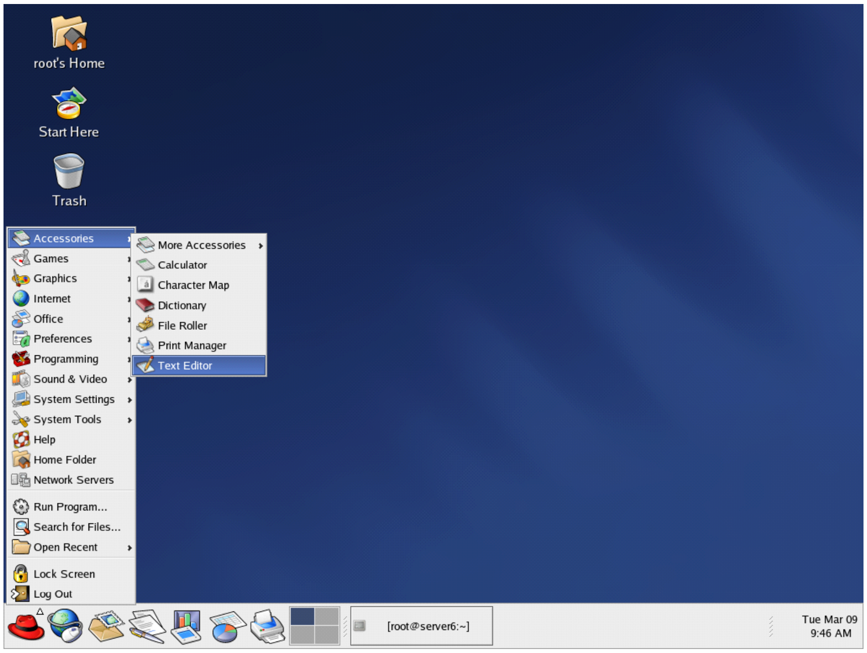
- Basic security measures
- Different home directories for each user
- A public share to allow access to anyone with access to the Samba server
- A printer share

There are many ways to configure Samba. In this exercise, you will use a text editor to edit the smb.conf file.

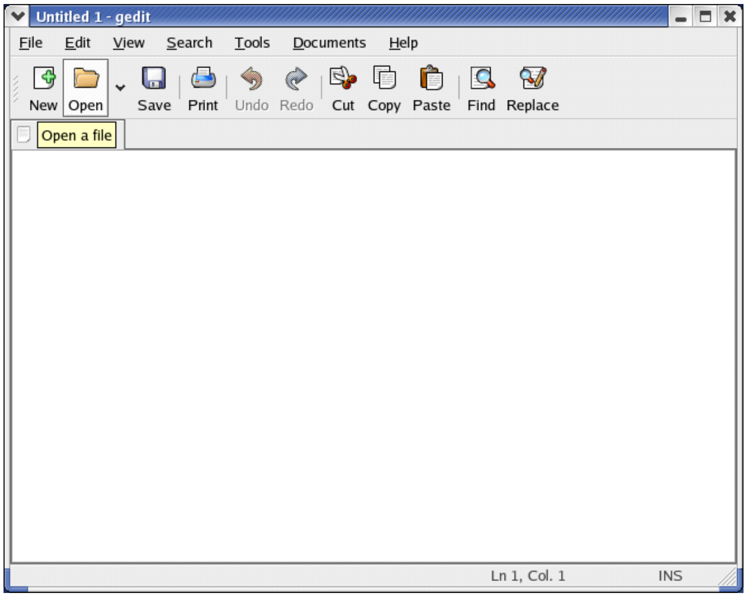
Configuring a Samba server using the smb.conf file

1. Log in to the machine as *root*.
2. Rename the */etc/samba/smb.conf* file to back it up:
   ```
   mv /etc/samba/smb.conf /etc/samba/smb.conf.bak
   ```
3. Create a new *smb.conf* file:
   ```
   touch /etc/samba/smb.conf
   ```
4. Create a new folder called *public*:
   ```
   mkdir /home/public
   ```
5. Change permissions on the folder to allow everyone read, write, and list access:
   ```
   chmod 777 /home/public
   ```
6. If Xwindows is not started, start Xwindows with the following command:
   ```
   startx
   ```

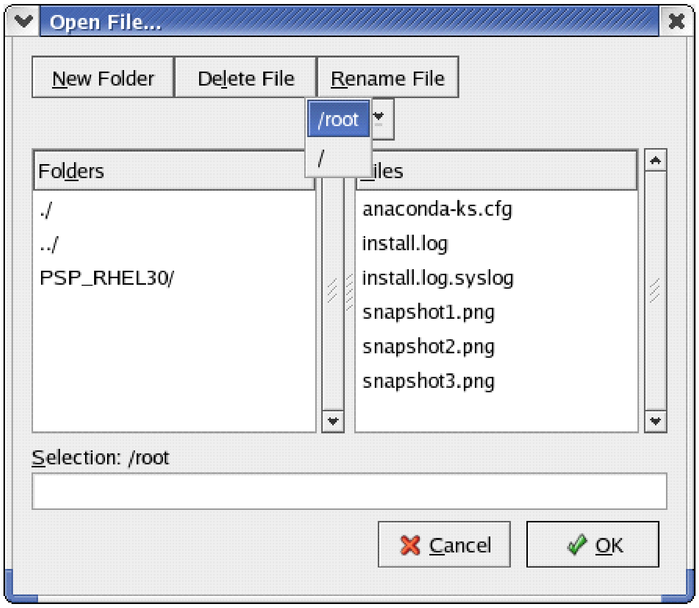
7. Click the *Red Hat Main Menu* icon in the lower left-hand corner of the screen. Click *Accessories* → *Text Editor*.



8. Click *Open* on the toolbar of the text editor to display the Open File Dialog box.

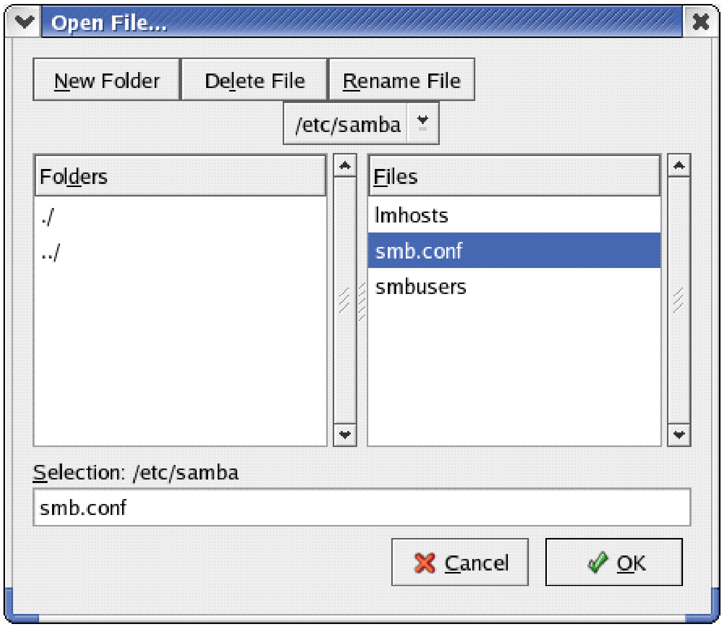


9. Click the box labeled */root* and change the directory to /.



Selection: /root

10. Double-click the *etc* folder.
11. Double-click the *samba* folder.
12. Select the *smb.conf* file and click *OK*.



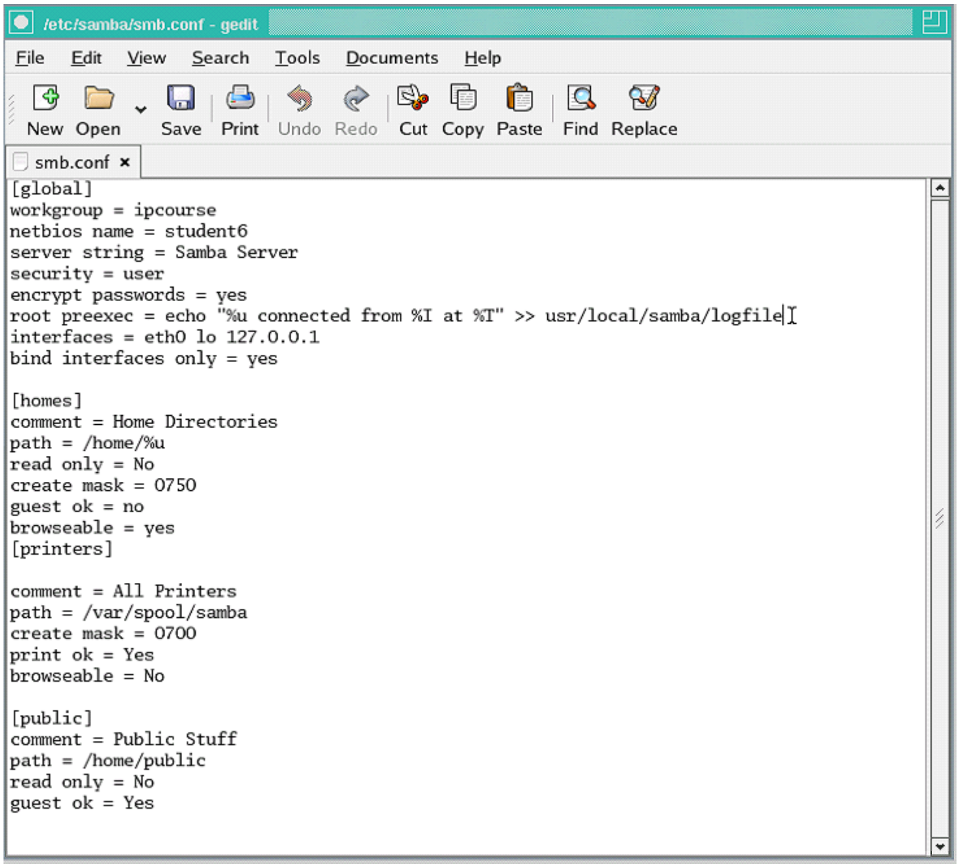
Selection: /etc/samba

smb.conf

13. Add the following code to the smb.conf file:

```
[global]

    workgroup = ipcourse
    netbios name = studentxx (where xx is a number
    assigned by your instructor)
    server string = Samba Server
    security = user
    encrypt passwords = yes
    root preexec = echo “%u connected from %I at %T” >>
    usr/local/samba/logfile
    interfaces = eth0 lo 127.0.0.1
    bind interfaces only = yes

[homes]

    comment = Home Directories
    path = /home/%u
    read only = No
    create mask = 0750
    guest ok = no
    browseable = yes

[printers]

    comment = All Printers
    path = /var/spool/samba
    create mask = 0700
    print ok = Yes
    browseable = No

[public]

    comment = Public Stuff
    path = /home/public
    read only = No
    guest ok = Yes
```

Your file should resemble the following screen shot.



```
[global]
workgroup = ipcourse
netbios name = student6
server string = Samba Server
security = user
encrypt passwords = yes
root preexec = echo "%u connected from %I at %T" >> usr/local/samba/logfile
interfaces = eth0 lo 127.0.0.1
bind interfaces only = yes

[homes]
comment = Home Directories
path = /home/%u
read only = No
create mask = 0750
guest ok = no
browseable = yes
[printers]

comment = All Printers
path = /var/spool/samba
create mask = 0700
print ok = Yes
browseable = No

[public]
comment = Public Stuff
path = /home/public
read only = No
guest ok = Yes
```

14. Save the file and exit the text editor.

15. Test the values entered into smb.conf by entering the `testparm` command from a command shell to test the file. If you entered everything correctly, no error messages will display.

Note

To launch a command shell in Xwindows, right-click the desktop and select *New Terminal*.

---

16. If no errors were reported when executing the testparm command, enter the following command to restart Samba:

    ```
    service smb restart
    ```

17. Create a new local Linux user for testing the Samba service. From a command shell, execute the following command:

    ```
    useradd sambauser
    ```

18. Create a Samba password for the user added in the previous step.

    ```
    smbpasswd –a sambauser
    ```

19. Enter a password of *password* and press *Enter*. Then enter *password* again to confirm. You should receive a message that resembles the following:

    ```
    startsmbfilepwent_internal: file /etc/samba/smbpasswd
    did not exist. File successfully created.
    ```

    You are now ready to test the Samba server from a Windows client.

20. Using a Windows client, verify that you can connect to the Samba server by mapping a network drive to the Samba server’s public folder. From a Windows command prompt, enter the following command:

    ```
    net use z: \\studentxx\sambauser /USER:sambauser
    ```

    A new Z: drive will be available on the Windows client, which will write to the Samba server.

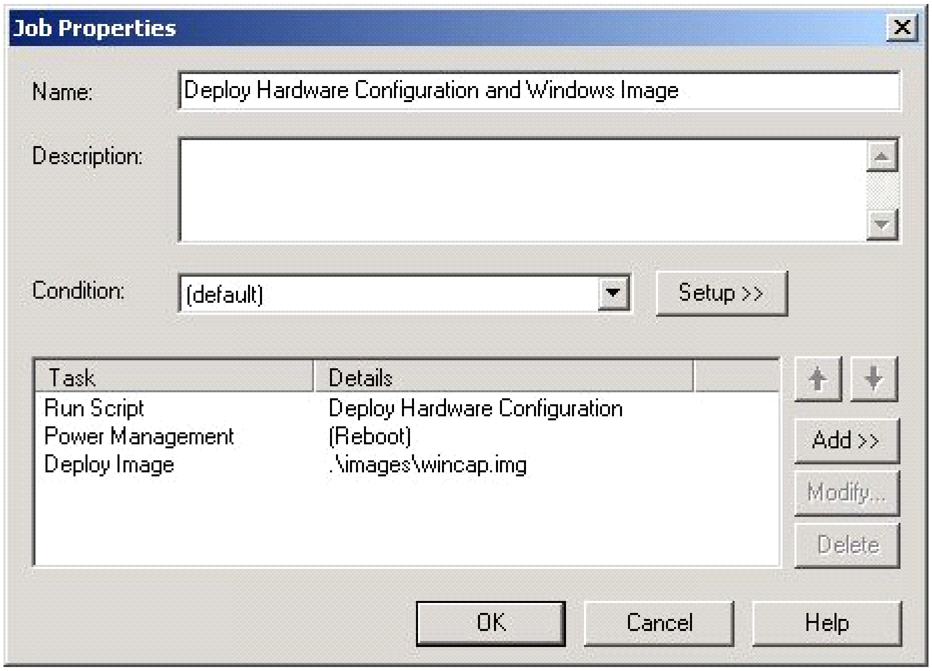
This exercise created a simple file server using Samba. You modified the smb.conf file to set up basic file sharing and created a user account in the Linux passwd file with the useradd file. Then you granted the Linux account access to Samba with the smbpasswd command.

INTERNET For more information about Samba, visit: **http://www.samba.org**

Exercise 5 — Deploying a Windows disk image

To redeploy a Windows disk image, follow these steps:

1. In the Jobs pane of the Deployment Server console, expand the SmartStart Toolkit and OS Imaging Jobs folder and double-click the *Deploy Hardware Configuration and Windows Image* job.
2. In the Job Properties screen, double-click the *Run Script* task. The Run Script screen displays.



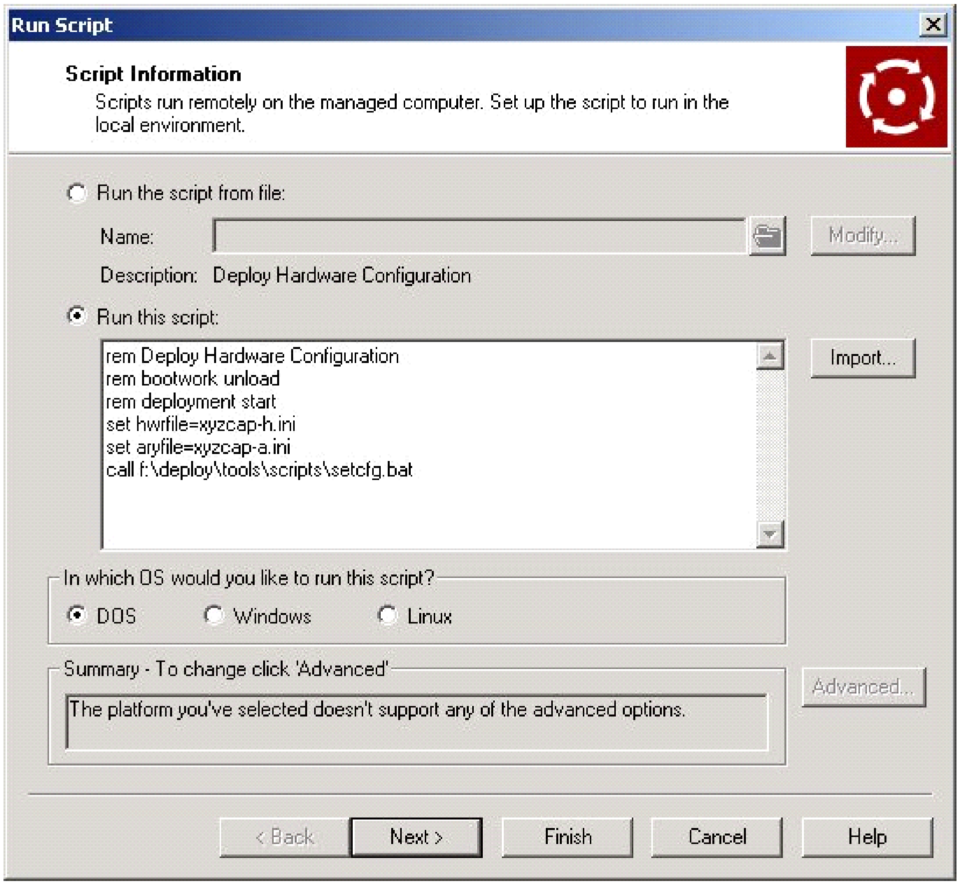
Name: Deploy Hardware Configuration and Windows Image

Description:

Condition: (default)

Task	Details
Run Script	Deploy Hardware Configuration
Power Management	(Reboot)
Deploy Image	.\images\wincap.img

3. In the Run Script screen, change the default names of the hardware information and array information files that will be used in the deployment. These are the files that you captured previously.
   - Change the wincap-h.ini file to *xyzcap-h.ini* (where *xyz* are your initials).
   - Change the wincap-a.ini file to *xyzcap-a.ini* (where *xyz* are your initials).


Run Script
Script Information
Scripts run remotely on the managed computer. Set up the script to run in the local environment.
○ Run the script from file:
Name:
Modify...
Description: Deploy Hardware Configuration
● Run this script:
Import...
In which OS would you like to run this script?
● DOS
○ Windows
○ Linux
Summary - To change click 'Advanced'
Advanced...
< Back
Next >
Finish
Cancel
Help

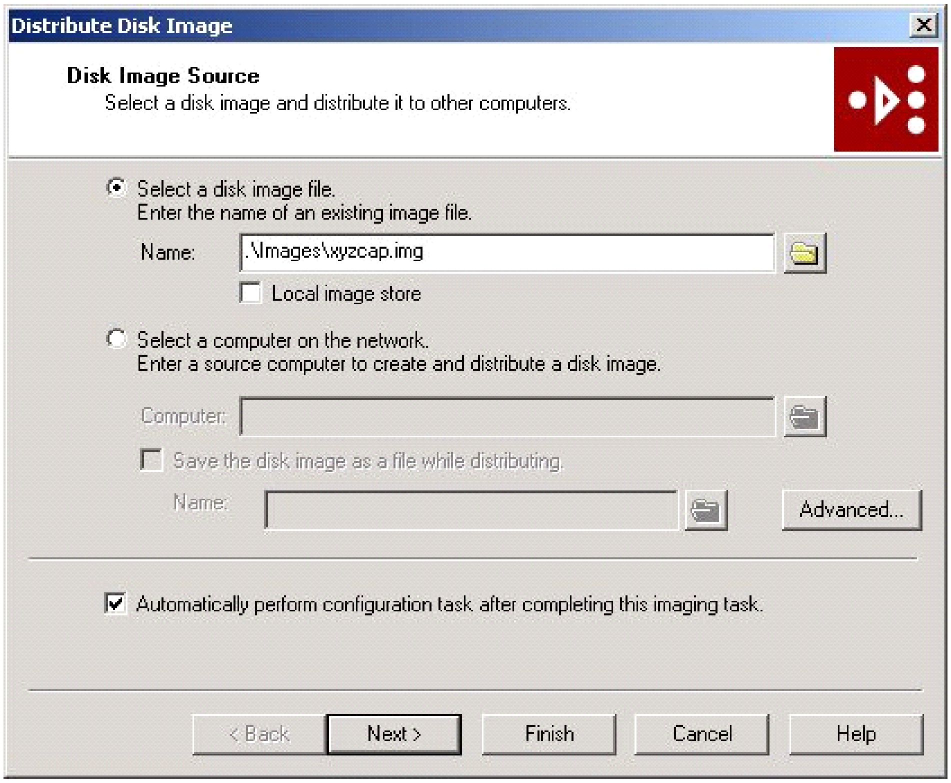
```
rem Deploy Hardware Configuration
rem bootwork unload
rem deployment start
set hwrfile=xyzcap-h.ini
set aryfile=xyzcap-a.ini
call f:\deploy\tools\scripts\setcfg.bat
```

The platform you've selected doesn't support any of the advanced options.

4. Click *Finish* to return to the Job Properties screen.

5. In the Job Properties screen, double-click the *Deploy Image* task to open the Disk Image Source screen.

6. Change the default image name *wincap.img* to *xyzcap.img* (where *xyz* are your initials). Click *Advanced* to see the additional settings available when deploying an image.



Distribute Disk Image

Disk Image Source

Select a disk image and distribute it to other computers.

● Select a disk image file.
Enter the name of an existing image file.

Name: .\Images\xyzcap.img

☐ Local image store

○ Select a computer on the network.
Enter a source computer to create and distribute a disk image.

Computer:

☐ Save the disk image as a file while distributing.

Name:

☑ Automatically perform configuration task after completing this imaging task.

7. Click *OK* → *Finish* to return to the Job Properties screen.

8. Click *OK* to close the Job Properties screen.

9. Erase the configuration on your Linux server before deploying the captured image file by performing these steps.

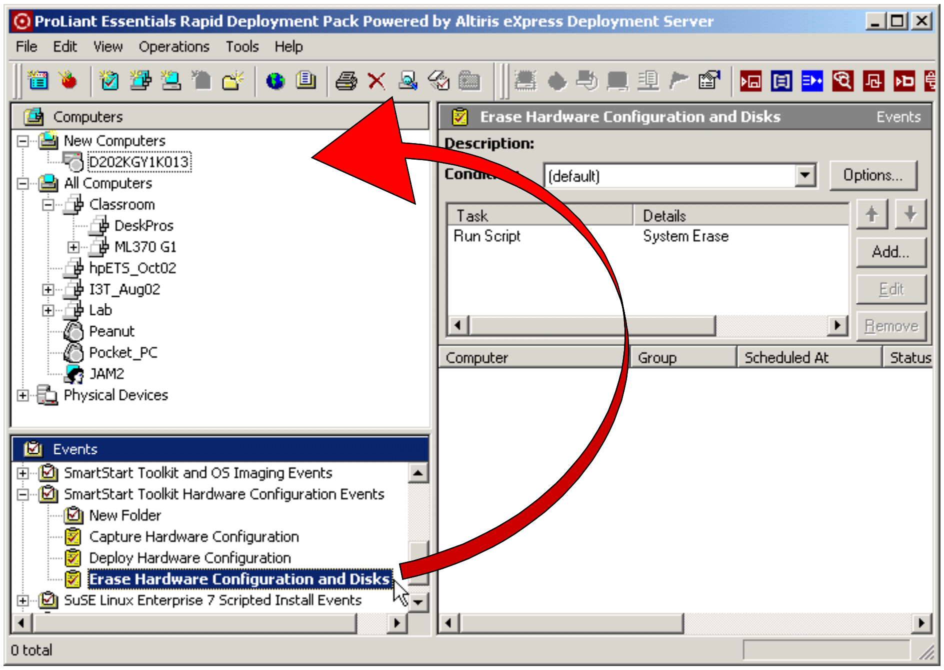
△ **Caution**

This step is data destructive.

---

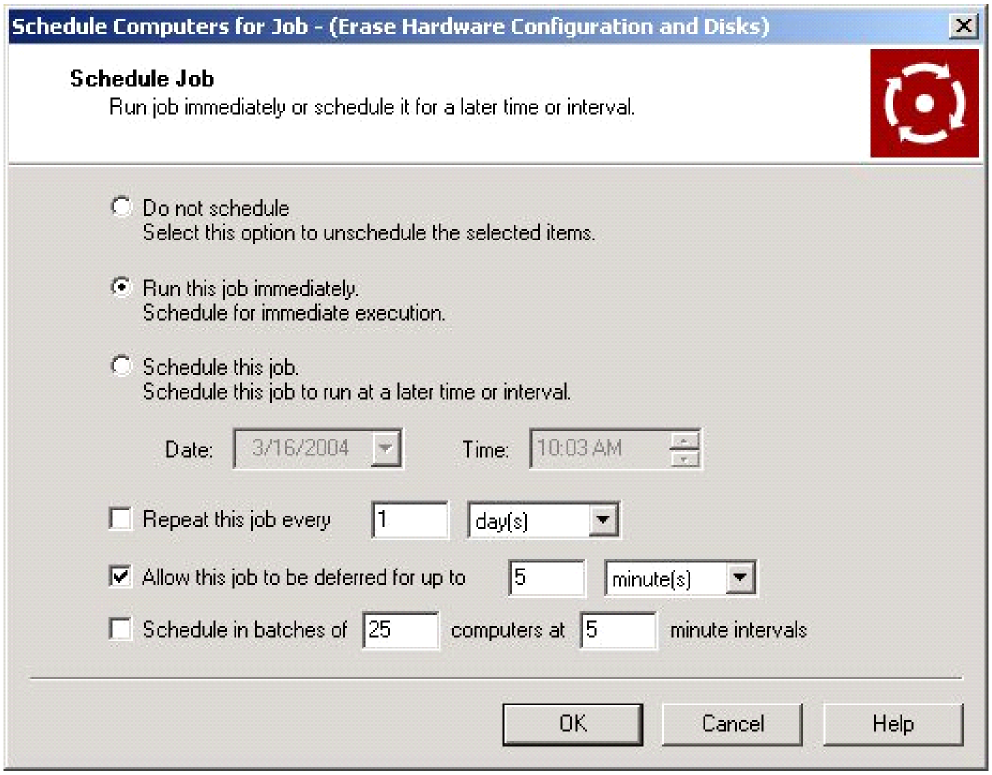
a. In the Deployment Server console, expand the *SmartStart Toolkit Hardware Configuration Jobs* folder.

b. Drag and drop the *Erase Hardware Configuration and Disks* job to the reference server icon in the Computers pane.


ProLiant Essentials Rapid Deployment Pack Powered by Altiris eXpress Deployment Server
File
Edit
View
Operations
Tools
Help
Computers
New Computers
D202KGY1K013
All Computers
Classroom
DeskPros
ML370 G1
hpETS_Oct02
I3T_Aug02
Lab
Peanut
Pocket_PC
JAM2
Physical Devices
Events
SmartStart Toolkit and OS Imaging Events
SmartStart Toolkit Hardware Configuration Events
New Folder
Capture Hardware Configuration
Deploy Hardware Configuration
Erase Hardware Configuration and Disks
SuSE Linux Enterprise 7 Scripted Install Events
0 total
Erase Hardware Configuration and Disks
Events
Description:
Condi
(default)
Options...
Add...
Edit
Remove
Computer
Group
Scheduled At
Status

Task	Details
Run Script	System Erase

10. From the Schedule Computers for Job screen, select *Run this job immediately* and click *OK* to start the job.



Schedule Computers for Job - (Erase Hardware Configuration and Disks)

Schedule Job

Run job immediately or schedule it for a later time or interval.

○ Do not schedule
Select this option to unschedule the selected items.

● Run this job immediately.
Schedule for immediate execution.

○ Schedule this job.
Schedule this job to run at a later time or interval.

Date: 3/16/2004 Time: 10:03 AM

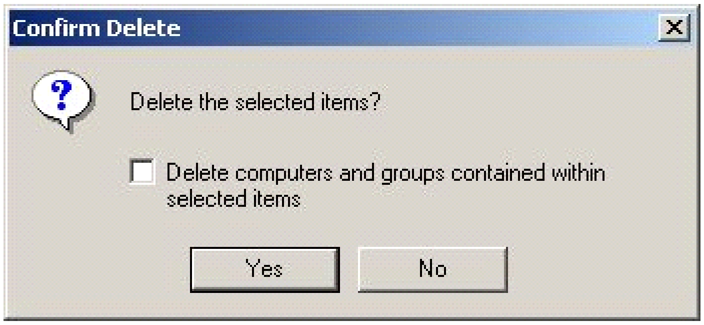
☐ Repeat this job every 1 day(s)

☑ Allow this job to be deferred for up to 5 minute(s)

☐ Schedule in batches of 25 computers at 5 minute intervals

11. After the erase job has run, delete your reference server from the Deployment Server console by right-clicking its icon and selecting *Delete*.

12. Select the *Delete computers and groups contained within the selected items* box and click *Yes*.



Confirm Delete

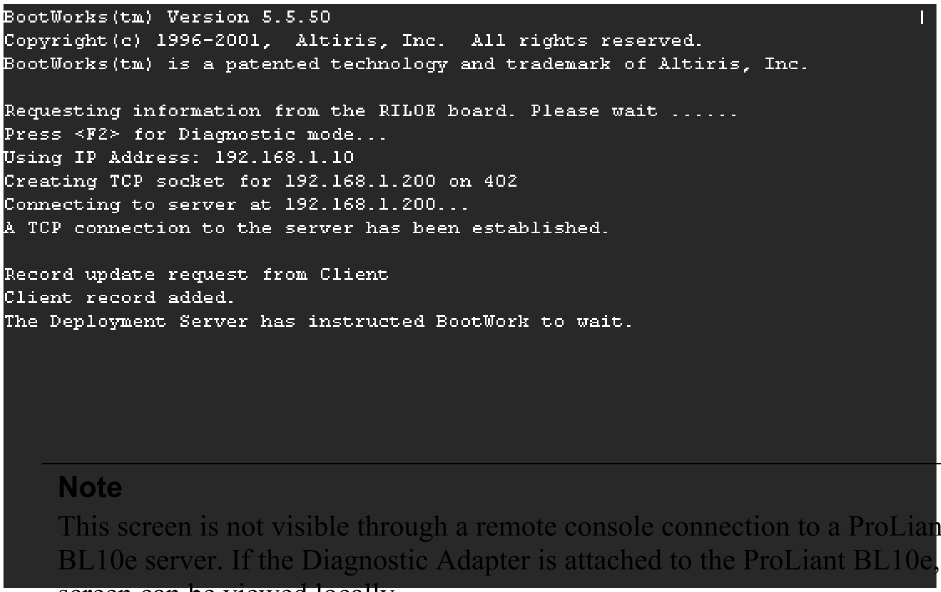
Delete the selected items?

☐ Delete computers and groups contained within selected items

13. If necessary, cycle the power your target server. At the PXE Boot Selection menu, *Altiris BootWorks (Initial Deployment)* should be auto-selected. The Initial Deployment job is run for all new computers that are not registered in the Altiris database. This job will not perform any work, such as imaging the server. It displays the new computer in the Deployment Server console and waits for further instructions.

> **Note**
>
> This screen is not visible through a remote console connection to a ProLiant BL10e server. If the Diagnostic Adapter is attached to the ProLiant BL10e server, you can view the screen locally. The ProLiant BL10e has limited remote console capabilities. After the system loads any operating system, including a DOS-based PXE boot image, the Integrated Administrator Remote Console session is no longer updated.

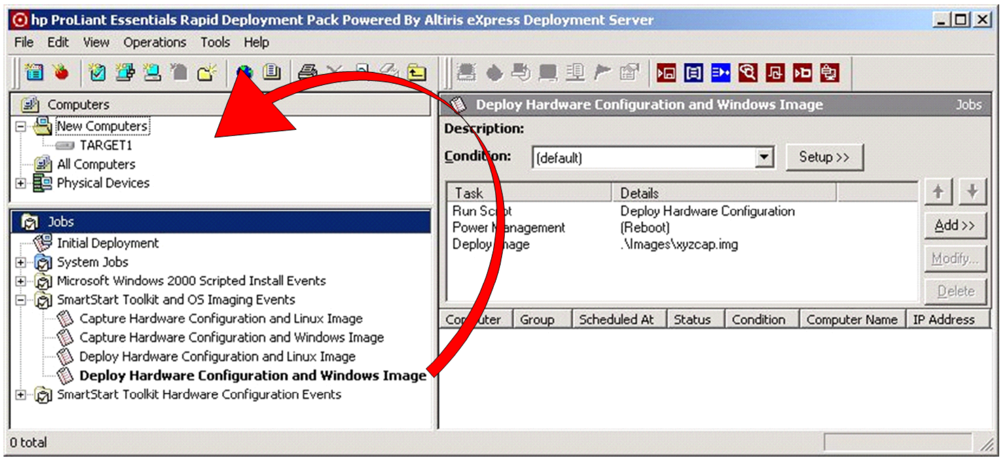
The Initial Deployment job adds the target server to the New Computers group in the Deployment Server console. The target server displays in the Deployment Server console with the Waiting State icon:



```
BootWorks(tm) Version 5.5.50
Copyright(c) 1996-2001,  Altiris, Inc.  All rights reserved.
BootWorks(tm) is a patented technology and trademark of Altiris, Inc.

Requesting information from the RILOE board. Please wait ......
Press <F2> for Diagnostic mode...
Using IP Address: 192.168.1.10
Creating TCP socket for 192.168.1.200 on 402
Connecting to server at 192.168.1.200...
A TCP connection to the server has been established.

Record update request from Client
Client record added.
The Deployment Server has instructed BootWork to wait.
```

> **Note**
>
> This screen is not visible through a remote console connection to a ProLiant BL10e server. If the Diagnostic Adapter is attached to the ProLiant BL10e, the screen can be viewed locally.

14. In the Deployment Server console, drag and drop the modified *Deploy Hardware Configuration and Windows Image* job to the target server icon in the Computers pane.

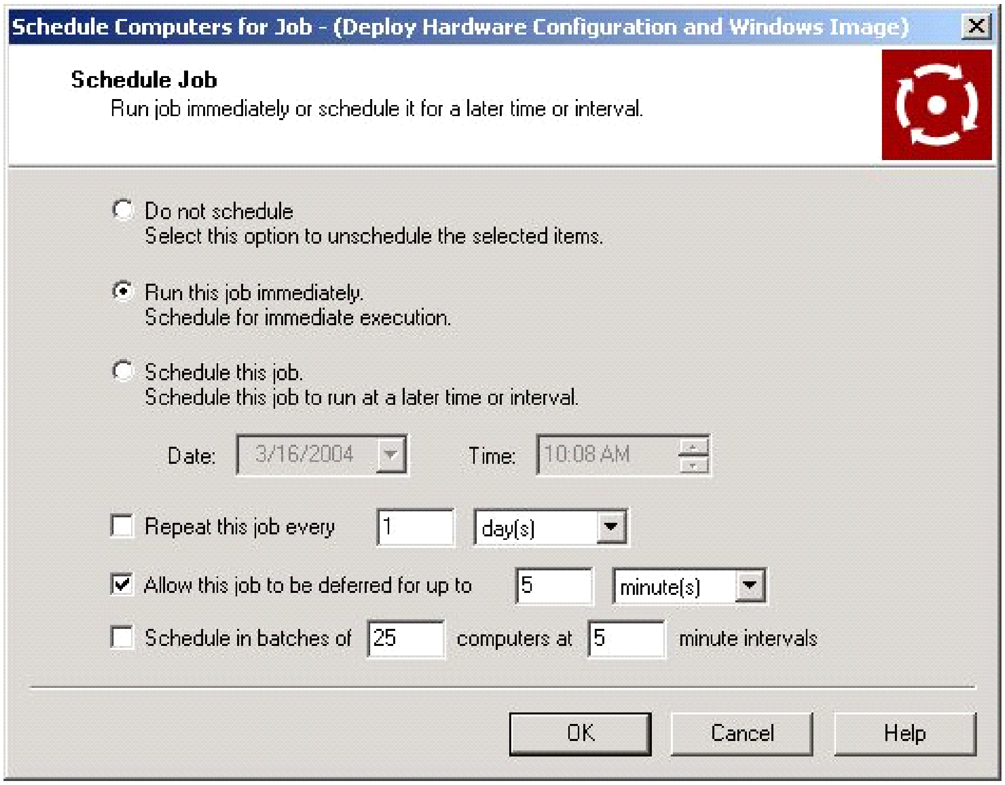

hp ProLiant Essentials Rapid Deployment Pack Powered By Altiris eXpress Deployment Server
File Edit View Operations Tools Help
Computers
New Computers
TARGET1
All Computers
Physical Devices
Jobs
Initial Deployment
System Jobs
Microsoft Windows 2000 Scripted Install Events
SmartStart Toolkit and OS Imaging Events
Capture Hardware Configuration and Linux Image
Capture Hardware Configuration and Windows Image
Deploy Hardware Configuration and Linux Image
Deploy Hardware Configuration and Windows Image
SmartStart Toolkit Hardware Configuration Events
0 total
Deploy Hardware Configuration and Windows Image
Jobs
Setup >>
Add >>
Modify...
Delete
Computer
Group
Scheduled At
Status
Condition
Computer Name
IP Address

Description:

Condition: (default)

Task	Details
Run Script	Deploy Hardware Configuration
Power Management	(Reboot)
Deploy Image	.\Images\xyzcap.img

15. In the Schedule Computers for Job screen, select *Run this job immediately* and click *OK*.


Schedule Computers for Job - (Deploy Hardware Configuration and Windows Image)
Schedule Job
Run job immediately or schedule it for a later time or interval.
OK
Cancel
Help

○ Do not schedule
Select this option to unschedule the selected items.

● Run this job immediately.
Schedule for immediate execution.

○ Schedule this job.
Schedule this job to run at a later time or interval.

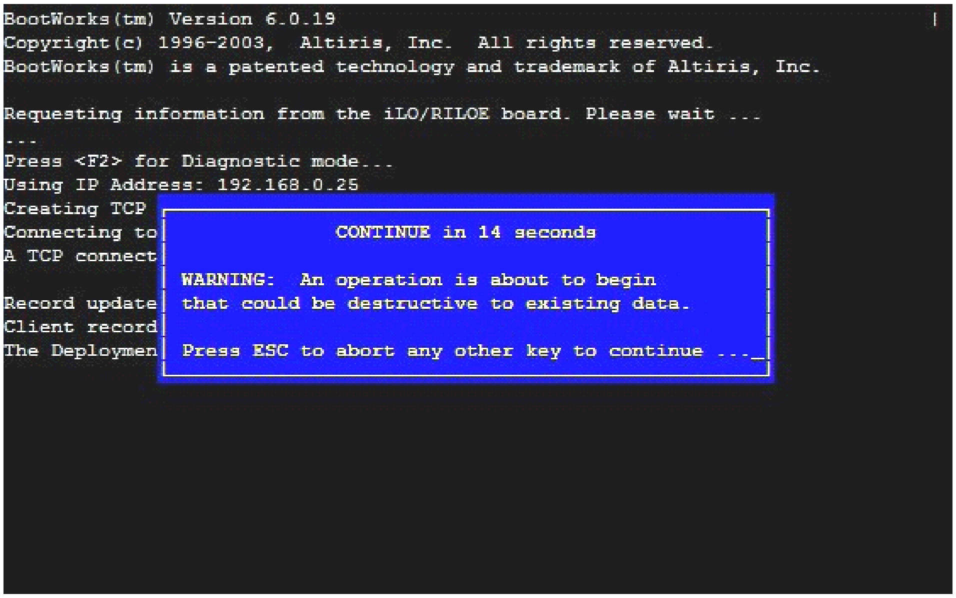
Date: 3/16/2004 Time: 10:08 AM

☐ Repeat this job every 1 day(s)

☑ Allow this job to be deferred for up to 5 minute(s)

☐ Schedule in batches of 25 computers at 5 minute intervals

16. When a warning message displays on the target server, let the timer count down or press any key (**except** *Esc*) to continue with the installation. No further interaction with the target server is required as the image deploys.



```
BootWorks(tm) Version 6.0.19                                                 |
Copyright(c) 1996-2003,  Altiris, Inc.  All rights reserved.
BootWorks(tm) is a patented technology and trademark of Altiris, Inc.

Requesting information from the iLO/RILOE board. Please wait ...
...
Press <F2> for Diagnostic mode...
Using IP Address: 192.168.0.25
Creating TCP ┌────────────────────────────────────────────────────┐
Connecting to│             CONTINUE in 14 seconds                 │
A TCP connect│                                                    │
             │ WARNING:  An operation is about to begin           │
Record update│ that could be destructive to existing data.        │
Client record│                                                    │
The Deploymen│ Press ESC to abort any other key to continue ..._  │
             └────────────────────────────────────────────────────┘
```

Enterprise Management

Lab 2

Objectives

After completing this lab, you should be able to:

- Install HP Systems Insight Manager on a Microsoft Windows server
- Configure the Systems Insight Manager environment
- Monitor managed systems using lists, event handling, and tasks
- Run reports to organize Systems Insight Manager database information
- Deploy software to managed systems

Requirements

To perform this lab, you will need:

- An HP ProLiant server with the following components installed:
  - Microsoft Windows 2000 Server or Advanced Server with Service Pack (SP) 4 or later
  - Microsoft Internet Explorer 6.0 or later
  - TCP/IP and Simple Network Management Protocol (SNMP)
  - Monitor combination capable of supporting 1024 x 768 resolution with 16-bit colors
  - OpenSSH server for managed systems
- HP ProLiant Essentials Foundation Pack
- HP Management CD

Introduction

To enable Jackie to manage the network systems at RC Engineering, you must first install Systems Insight Manager on one of the company’s Windows servers. Then you will need to configure the server to detect and monitor managed systems.

After configuring security on the managed systems and running reports to compare data collection snapshots, you will configure HP ProLiant Support Packs (PSPs) to deploy software to the managed systems. To do this you first must install Version Control Repository Manager (VCRM) on a network server.

Exercise 1 — Installing Systems Insight Manager

To install Systems Insight Manager you must:

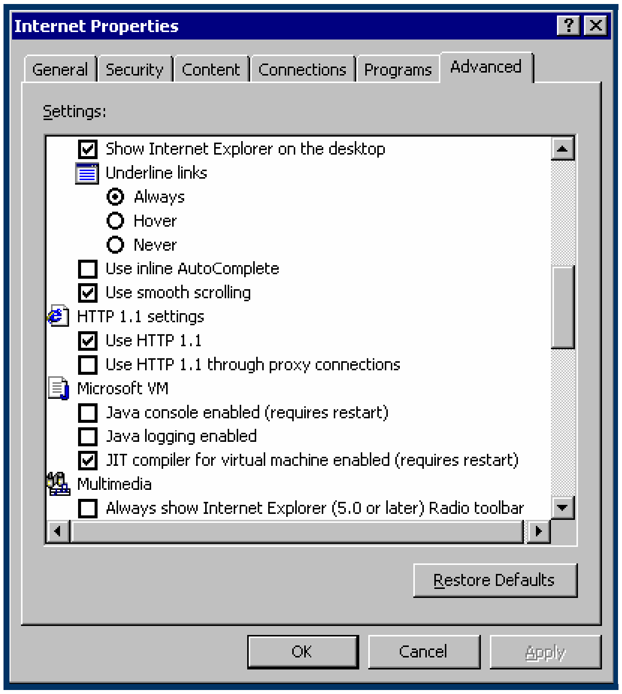
- Verify the hardware and software requirements
- Create users to access Systems Insight Manager from a client

Verify hardware and software requirements

The following table lists the minimum hardware and software requirements to install Systems Insight Manager on a central management server (CMS) and access Systems Insight Manager from a client.

Hardware and software	Minimum requirements
Web browser	■ Intel Pentium III or better ■ Microsoft Internet Explorer 6.0 or later
System memory	■ 512MB RAM for Windows 2000, Windows 2000 Advanced Server, Windows XP Professional, or Windows Server 2003
Monitor resolution	■ 1024 x 768 with 256 colors ■ 16-bit or better recommended

From the Control Panel, double-click the *Internet Options* icon. Then select the *Advanced* tab and verify that *JIT compiler for virtual machine enabled* is selected (usually enabled by default).



☑ Show Internet Explorer on the desktop
Underline links
● Always
○ Hover
○ Never
☐ Use inline AutoComplete
☑ Use smooth scrolling
HTTP 1.1 settings
☑ Use HTTP 1.1
☐ Use HTTP 1.1 through proxy connections
Microsoft VM
☐ Java console enabled (requires restart)
☐ Java logging enabled
☑ JIT compiler for virtual machine enabled (requires restart)
Multimedia
☐ Always show Internet Explorer (5.0 or later) Radio toolbar

Creating users to access Systems Insight Manager from a client

In this exercise you will create a system administrator account, which is required to complete the Systems Insight Manager installation on the CMS. You will also create two additional users to administer the CMS in subsequent exercises.

1. Log in to Windows 2000 as *administrator*.
2. Right-click *My Computer* and select *Manage*.
3. Under System Tools, expand *Local Users and Groups*.
4. Right-click the *Users* folder and select *New User*. In the User Name field, enter *ServerAdmin.* In the Password and Confirm Password boxes, enter *password*. Deselect the *User must change password at next logon* option and click *Create*.
5. On the New User page, click *Close*.
6. Under Local Users and Computers, ensure that *Users* is selected. In the right pane, right-click the *ServerAdmin* user and select *Properties*.
7. From the Properties screen, click the *Member Of* tab and click *Add*.
8. On the Select Groups page, click *Administrators* from the list of groups and click *Add*.
9. Click *OK* and *OK* again.
10. Repeat the process to create KMorgan (Kathy Morgan) and BParker (Brandon Parker) user accounts with a password of *password*. However, these users should not have administrator rights.
11. Close the Computer Management interface.

Installing Systems Insight Manager

In this exercise, you will install Systems Insight Manager on the CMS. Systems Insight Manager can be installed from the HP Management CD or from a self-extracting file that can be downloaded from the HP website.

By default, the installation process installs Microsoft Desktop Engine (MSDE) 2000 and Windows Management Instrumentation (WMI) Mapper if these applications are not present on the server.

Note

Before Systems Insight Manager is installed, the CMS requires:

- A static IP address
- Domain Name Service (DNS) available on the network, with the proper DNS suffix (in this class, *ase.class*) enabled in the IP settings of the server
- All unused network interfaces disabled

In most classrooms, these procedures will have been performed for you as part of the classroom setup.

Initiating a Systems Insight Manager installation from the HP Management CD

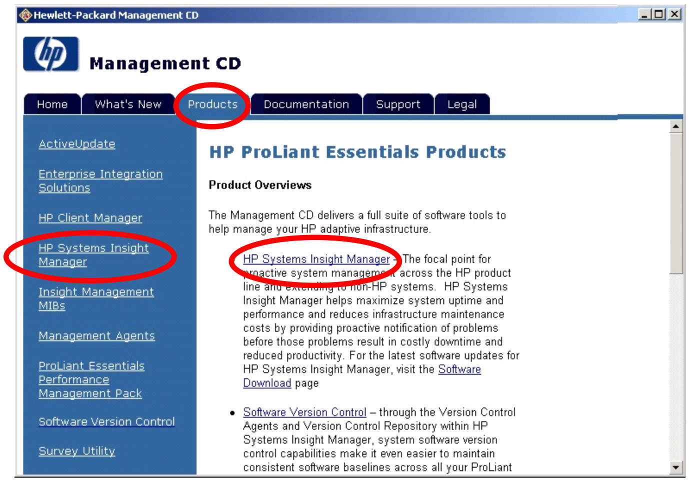
Systems Insight Manager is included on the HP Management CD in the HP ProLiant Essentials Foundation Pack. To install Systems Insight Manager from the HP Management CD:

1. Log in to the CMS as *ServerAdmin*.
2. Insert the HP Management CD into the CD-ROM drive. The Management CD interface should automatically run. If it does not, navigate to the CD-ROM drive and run:

   ```
   autorun.exe
   ```

3. Scroll down the page, review the end user license agreement, and click *Agree*.

4. Click the *Products* tab and then click *HP Systems Insight Manager* on the left panel of the screen or from the Product Overviews list on the right.



HP ProLiant Essentials Products

Product Overviews

The Management CD delivers a full suite of software tools to help manage your HP adaptive infrastructure.

- HP Systems Insight Manager – The focal point for proactive system management across the HP product line and extending to non-HP systems. HP Systems Insight Manager helps maximize system uptime and performance and reduces infrastructure maintenance costs by providing proactive notification of problems before those problems result in costly downtime and reduced productivity. For the latest software updates for HP Systems Insight Manager, visit the Software Download page
- Software Version Control – through the Version Control Agents and Version Control Repository within HP Systems Insight Manager, system software version control capabilities make it even easier to maintain consistent software baselines across all your ProLiant

5. Click *Install*. A list of all software available for installation on the CD displays. Click *Install* next to *HP Systems Insight Manager*.

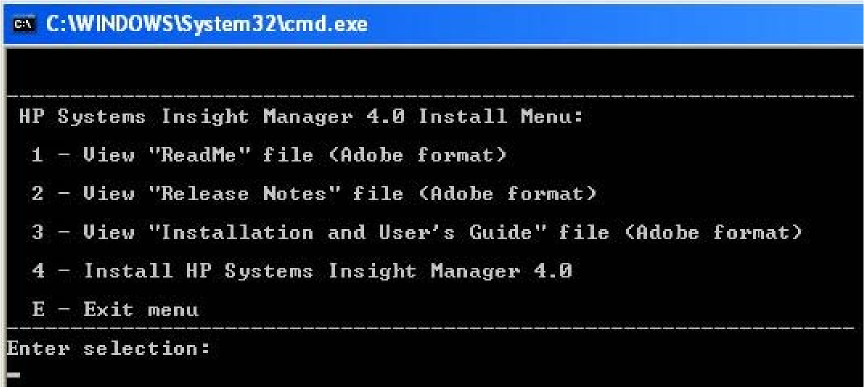
Starting a Systems Insight Manager installation from the self-extracting file

When you download Systems Insight Manager from the Systems Insight Manager website, it is in the form of a self-extracting file. To install it using this file:

1. Run the self-extracting file:

   `HPSIM-setup.exe`

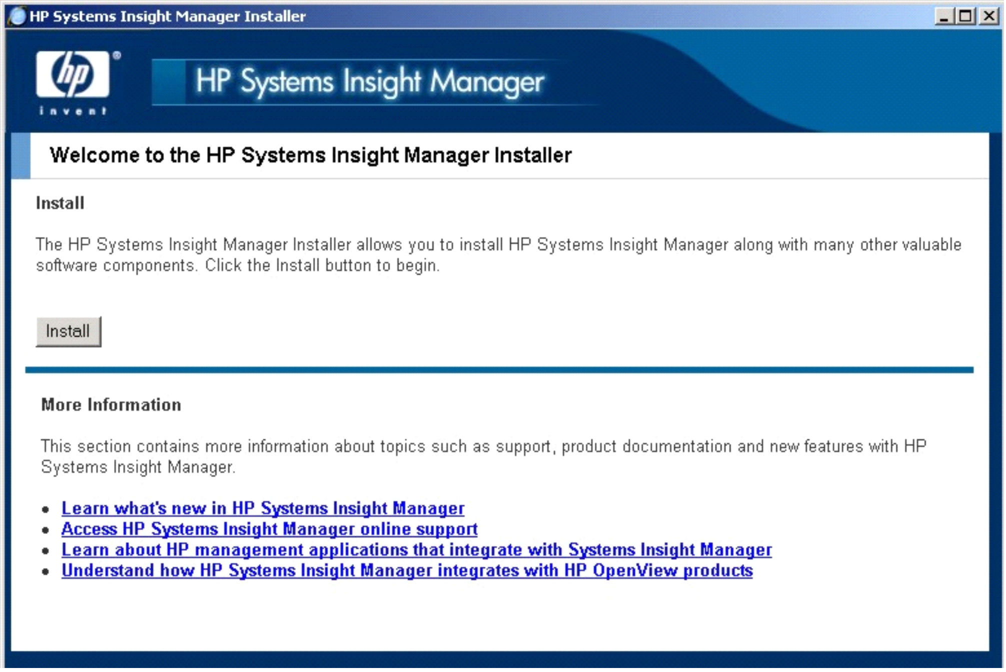
2. Click *OK*.
3. Click *Setup*. The install menu displays from a command line prompt.



```
-------------------------------------------------------------------
 HP Systems Insight Manager 4.0 Install Menu:
  1 - View "ReadMe" file (Adobe format)
  2 - View "Release Notes" file (Adobe format)
  3 - View "Installation and User's Guide" file (Adobe format)
  4 - Install HP Systems Insight Manager 4.0
  E - Exit menu
-------------------------------------------------------------------
Enter selection:
_
```

4. Enter *4* to begin the installation of Systems Insight Manager.

Navigating the Systems Insight Manager installer


HP Systems Insight Manager Installer
invent
HP Systems Insight Manager

Welcome to the HP Systems Insight Manager Installer

Install

The HP Systems Insight Manager Installer allows you to install HP Systems Insight Manager along with many other valuable software components. Click the Install button to begin.

More Information

This section contains more information about topics such as support, product documentation and new features with HP Systems Insight Manager.

- Learn what's new in HP Systems Insight Manager
- Access HP Systems Insight Manager online support
- Learn about HP management applications that integrate with Systems Insight Manager
- Understand how HP Systems Insight Manager integrates with HP OpenView products

The welcome screen of the Systems Insight Manager installer provides links to valuable information. Before installing Systems Insight Manager, you can learn more about the program and how it integrates with other management applications such as HP OpenView.

To continue the installation of Systems Insight Manager, click *Install* on the HP Systems Insight Manager Installer screen.

Installing MSDE 2000

1. If Microsoft SQL Server is not detected locally, you are prompted to install MSDE 2000 SP3A. Click *Install MSDE*.
2. When you are prompted to restart, select *Reboot the system*.
3. After the server restarts, log in as *ServerAdmin*.

Note

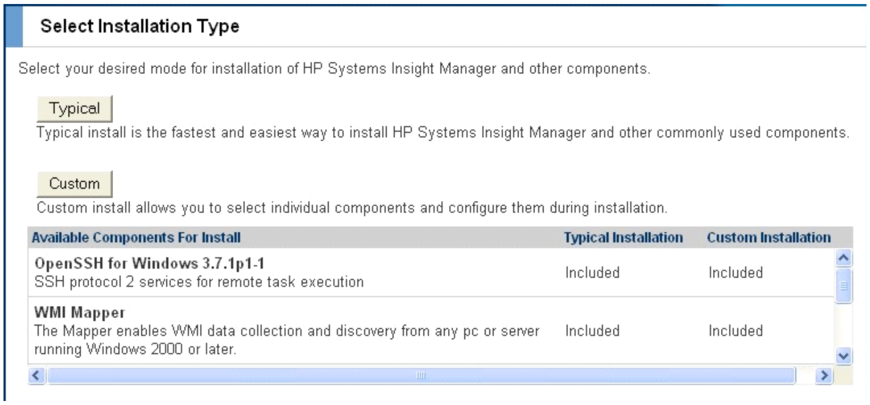
MSDE can be installed as the Administrator user, but for the purposes of this lab, you are installing as *ServerAdmin*. If you install MSDE as *Administrator*, some steps in this lab might not match your experience.

---

4. If you are installing Systems Insight Manager from the HP Management CD, from the CD-ROM drive run:

   `\HPSIM\win\eng\inshell.exe`

   Otherwise repeat the steps in the section titled *Starting a Systems Insight Manager installation from the self-extracting file*.
5. On the Welcome to the Systems Insight Manager Installer screen, click *Install*.



Select Installation Type

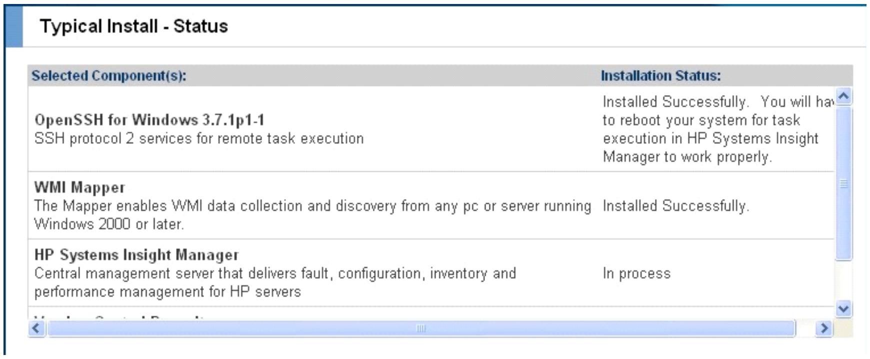
Select your desired mode for installation of HP Systems Insight Manager and other components.

Typical install is the fastest and easiest way to install HP Systems Insight Manager and other commonly used components.

Custom install allows you to select individual components and configure them during installation.

Available Components For Install	Typical Installation	Custom Installation
OpenSSH for Windows 3.7.1p1-1 SSH protocol 2 services for remote task execution	Included	Included
WMI Mapper The Mapper enables WMI data collection and discovery from any pc or server running Windows 2000 or later.	Included	Included

6. There are two Systems Insight Manager installation options—*Typical* and *Custom*. Both options install OpenSSH for Windows, WMI Mapper, Systems Insight Manager, and Version Control Repository Manager (VCRM). The Custom option enables you to change the settings for the drive, installation directory, or program group. For this exercise, click *Typical*.
7. On the Account Authentication screen, enter the password for the ServerAdmin account and your machine name in the database server field (if you do not know your machine name, consult your instructor). Click *Next*.
8. On the Summary screen, click *Install*. The Status page displays when the selected components install.



Typical Install - Status

Selected Component(s):	Installation Status:
OpenSSH for Windows 3.7.1p1-1 SSH protocol 2 services for remote task execution	Installed Successfully. You will ha to reboot your system for task execution in HP Systems Insight Manager to work properly.
WMI Mapper The Mapper enables WMI data collection and discovery from any pc or server running Windows 2000 or later.	Installed Successfully.
HP Systems Insight Manager Central management server that delivers fault, configuration, inventory and performance management for HP servers	In process

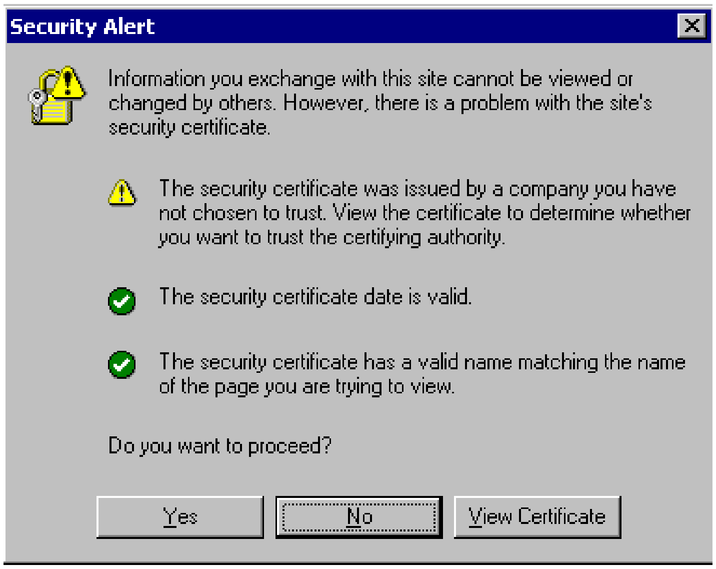
9. When the installation is complete, click *Finished*.

Installing the Java Runtime Environment on the client

You need the Java Runtime Environment (JRE) to access the Systems Insight Manager browser interface from a client. To install the JRE:

1. Log in to the client as *ServerAdmin*.
2. Open Internet Explorer and enter *HTTP://MachineName:280* in the Address bar. Then click *GO* or press *Enter*.
3. A Security Alert message displays indicating that you are about to view pages over a secure connection. Click *OK*.

4. Another Security Alert dialog box displays because the system does not trust the issuer of the certificate. Certificates are used for authentication and security within Systems Insight Manager. To configure a trust of the certificate issuer and prevent this Security Alert dialog box from displaying again, click the *View Certificate* button.



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

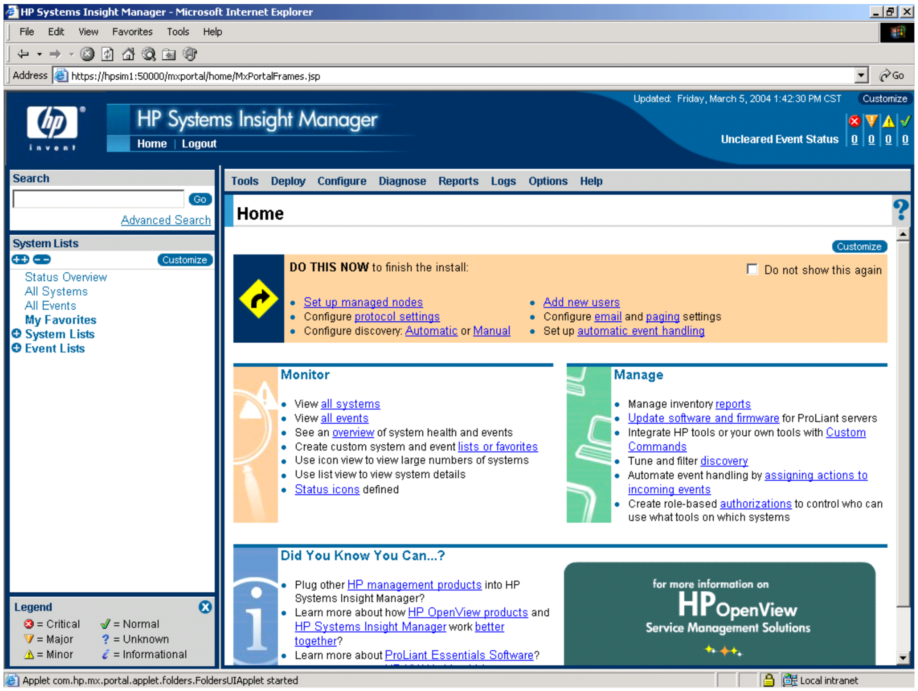
The security certificate date is valid.

The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

5. Click the *General* tab and then click *Install Certificate.*
6. The Welcome to the Certificate Import Wizard dialog box displays. Click *Next.*
7. Ensure that *Automatically select the certificate store based on the type of certificate* is selected and click *Next* → *Finish*.
8. Review the certificate information and click *Yes* on the Root Certificate Store dialog box.
9. When the import is successful, click *OK* → *OK* → *Yes*.
10. The page displays to install the Java 2 Runtime Environment from Sun Microsystems Inc. Click *Install JRE* and then click *Open* to run the application.
11. Click *Yes* to accept the license agreement.
12. Click *Typical* for the setup type and then click *Next*.
13. When the JRE installation completes, click *Refresh Login*.

14. A Warning – Security dialog box displays requesting the acceptance of the certificate associated with the Systems Insight Manager server. Click *Always*.
15. A *Hostname Mismatch* dialog box displays. Click *Yes* to proceed. When the dialog box displays again, click *Always*.
16. Log in to Systems Insight Manager using the ServerAdmin account and password. The Systems Insight Manager Home page displays.



Legend

- ✕ = Critical
- ✓ = Normal
- ▼ = Major
- ? = Unknown
- ⚠ = Minor
- ℹ = Informational

Home

DO THIS NOW to finish the install:

☐ Do not show this again

- Set up managed nodes
- Configure protocol settings
- Configure discovery: Automatic or Manual
- Add new users
- Configure email and paging settings
- Set up automatic event handling

Monitor

- View all systems
- View all events
- See an overview of system health and events
- Create custom system and event lists or favorites
- Use icon view to view large numbers of systems
- Use list view to view system details
- Status icons defined

Manage

- Manage inventory reports
- Update software and firmware for ProLiant servers
- Integrate HP tools or your own tools with Custom Commands
- Tune and filter discovery
- Automate event handling by assigning actions to incoming events
- Create role-based authorizations to control who can use what tools on which systems

Did You Know You Can...?

- Plug other HP management products into HP Systems Insight Manager?
- Learn more about how HP OpenView products and HP Systems Insight Manager work better together?
- Learn more about ProLiant Essentials Software?

Navigating the Systems Insight Manager Home page

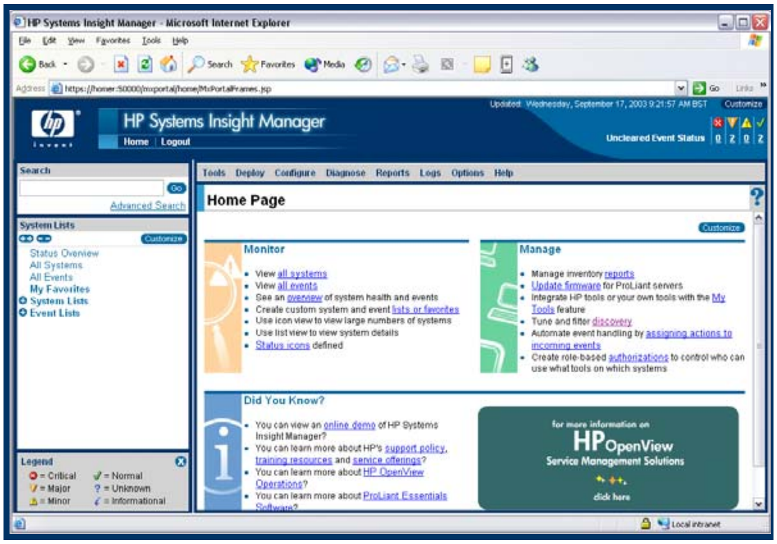
To familiarize yourself with Systems Insight Manager and set it up for your environment, experiment with each of the links on the Systems Insight Manager Home page.

1. If necessary, log in to the management console as *ServerAdmin*.

> **Note**
>
> Logging in as an administrator is not a requirement. For the purpose of this lab, you are running the browser on the Systems Insight Manager server and logging in as an existing user, *ServerAdmin*.

2. Open Internet Explorer and enter *HTTP://MachineName:280* in the Address bar. Then click *GO* or press *Enter*.
3. If a Security Alert message displays alerting you that you are about to view pages over a secure connection, click *OK*.
4. Log in to Systems Insight Manager using *ServerAdmin* and the password. The Systems Insight Manager Home page displays.

> **Note**
>
> If you have not done so already, select the *Do not show this again* check box in the box labeled *DO THIS NOW to finish the install*.


HP Systems Insight Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://homer:50000/mxportal/home/MxPortalFrames.jsp
Go Links
HP Systems Insight Manager
Home Logout
Updated: Wednesday, September 17, 2003 9:21:57 AM BST
Customize
Uncleared Event Status
0 2 0 2
Search
Go
Advanced Search
System Lists
Customize
Status Overview
All Systems
All Events
My Favorites
System Lists
Event Lists
Legend
= Critical
= Major
= Minor
= Normal
= Unknown
= Informational
Tools Deploy Configure Diagnose Reports Logs Options Help
Home Page
Customize
for more information on
HP OpenView
Service Management Solutions
click here
Local intranet

Monitor

- View all systems
- View all events
- See an overview of system health and events
- Create custom system and event lists or favorites
- Use icon view to view large numbers of systems
- Use list view to view system details
- Status icons defined

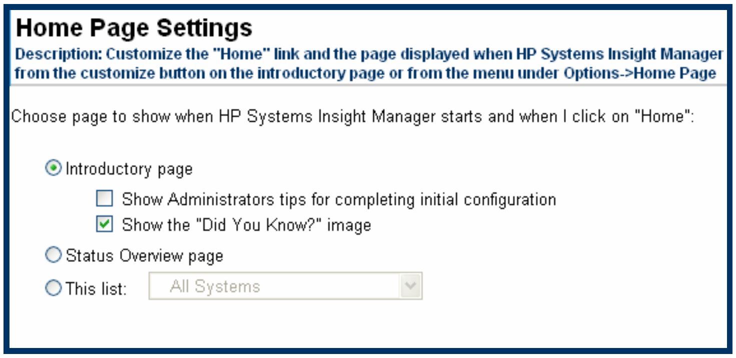
Manage

- Manage inventory reports
- Update firmware for ProLiant servers
- Integrate HP tools or your own tools with the My Tools feature
- Tune and filter discovery
- Automate event handling by assigning actions to incoming events
- Create role-based authorizations to control who can use what tools on which systems

Did You Know?

- You can view an online demo of HP Systems Insight Manager?
- You can learn more about HP's support policy, training resources and service offerings?
- You can learn more about HP OpenView Operations?
- You can learn more about ProLiant Essentials Software?

5. You can configure the Systems Insight Manager Home page by clicking one of the Customize links that are in the top right corner of each frame on the page. From the Home page, click the *Customize* link in the top right corner of the main frame or select *Options* → *Home Page Settings*.



Home Page Settings

Description: Customize the "Home" link and the page displayed when HP Systems Insight Manager from the customize button on the introductory page or from the menu under Options->Home Page

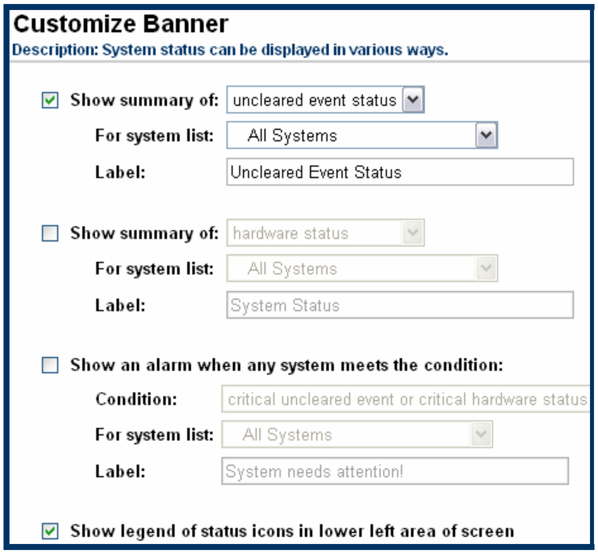
Choose page to show when HP Systems Insight Manager starts and when I click on "Home":

● Introductory page
  ☐ Show Administrators tips for completing initial configuration
  ☑ Show the "Did You Know?" image
○ Status Overview page
○ This list: All Systems

6. The Home Page Settings screen displays. Select the *This list* radio button and *All Servers* in the list box. Click *OK*. The Home page displays the *All Servers* list.

7. To reconfigure the Home page, select *Options* → *Home Page*.

8. Click *Customize* in the top right corner of the screen adjacent to the Uncleared Event Status information.



Customize Banner

Description: System status can be displayed in various ways.

☑ **Show summary of:** uncleared event status
  For system list: All Systems
  Label: Uncleared Event Status

☐ **Show summary of:** hardware status
  For system list: All Systems
  Label: System Status

☐ **Show an alarm when any system meets the condition:**
  Condition: critical uncleared event or critical hardware status
  For system list: All Systems
  Label: System needs attention!

☑ **Show legend of status icons in lower left area of screen**

9. Notice that you can change the way Systems Insight Manager displays this status information. Experiment with the various ways the status information can be displayed. Then return to the Home page.

Exercise 2 — Configuring the Systems Insight Manager environment

To execute commands and deploy software to managed systems, two tasks must be performed:

- Install and configure SSH
- Configure each managed system to send SNMP traps

Installing and configuring SSH

A public SSH key must be installed on each managed system to enable Systems Insight Manager by means of the Distributed Task Facility (DTF) to execute commands on that system. The private key is stored on the CMS.

Run the OpenSSH application on the managed system

1. Insert the HP Management CD into the CD-ROM drive on the managed system. Navigate to the openssh folder and execute the following command:

   ```
   OpenSSH_3.7.1p11.exe
   ```

   Accept all the default prompts.

2. Open a command prompt, navigate to the C:\Program Files\OpenSSH\etc directory, and enter:

   ```
   cd C:\Program Files\OpenSSH\etc
   ```

   This command assumes that OpenSSH was installed in the default location.

3. Execute the following command to see which users are registered with OpenSSH:

   ```
   type passwd
   ```

4. Restart the server.

Copy the SSH key from the CMS

1. On the CMS, copy the SSH generated public key from the CMS to the managed system and place it in the authorized keys file of the root or administrator user. To launch the Manage SSH Keys dialog box from the CMS command prompt, enter the following command:

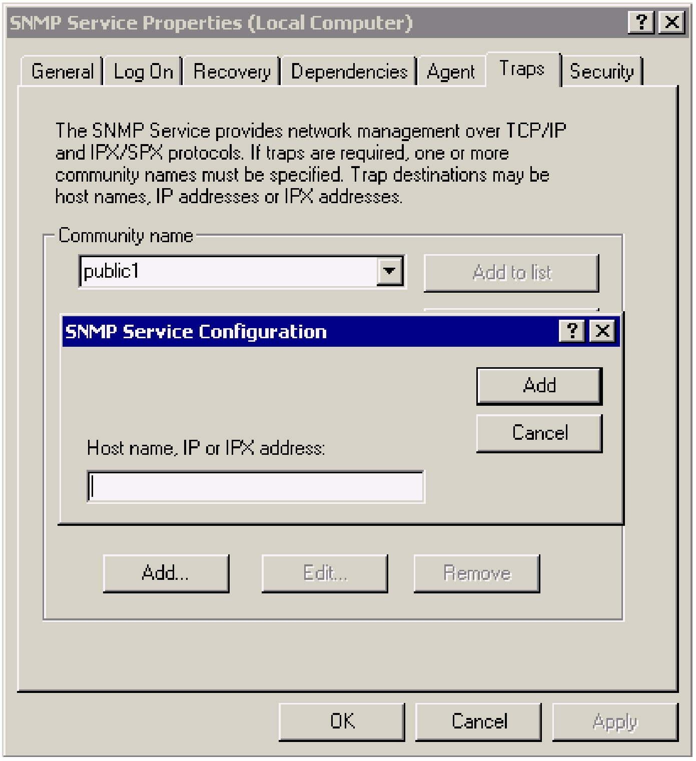
   ```
   mxagentconfig -g
   ```

2. In the dialog box, enter the hostname of the managed system. Then enter *root* or *administrator* for the username and the associated password. Click *Connect*.
3. Click *Close.*
4. Close the command shell.

Configuring a managed system to send SNMP traps

Perform the following steps on each managed system:

1. Select *Start* → *Programs* → *Administrative Tools* → *Services*. On Windows 2003 and Windows XP, the Programs submenu is *All Programs*.
2. Scroll down the list and right-click *SNMP Service*. Then select *Properties*.
3. On the Security tab, click *Add*.
4. Select *READ WRITE* from the Community rights drop-down list.
5. Enter *publicn* for the Community Name, where *n* reflects the table in the classroom where your server is located.
6. Click *Add*.
7. Select the *Traps* tab, enter the Community Name from step 5, and click *Add to List*.
8. Click *Add* in the Trap Destination section.



The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses or IPX addresses.

Community name: public1

Host name, IP or IPX address:

9. Enter the IP address of the CMS and click *Add*.
10. Click *Apply* to save the changes and *OK* to close the dialog box.

Configuring protocol settings for managed systems

Configuring the protocol settings determines which systems are added to Systems Insight Manager. In this exercise, you will set global protocols to configure default system-wide protocol settings. These defaults apply to all newly discovered systems.

1. If you have logged out, log back in to Systems Insight Manager.
2. Select *Options* → *Protocol Settings* → *Global Protocol Settings*.
3. If some systems are managed over a WAN or satellite link, use a larger default ping (Internet Control Message Protocol [ICMP]) setting timeout (for example, five seconds) with at least one retry. For a LAN such as a classroom network, use a shorter timeout of three seconds and one retry.
4. Select *Enable WBEM*.
5. In the Default WBEM settings section, enter the default user names and passwords shown in the following table.

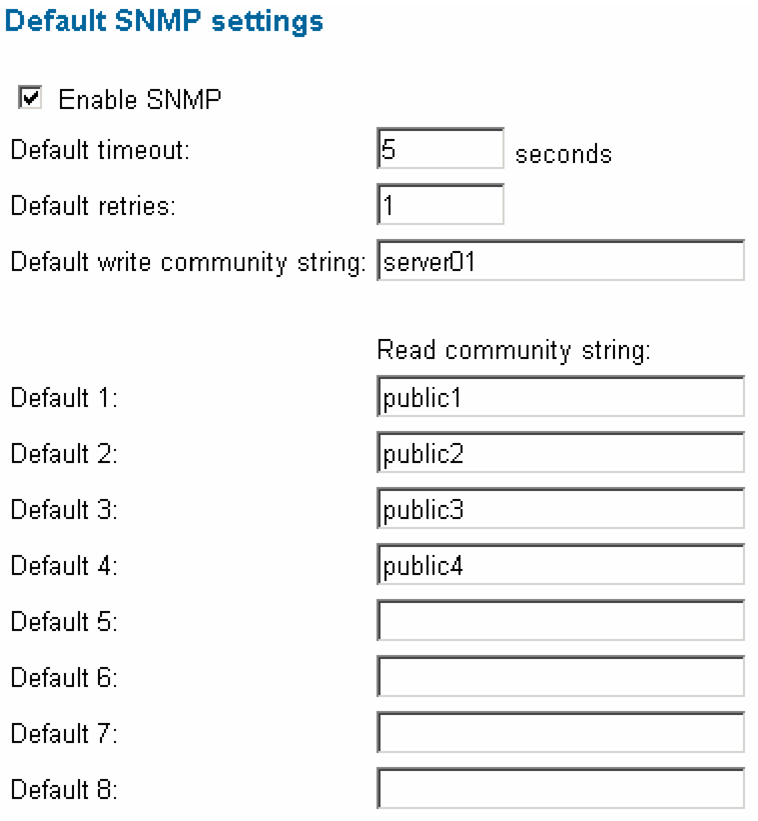
Username	Password
Administrator	password
ServerAdmin	password
KMorgan	password

The identification process attempts each of these user name and password pairs until a successful response is obtained. Future Web-Based Enterprise Management (WBEM) requests to that system use the user name and password that succeeded.

Note
For Windows-based systems, the user name should include the domain name, for example, domainname\username.

6. In the Default HTTP settings section, select *Enable HTTP and HTTPS* to enable web-based agents and other HTTP port scans to be identified.

7. In the Default SNMP settings section, select *Enable SNMP* and set the Default timeout to *3* and Default retries to *1*. The same consideration applies for this setting as the Default ping (ICMP) setting.



Default SNMP settings

☑ Enable SNMP

Default timeout:	5 seconds
Default retries:	1
Default write community string:	server01
	Read community string:
Default 1:	public1
Default 2:	public2
Default 3:	public3
Default 4:	public4
Default 5:	
Default 6:	
Default 7:	
Default 8:	

Enter the name of the CMS as the Default write community string.

The community string is set to *public* by default. HP recommends that the community string be changed to prevent unauthorized users from viewing system information. Enter *publicn* as the Default 1 read community string, where *n* represents the table location in the classroom. Enter read community strings for other student servers in the class.

8. In the Default DMI settings section, select *Enable DMI* to enable DMI identification to run on systems.

9. Click *OK* to accept the settings.

Running the first device discovery

Before running the first discovery of systems on the network, you must:

- Ensure that HP Insight Management Agents are installed and running correctly on the target systems
- Verify that the SNMP community strings settings and WBEM user name and passwords in Systems Insight Manager and on the system agents are configured correctly

Verifying installation of HP Insight Management Agents

The HP Insight Management Agents enable you to view subsystem and status information from a web browser, either locally or remotely.

1. To view information on a managed system locally, enter either URL:

   ```
   https://127.0.0.1:2381/
   https://localhost:2381/
   ```

2. To view information on a managed system from the CMS (remotely), enter the URL:

   ```
   https://machine:2381/
   ```

   where *machine* is the IP address or the computer name under DNS.

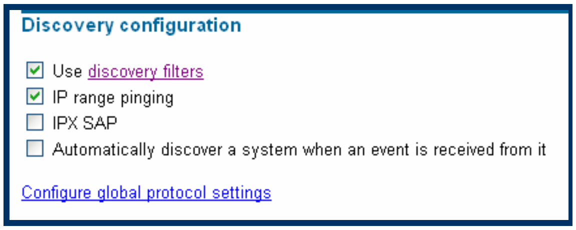
   > **Note**
   > If the managed system is not set up to trust the CMS, a Security Alert dialog box displays prompting you to indicate whether or not to trust the server. This dialog box is followed by a login page.

3. The System Management Home Page should display. If it does not, you must install the agents from a SmartStart or Management CD. Consult your instructor if you need help obtaining these CDs. Close the browser after the presence of the HP Insight Management Agents is confirmed.

Initiating automatic discovery

In this exercise, you will run the first device discovery to discover the systems in your student set.

1. From the Systems Insight Manager Home page, select *Options* → *Discovery* → *Automatic Discovery*.
2. When the Automatic Discovery – General Settings page displays, ensure that IP range pinging is selected.

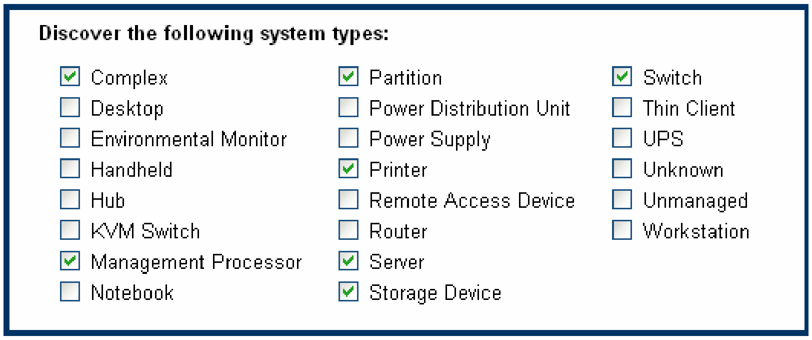


Discovery configuration

☑ Use discovery filters
☑ IP range pinging
☐ IPX SAP
☐ Automatically discover a system when an event is received from it

Configure global protocol settings

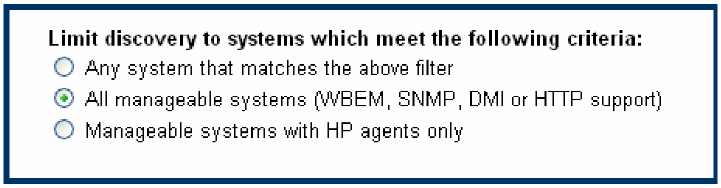
3. Click the *discovery filters* link. Filters are enabled for new installations and are set to the system types shown in the graphic.



Discover the following system types:

☑ Complex
☐ Desktop
☐ Environmental Monitor
☐ Handheld
☐ Hub
☐ KVM Switch
☑ Management Processor
☐ Notebook
☑ Partition
☐ Power Distribution Unit
☐ Power Supply
☑ Printer
☐ Remote Access Device
☐ Router
☑ Server
☑ Storage Device
☑ Switch
☐ Thin Client
☐ UPS
☐ Unknown
☐ Unmanaged
☐ Workstation

4. Notice that you can limit the scope of discovery using certain criteria. Select *All manageable systems (WBEM, SNMP, DMI or HTTP support)* and click *OK*.



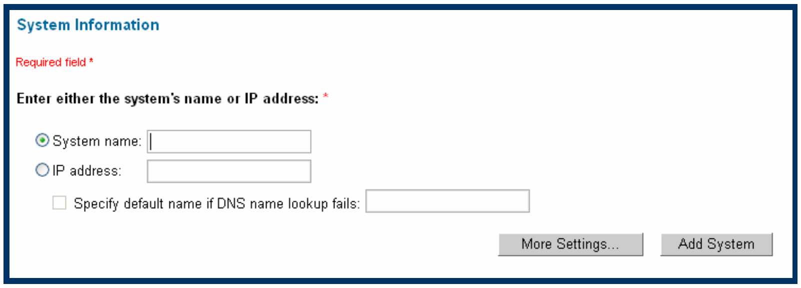
Limit discovery to systems which meet the following criteria:
○ Any system that matches the above filter
● All manageable systems (WBEM, SNMP, DMI or HTTP support)
○ Manageable systems with HP agents only

5. Click *Home* to return to the Systems Insight Manager Home page.
6. Select *Options* → *Discovery* → *Automatic Discovery*.
7. Notice that discovery is scheduled to execute automatically every day.
8. Scroll down the page and click *Save and Run*.
9. Under *Status*, notice the *Last Run: Running* percentage. When this reaches 100%, the time of the last discovery process is displayed. When complete, click *Save*.
10. In the left-hand pane, click the *All Systems* link. The All Systems page displays the discovered devices for your classroom.
11. Click *Home* to return to the Systems Insight Manager Home page.

Performing a manual discovery

In this exercise, you will perform a manual device discovery. This exercise enables you view the options for adding devices.

1. Select *Options* → *Discovery* → *Manual Discovery*. The IP address or name of the device is required to discover a device in Systems Insight Manager.



System Information

Required field *

Enter either the system's name or IP address: *

● System name:

○ IP address:

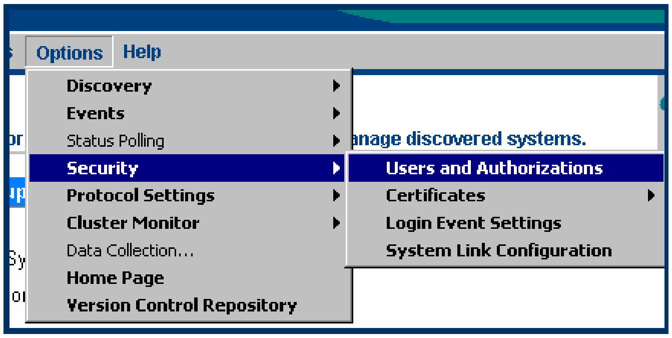
☐ Specify default name if DNS name lookup fails:

2. Click *More Settings* and review the additional information that can be provided.
3. Return to the Systems Insight Manager Home page.

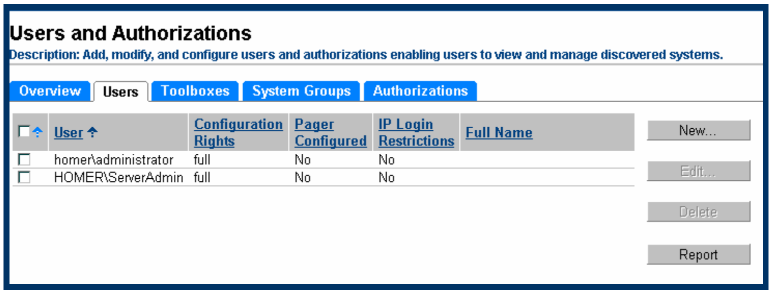
Creating users

In this exercise, you will configure a limited Systems Insight Manager administrator.

1. From the Systems Insight Manager Home page, select *Options* → *Security* → *Users and Authorizations*.



2. The *Users and Authorizations* page opens. Click the *Users* tab.
3. Click *New*.


Users and Authorizations

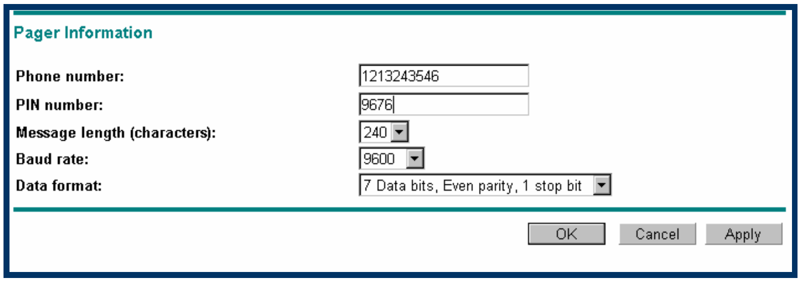
Description: Add, modify, and configure users and authorizations enabling users to view and manage discovered systems.

☐	User	Configuration Rights	Pager Configured	IP Login Restrictions	Full Name
☐	homer\administrator	full	No	No	
☐	HOMER\ServerAdmin	full	No	No	

4. The *Users and Authorizations* page expands to enable you to enter details for a new user. Enter the information shown in the following table.

Field	Information
Login name	KMorgan
Domain	<the name of the CMS system>
Full name	Kathy Morgan
Phone	222-555-1234
Email address	kmorgan@hp.com
Copy all authorizations of this user or [template]	None
Central management server configuration rights	limited, allowed to create tools, edit events, create reports, and so forth

5. Scroll down the page and fill in the pager information. Click *OK*. Kathy Morgan is now in the list of users.



Pager Information

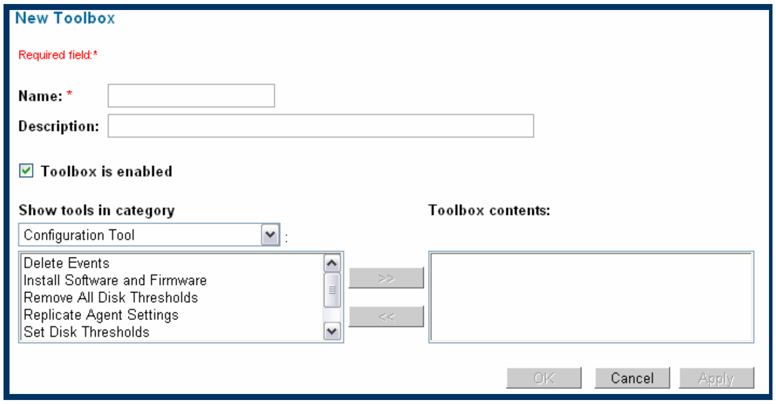
Phone number: 1213243546
PIN number: 9676
Message length (characters): 240
Baud rate: 9600
Data format: 7 Data bits, Even parity, 1 stop bit

6. Click *Home* to return to the Systems Insight Manager Home page.

Creating toolboxes

Toolboxes are used to customize the administrative capabilities of Systems Insight Manager users. This exercise lists steps to create toolboxes that can be assigned to specific users.

1. From the HP Systems Management Home page, select *Options* → *Security* → *Users and Authorizations*. On the Users and Authorizations page, click the *Toolboxes* tab.
2. Click *New*. The New Toolbox page displays.



New Toolbox

Required field:*

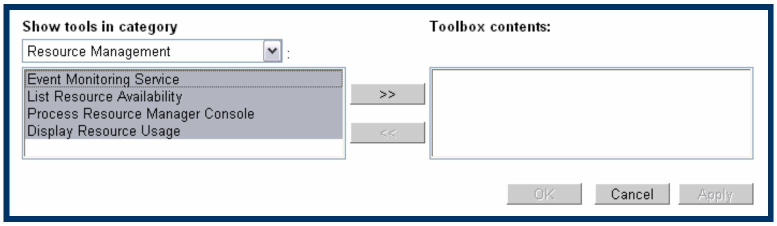
Name: *

Description:

☑ Toolbox is enabled

Show tools in category: Configuration Tool

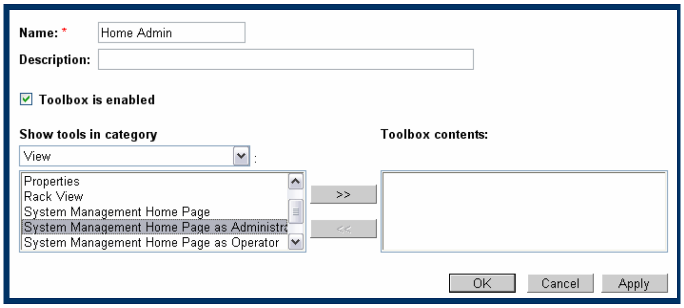
3. In the Name field, enter *Res Management*. From the Show tools in category drop-down list, select *Resource Management*.



Show tools in category: Resource Management

4. Select all of the tools in the left box. Click the >> arrow button to move the selected tools into the Toolbox contents box. Click *OK*. The *Res Management* toolbox is now available.

5. Click *New*. The New Toolbox page displays.
6. In the Name field, enter *Home Admin*. From the Show tools in category drop-down list, select *View*.
7. Scroll down the list to select *System Management Home Page as Administrator*. Click the arrow to move it into the Toolbox contents box. Click *OK*.



Name: * Home Admin

Description:

☑ **Toolbox is enabled**

Show tools in category View

Toolbox contents:

Properties
Rack View
System Management Home Page
System Management Home Page as Administra
System Management Home Page as Operator
>>
<<
OK
Cancel
Apply

8. The *Home Admin* toolbox is now available.
9. At the top of the screen, click *Logout* under the Systems Insight Manager heading.

Adding authorizations

In this exercise you will authorize Kathy Morgan to use the Res Management and Home Admin toolboxes.

1. Log in as *KMorgan* with a password of *password*. Notice that the Home page is different from the one used by ServerAdmin. Why?

   ....

2. Under System Lists, click *All Systems*. What do you observe?

   ....

3. How many Uncleared System Events are shown in the top right corner?

   ....

4. Log out and then log in as *ServerAdmin*.
5. Select *Options* → *Security* → *Users and Authorizations.*
6. On the Users and Authorizations page, click the *Authorizations* tab.
7. Click *New*. The New Authorizations page displays.
8. Select *Kathy Morgan* from the Select User(s) list and *Res Management* from the Select Toolbox(es) list.
9. Choose *System(s)* from the *Select* drop-down list and select your system. Click *OK*. The newly created authorization is in the list.
10. Log out and log in as *KMorgan*. How many Uncleared Status Events display?

    ....

11. Under System Lists, click *All Systems*. What do you notice now?

    ....

12. Click the icon in the HW column for your server. This will open the System Management Homepage. What are you required to do before the System Management Homepage displays?

    ....

13. **Do not provide credentials to log in at this time**. Close the browser with the System Management Homepage login page.
14. Log out and log in as *ServerAdmin*.
15. Select *Options* → *Security* → *Users and Authorizations*. Select the *Authorizations* tab and click *New*.
16. Select *Kathy Morgan* from the Select User(s) list and *Home Admin* from the Select Toolbox(es) list.
17. Choose *System(s)* from the *Select* drop-down list and select your system. Click *OK*.
18. Log out and log in as *KMorgan*. Under System Lists, click *All Systems*. Click the icon in the HW column for your server. You should now see the System Management Homepage without providing any login credentials. Close the System Management Homepage browser.

Exercise 3 — Monitoring managed systems

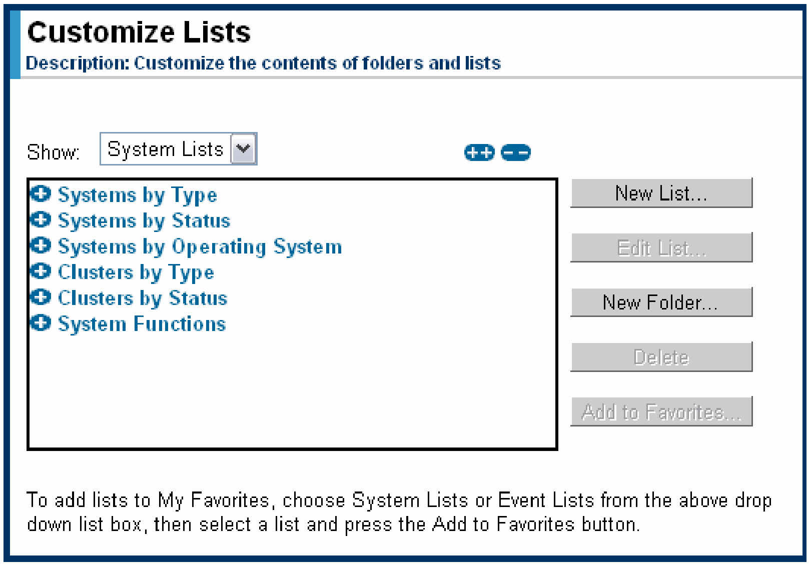
After the first discovery is run, you can monitor systems using the tools in the System Lists. It enables you to drill down to locate more information about managed systems.

Creating personal folders and lists

Task 1: Create a customized list of hardware resources

In this exercise you will create system folders and use the Advanced Search feature of Systems Insight Manager to create customized lists.

1. Connect and log in to Systems Insight Manager as *ServerAdmin*.
2. On the Systems Insight Manager Home page, click the *Customize* button near System Lists. The Customize Lists screen displays.



Customize Lists

Description: Customize the contents of folders and lists

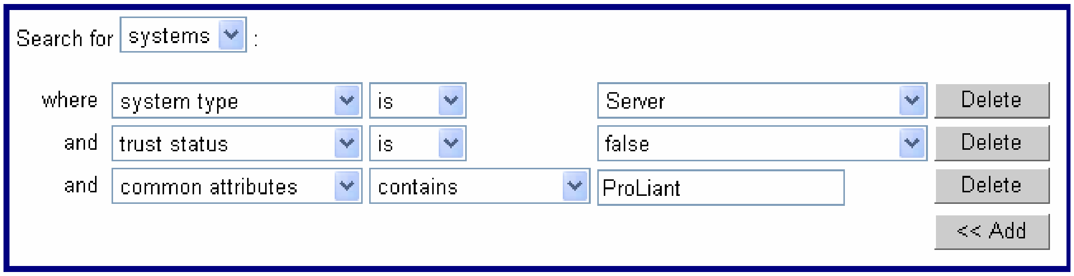
Show: System Lists

To add lists to My Favorites, choose System Lists or Event Lists from the above drop down list box, then select a list and press the Add to Favorites button.

3. Click *New Folder*. In the name box, enter *Environment Info* and then click *OK*. This creates a new system folder.

4. You can search for matches in common system attributes using Search. Common system attributes include:
   - DNS name
   - Device host name
   - Serial number
   - Operating system type
   - Operating system version
   - Operating system description
   - Operating system name
   - Product model
   - System type
   - IP address

   Enter *ProLiant* in the Search field and click *Go* or press *Enter*.
5. A list of servers displays that meet this criteria. You can save this list to use for a task. However, in this exercise, you will use the Advanced Search feature to specify a unique list of criteria. Click the *Advanced Search* link.
6. Configure the search using the criteria shown in the graphic.



Search for systems :

where system type is Server

and trust status is false

and common attributes contains ProLiant

7. To save the list, click the *Save As* button. In the Name box, enter *ProLiant systems without trust configured*. Select the *Existing personal folder* radio button and then select *Environment Info* from the drop-down list and click *OK*. Click *OK* in the confirmation box.
8. In the System Lists frame, expand *System Lists* → *Environment Info* and click *ProLiant systems without trust configured*. The results of the query displays in right-hand frame.

Task 2: Create a customized list based on protocols

If a system cannot be identified using discovery methods such as hardware status or components, create a list based on the protocols that are being used to manage the system.

1. In the left frame on the Systems Insight Manager Home page, click *Advanced Search*. Search for systems where management protocol is WBEM.
2. Click *Save As*. On the Save List As page, enter *Systems managed using WBEM*. Select the *Existing personal folder* radio button and then select the *Environment Info* folder from the drop-down list and click *OK*. Click *OK* in the confirmation box.
3. Expand *System Lists* → *Systems by Management Protocol* and click *Systems managed using WBEM*. The results of the query displays in the right-hand frame.

Task 3: Add lists to a Favorites folder

One benefit of creating a new list under My Favorites is that it can display as a status icon next to the list to show the most critical status within the list.

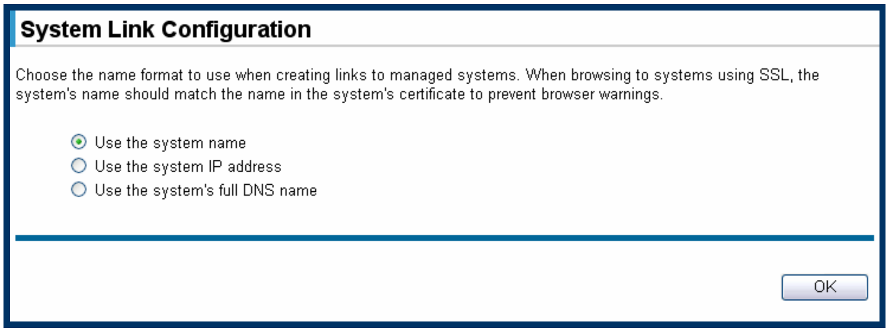
To create a list in the Favorites folder:

1. Click *Customize* in the System Lists pane. The Customizes List page displays.
2. Scroll down the list and select *ProLiant systems without trust configured*.
3. Click the *Add to Favorites* button.
4. Enter *Security info* in the New Folder field.
5. Click *OK* to add the folder and list to My Favorites. Click *OK* in the confirmation box.
6. The new folder and list display. Notice that the status of the list is represented by one of the status icons.

Task 4: Configuring system links

When you are browsing to systems, configuring system link information to ensure that the system name matches the name in the system certificate can prevent browser warnings.

1. From the Systems Insight Manager Home page, select *Options* → *Security* → *System Link Configuration*. The System Link Configuration page displays.



System Link Configuration

Choose the name format to use when creating links to managed systems. When browsing to systems using SSL, the system's name should match the name in the system's certificate to prevent browser warnings.

● Use the system name
○ Use the system IP address
○ Use the system's full DNS name

2. Select *Use the System Name* and then click *OK*.

   In the case of devices with multiple network interfaces, selecting *Use the System Name* provides only one link per destination to the device, whereas selecting *Use the system IP address* results in multiple links for the device.

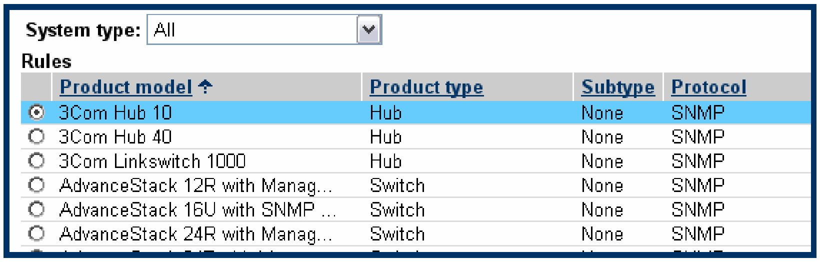
3. Return to the Systems Insight Manager Home page.

Managing system types

Systems categorized in Systems Insight Manager can be customized based on SNMP system object identifiers (OIDs). Manufacturers assign unique system object identifiers to their SNMP instrumented products. In this exercise, you will use System Type Manager to customize how third-party systems are identified by creating rules that map these system object identifiers to product categories and names.

HP can only guarantee the results on HP equipment in the classroom. Some of the actions are designed to demonstrate what would happen if there were third-party devices in the classroom. These actions are clearly labeled. Notify your instructor if your actions do not produce the expected result.

1. On the Systems Insight Manager Home page, select *Options → Discovery → Manage System Types*. The Manage System Types interface displays.

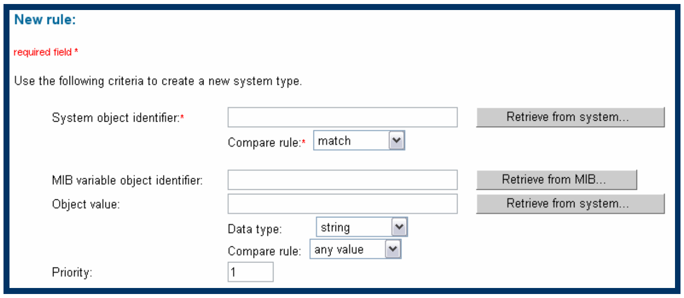


System type: All

Rules

	Product model	Product type	Subtype	Protocol
●	3Com Hub 10	Hub	None	SNMP
○	3Com Hub 40	Hub	None	SNMP
○	3Com Linkswitch 1000	Hub	None	SNMP
○	AdvanceStack 12R with Manag...	Switch	None	SNMP
○	AdvanceStack 16U with SNMP ...	Switch	None	SNMP
○	AdvanceStack 24R with Manag...	Switch	None	SNMP

2. Select one of the systems in the list and click *Edit*. Notice the data provided by the third party to allow identification of the device. Click *Cancel*.
3. On the Manage System Types page, click *New*. The New rule page displays.



New rule:

required field *

Use the following criteria to create a new system type.

System object identifier:*

Compare rule:* match

MIB variable object identifier:

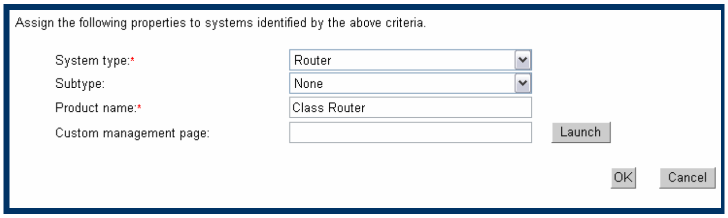
Object value:

Data type: string

Compare rule: any value

Priority: 1

4. Scroll down the page and select *Router* for the system type and *Class Router* for the product name.



Assign the following properties to systems identified by the above criteria.

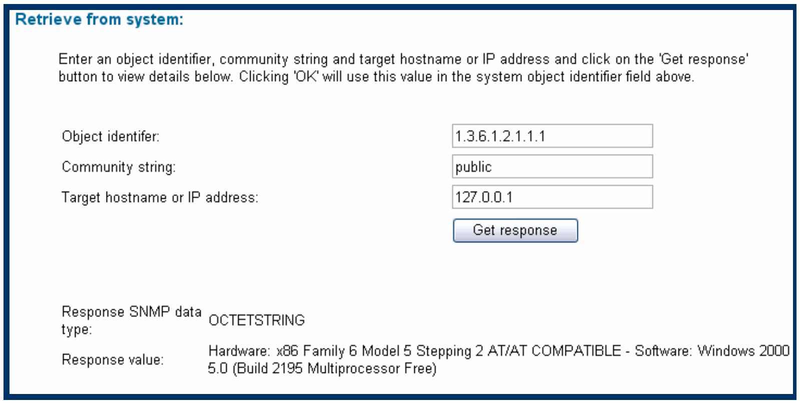
System type:* Router

Subtype: None

Product name:* Class Router

Custom management page:

5. Scroll up the page and click the *Retrieve from system* option opposite the System object identifier box. In the Target IP Address field, enter *127.0.0.1*. In a production environment this would normally be the IP address of the system you want to identify.
6. Click *Get Response*. The response values populate. Click *OK*.
7. On the New Rule page, click *Retrieve from MIB*. Select a MIB such as rfc1213 that would most likely be supported on the target system and a MIB variable from the drop-down list. Pick a MIB. On the Retrieve from MIB page, click *OK*.
8. On the New Rule page, click the *Retrieve from system* option opposite the Object value box. Click *Get response* → *OK*.



Retrieve from system:

Enter an object identifier, community string and target hostname or IP address and click on the 'Get response' button to view details below. Clicking 'OK' will use this value in the system object identifier field above.

Object identifer: 1.3.6.1.2.1.1.1

Community string: public

Target hostname or IP address: 127.0.0.1

Response SNMP data type: OCTETSTRING

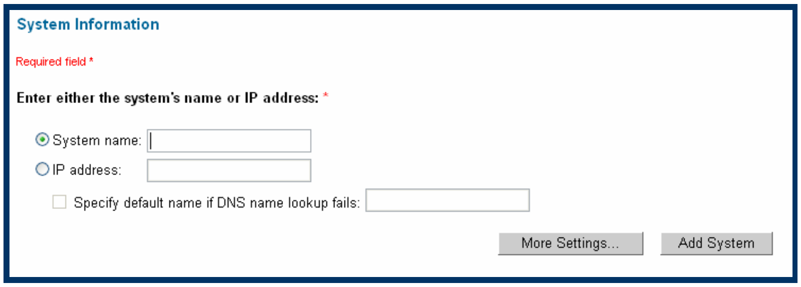
Response value: Hardware: x86 Family 6 Model 5 Stepping 2 AT/AT COMPATIBLE - Software: Windows 2000 5.0 (Build 2195 Multiprocessor Free)

9. On the New Rule page, click *OK*. Class Router is included in the list of third-party-devices.

Performing a manual discovery

In this exercise, you will perform a manual device discovery. This exercise enables you populate the database with the third-party system type added in the previous exercise.

1. From the Systems Insight Manager Home page, select *Options* → *Discovery* → *Manual Discovery*.


System Information
Required field *
Enter either the system's name or IP address: *
● System name:
○ IP address:
☐ Specify default name if DNS name lookup fails:
More Settings...
Add System

4. Enter the IP address of the system in the field.
5. Click *More Settings* to view the additional options.
6. Scroll down the page and click *Add System*.
7. When the status field on the top right indicates that identification is complete, click the *All Systems* link on the left to see your target system listed and identified as specified in your rule.

Uploading and registering a MIB using the command line interface

If you have third-party systems on your network, you can register the MIBs that accompany the systems. In this exercise you will use the command line to manage MIBS.

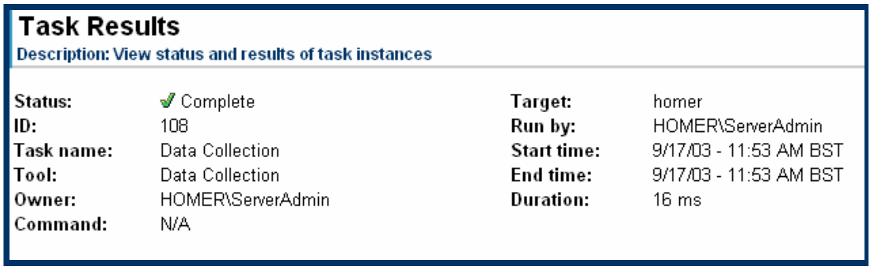
> **Note**
>
> Completion of this exercise requires you to copy MCompile.exe to the MIB directory and access the class folder.

1. On the Systems Insight Manager server, select *Start* → *Run*. In the Open box, enter *cmd* and click *OK*.
2. At the command prompt, enter *mxmib*. A list of registered MIBs displays.
3. At the command prompt, enter *cd c:\program files\hp\systems insight manager\mibs*.
4. Copy the .mib file from the class folder to this directory.
5. At the command prompt, enter *mcompile [mib_file_name]* where *mib_file_name* is the .mib file in the class folder. This creates a .cfg file from the .mib file.
6. To register the MIB, enter *mxmib –a [mib_cfg_file].cfg* where *mib_cfg_file* is the file created in step 5.
7. Enter *mxmib*. Notice the new MIB is now registered.

Running data collection

Now you will collect data to view information about discovered devices.

1. Click the *All Systems* link. Select your server from the list and then select *Options* → *Data Collection*.
2. Confirm that your system is the verified target and click *Next*.
3. On the Data Collection — Inventory Data Collection (single or historical) page, select *Overwrite existing data set* and click *Run Now*.
4. The *Task Results* page displays. Review the results to ensure that the task completed successfully.

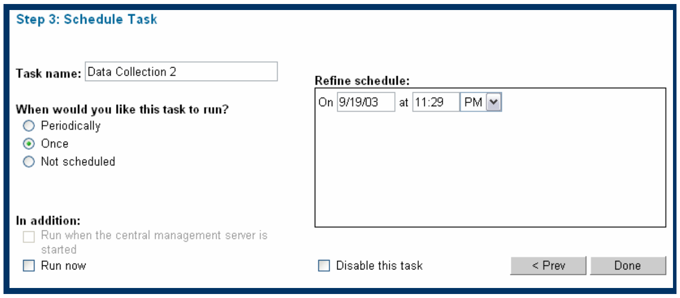


Task Results

Description: View status and results of task instances

Status:	✓ Complete	**Target:**	homer
ID:	108	**Run by:**	HOMER\ServerAdmin
Task name:	Data Collection	**Start time:**	9/17/03 - 11:53 AM BST
Tool:	Data Collection	**End time:**	9/17/03 - 11:53 AM BST
Owner:	HOMER\ServerAdmin	**Duration:**	16 ms
Command:	N/A		

5. Select *Tools* → *System Information* → *System Page*. Confirm that your system is the verified target and click *Run Now*. The System Page displays.
6. Click the *Links* tab and the *Data Collection Report* link. The report opens in a new browser. Review the data collection report.
7. Click the link at the top of the report to export the file in comma-separated values (CSV) format.
8. Close all browsers other than Systems Insight Manager.
9. Click the *All Systems* link. Select your server from the list and then select *Options* → *Data Collection*.
10. Confirm that your system is the verified target and click *Next*.
11. On the Data Collection — Inventory Data Collection (single or historical) page, select *Append new data set (for historical trend analysis)* and click *Schedule*. Select *Periodically* and configure the data collection to run every hour. Click *Done*.



Step 3: Schedule Task

Task name: Data Collection 2

When would you like this task to run?
○ Periodically
● Once
○ Not scheduled

In addition:
☐ Run when the central management server is started
☐ Run now

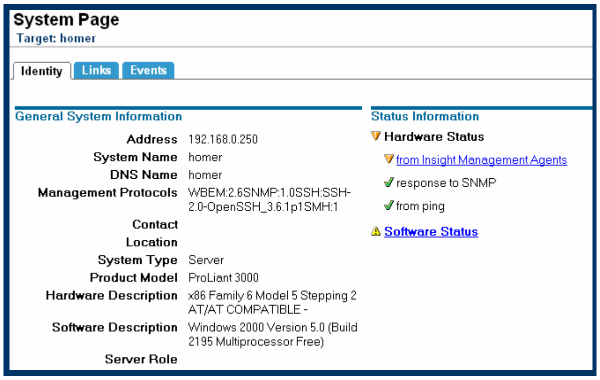
Refine schedule:
On 9/19/03 at 11:29 PM

☐ Disable this task

Viewing device information

In this exercise you will investigate the System Management Homepage. There is more than one way to access the Homepage; in this exercise you will use the System Page.

1. To display the System Page of your system, click the link of the system from the All Systems list. Confirm that your system is the verified target and click *Run Now*. The System Page displays.
2. Click the *Identity* tab. Notice the system and status information available.



System Page
Target: homer

General System Information

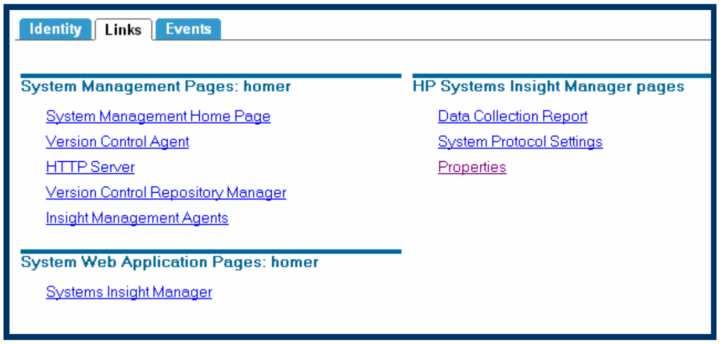
Address 192.168.0.250
System Name homer
DNS Name homer
Management Protocols WBEM:2.6SNMP:1.0SSH:SSH-2.0-OpenSSH_3.6.1p1SMH:1
Contact
Location
System Type Server
Product Model ProLiant 3000
Hardware Description x86 Family 6 Model 5 Stepping 2 AT/AT COMPATIBLE -
Software Description Windows 2000 Version 5.0 (Build 2195 Multiprocessor Free)
Server Role

Status Information

Hardware Status
- from Insight Management Agents
- ✓ response to SNMP
- ✓ from ping

Software Status

3. Click the *Links* tab. The *Links* tab has a list of hyperlinks to the system management web environment for the server. Click the *System Management Home Page* link to display the System Management Homepage for your server.



System Management Pages: homer

- System Management Home Page
- Version Control Agent
- HTTP Server
- Version Control Repository Manager
- Insight Management Agents

System Web Application Pages: homer

- Systems Insight Manager

HP Systems Insight Manager pages

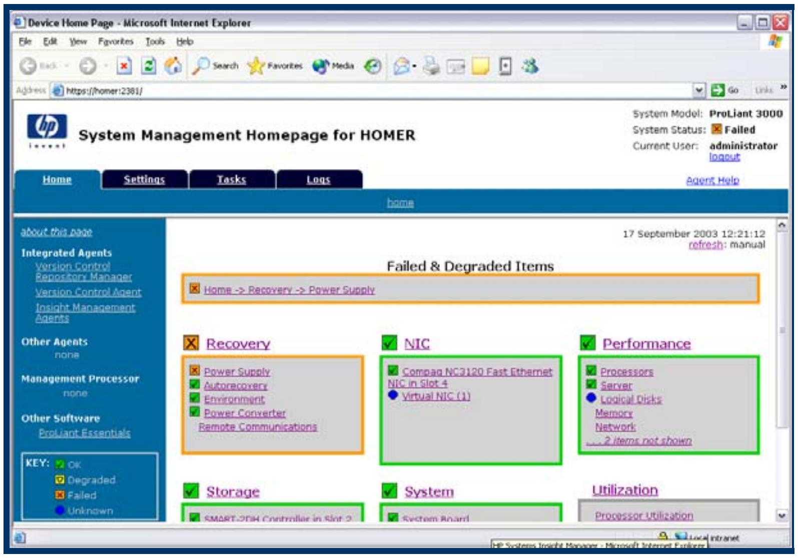
- Data Collection Report
- System Protocol Settings
- Properties

Note

If WBEM has been discovered on the device, a link to the property pages will be available.

---

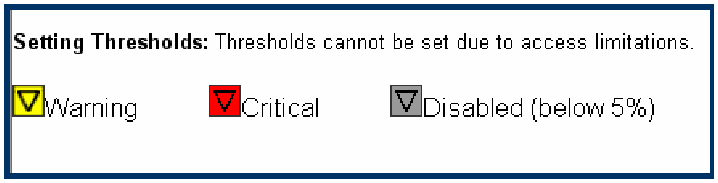
4. Notice the System Status in the top right corner and the Failed & Degraded Items section of the screen. If an item is in a failed or degraded state, its group on the System Management Homepage also displays as degraded and changes color accordingly. It is possible to follow this color change to the degraded item. In the Performance section, click *Processors*.



System Model: ProLiant 3000
System Status: ☒ Failed
Current User: administrator

17 September 2003 12:21:12

5. Review the information available. Notice that your ability to set thresholds is currently denied. Click the *Home* tab to return to the Homepage.


Setting Thresholds: Thresholds cannot be set due to access limitations.

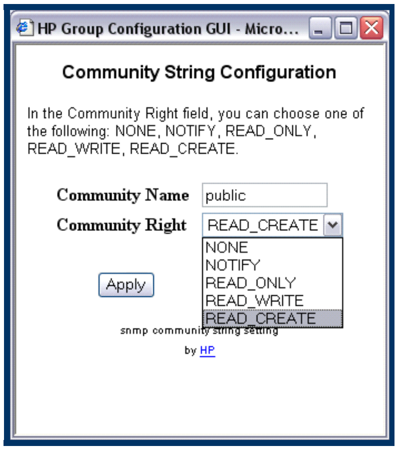
6. Using the links on the Homepage, complete the information in the table.

Variable	Value
Speed of the NIC	
MAC address	
Amount of transmitted bytes	
Firmware version of the disk controller	
Size of the disk controller on-board cache	
Machine	
Total system memory	
Number of memory slots available	
Processor utilization over the last 30 minutes	

7. Return to the System Page and click the *Identity* tab. Click the *Insight Management Agents* link. On the Account Login page, enter *password* as the administrator password. Click *OK*.

8. Notice the various links on the Insight Management Agents page. Use them to navigate around the environment and familiarize yourself with the information provided.

9. In the left pane under Configuration, click the *SNMP Configuration* link. Click the *Security* link under SNMP Configuration. Notice that the public Community Name has the READ_ONLY right. Select the *public* community name and click *Edit*. The Community String Configuration page displays.



Community String Configuration

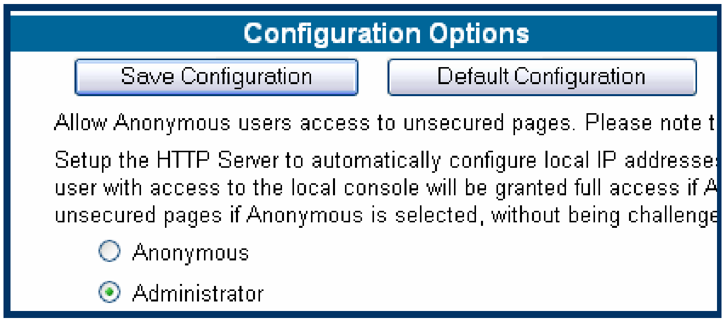
In the Community Right field, you can choose one of the following: NONE, NOTIFY, READ_ONLY, READ_WRITE, READ_CREATE.

Community Name public

Community Right READ_CREATE

snmp community string setting
by HP

10. From the drop-down list, select *READ_CREATE* and click *Apply*. On the Security Configuration page, click *Apply*.
11. Enable SNMP sets on the server and clients by selecting *Start* → *Control Panel* → *HP management agents* → *SNMP settings*. Select *Enable SNMP sets* → *OK*. The agents will restart with SNMP sets enabled.
12. Return to the Systems Insight Manager System Page.
13. Click the *Links* tab and then the *System Management Home Page* link.
14. Click the *Settings* tab. In the HTTP Server section, click *Options*. This Configuration Options page allows the configuration and authentication of access to the management web environment on the server. Ensure that the *Local Access* check box and the *Administrator* radio button are selected, and then click *Save Configuration*.



Allow Anonymous users access to unsecured pages. Please note t

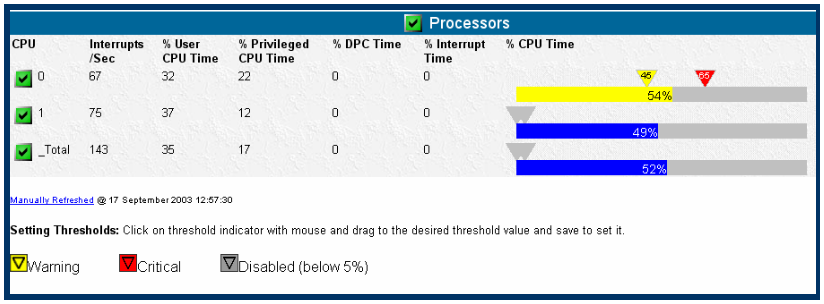
Setup the HTTP Server to automatically configure local IP addresse
user with access to the local console will be granted full access if A
unsecured pages if Anonymous is selected, without being challenge

○ Anonymous

● Administrator

15. On the System Management Homepage, click the *Tasks* tab.

16. In the Performance section, click the *3 Items Not Shown* link and then click *Processors*. Notice that you can now move the threshold indicators under % CPU Time. When they are moved the Warning indicator becomes yellow and the Critical indicator red, both of them displaying the numerical value of the position on the % bar. Click *Save Thresholds* to apply the settings.



☑ Processors

CPU	Interrupts /Sec	% User CPU Time	% Privileged CPU Time	% DPC Time	% Interrupt Time	% CPU Time
☑ 0	67	32	22	0	0	54%
☑ 1	75	37	12	0	0	49%
☑ _Total	143	35	17	0	0	52%

Manually Refreshed @ 17 September 2003 12:57:30

Setting Thresholds: Click on threshold indicator with mouse and drag to the desired threshold value and save to set it.

▽ Warning ▽ Critical ▽ Disabled (below 5%)

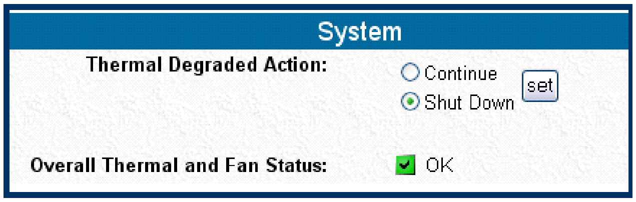
Note

If the java applets fail to load for setting the thresholds, then the Sun Java Plug-in is probably being used. Ensure that the *Use Java 2 v1.4.1_04 for <applet> (requires restart)* option is not checked in the Internet Options of Internet Explorer.

---

17. Review the data available through the other links in the Performance section.

18. In the Recovery section of the Tasks tab, click *Environment – Thermal Degraded Action*. Notice the Temperature and Threshold columns. Notice also the Thermal Degraded Action options.



System

Thermal Degraded Action: ○ Continue ● Shut Down

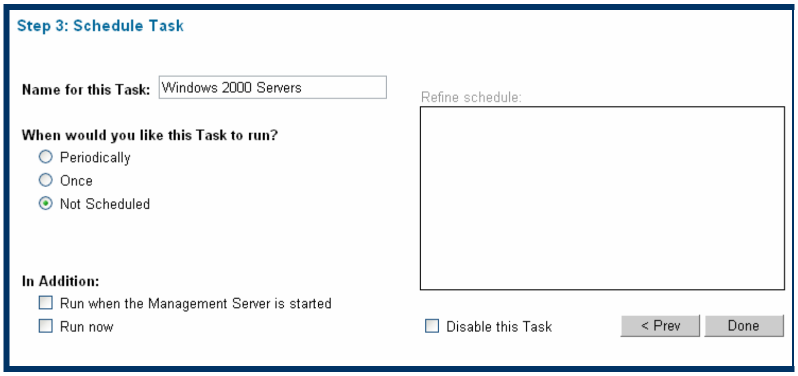
Overall Thermal and Fan Status: ☑ OK

19. Close the browser showing the System Management Homepage and return to the System Page. Click the *Events* tab. Notice the list of events that displays. Click each event link to view additional information.

Viewing hardware status polling

Systems Insight Manager collects status information of discovered devices based on predefined collection schedules. You can use hardware status polling to configure groups of devices with different polling schedules based on the importance of the devices.

1. From the Systems Insight Manager Home page, select *Options* → *Status Polling* → *Hardware Status Polling*.
2. The Hardware Status Polling page displays. Under Choose Targets by Selecting, select the *Individual Systems in the List* radio button. Select *Microsoft Windows 2000* from the drop-down list.
3. You will see a table of all discovered devices that are running Windows 2000. Select your server from the table and then click *Apply Selections*. Click *Next*.
4. View the available *Protocol Settings*. Click *Schedule*.



Step 3: Schedule Task

Name for this Task: Windows 2000 Servers

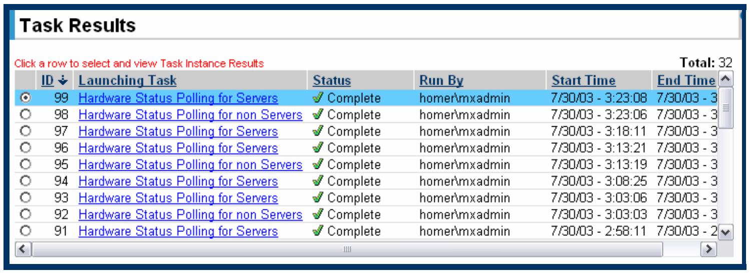
When would you like this Task to run?

○ Periodically
○ Once
● Not Scheduled

In Addition:

☐ Run when the Management Server is started
☐ Run now

5. Select *Periodically* and then *Once* for the 'When would you like this task to run?' field. Notice the schedules that display in the Refine Schedule box.
6. Select *Periodically* and then click *Done*.
7. The *All Scheduled Tasks* page displays. In the list of tasks, select *Hardware Status Polling for Servers*. View the Last Run and Schedule information.
8. View the information under *Task Results*. Click the *Server Status Polling List* link to view the servers being polled by that task. Then click *OK*.
9. Click *Logs* → *View Task Results*. This table shows the tasks that have completed and their status. Select a task to show extended information below the list. Return to the Systems Insight Manager Home page.



Task Results

Click a row to select and view Task Instance Results

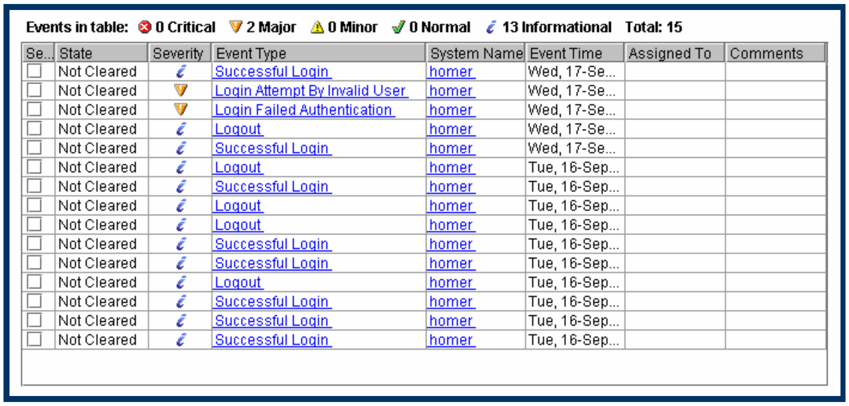
Total: 32

	ID ↓	Launching Task	Status	Run By	Start Time	End Time
●	99	Hardware Status Polling for Servers	✓ Complete	homer\mxadmin	7/30/03 - 3:23:08	7/30/03 - 3
○	98	Hardware Status Polling for non Servers	✓ Complete	homer\mxadmin	7/30/03 - 3:23:06	7/30/03 - 3
○	97	Hardware Status Polling for Servers	✓ Complete	homer\mxadmin	7/30/03 - 3:18:11	7/30/03 - 3
○	96	Hardware Status Polling for Servers	✓ Complete	homer\mxadmin	7/30/03 - 3:13:21	7/30/03 - 3
○	95	Hardware Status Polling for non Servers	✓ Complete	homer\mxadmin	7/30/03 - 3:13:19	7/30/03 - 3
○	94	Hardware Status Polling for Servers	✓ Complete	homer\mxadmin	7/30/03 - 3:08:25	7/30/03 - 3
○	93	Hardware Status Polling for Servers	✓ Complete	homer\mxadmin	7/30/03 - 3:03:06	7/30/03 - 3
○	92	Hardware Status Polling for non Servers	✓ Complete	homer\mxadmin	7/30/03 - 3:03:03	7/30/03 - 3
○	91	Hardware Status Polling for Servers	✓ Complete	homer\mxadmin	7/30/03 - 2:58:11	7/30/03 - 2

Viewing Systems Insight Manager events

In this exercise, you will generate events on the Systems Insight Manager management system and then view the events in the Systems Insight Manager interface.

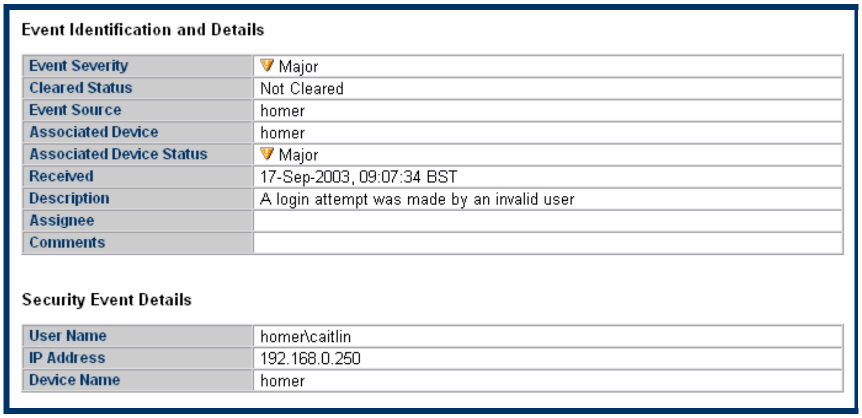
1. If it is still open, close the browser that you are using to manage Systems Insight Manager.
2. Reopen the browser and connect to the management server on port 280.
3. At the logon page, enter the user name *ServerAdmin* with a password of *bananas*. The logon should fail.
4. Click the link again and enter the user name *Kit* with a password of *horses*. The login should fail.
5. Click the link again and enter *ServerAdmin* with a password of *password*. This should create two Systems Insight Manager events.
6. On the left pane of the Systems Insight Manager page, expand *Event Lists* → *Login Events* and click *All Login and Logout Events*. The All Login and Logout page displays showing informational events and at least two major events. Expand the *Event Type* column until you can see all event types.



Events in table: ⊗ **0 Critical** ▼ **2 Major** ⚠ **0 Minor** ✓ **0 Normal** ℹ **13 Informational** **Total: 15**

Se...	State	Severity	Event Type	System Name	Event Time	Assigned To	Comments
☐	Not Cleared	ℹ	Successful Login	homer	Wed, 17-Se...		
☐	Not Cleared	▼	Login Attempt By Invalid User	homer	Wed, 17-Se...		
☐	Not Cleared	▼	Login Failed Authentication	homer	Wed, 17-Se...		
☐	Not Cleared	ℹ	Logout	homer	Wed, 17-Se...		
☐	Not Cleared	ℹ	Successful Login	homer	Wed, 17-Se...		
☐	Not Cleared	ℹ	Logout	homer	Tue, 16-Sep...		
☐	Not Cleared	ℹ	Successful Login	homer	Tue, 16-Sep...		
☐	Not Cleared	ℹ	Logout	homer	Tue, 16-Sep...		
☐	Not Cleared	ℹ	Logout	homer	Tue, 16-Sep...		
☐	Not Cleared	ℹ	Successful Login	homer	Tue, 16-Sep...		
☐	Not Cleared	ℹ	Successful Login	homer	Tue, 16-Sep...		
☐	Not Cleared	ℹ	Logout	homer	Tue, 16-Sep...		
☐	Not Cleared	ℹ	Successful Login	homer	Tue, 16-Sep...		
☐	Not Cleared	ℹ	Successful Login	homer	Tue, 16-Sep...		
☐	Not Cleared	ℹ	Successful Login	homer	Tue, 16-Sep...		

7. In the Event Type column, click the link for one of the major events and notice the event details. Take note of the information returned. Scroll up to the event list and notice the ability to add comments and to assign the event using the buttons provided



Event Identification and Details

Event Severity	▼ Major
Cleared Status	Not Cleared
Event Source	homer
Associated Device	homer
Associated Device Status	▼ Major
Received	17-Sep-2003, 09:07:34 BST
Description	A login attempt was made by an invalid user
Assignee	
Comments	

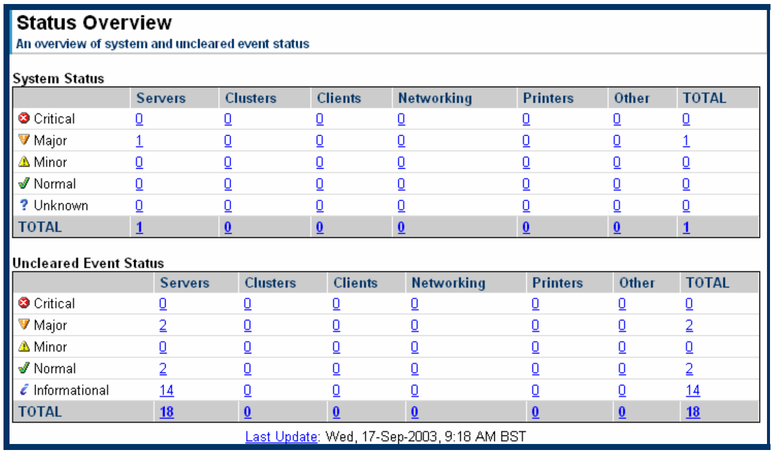
Security Event Details

User Name	homer\caitlin
IP Address	192.168.0.250
Device Name	homer

8. Click the link for the other major event and again notice the event details. What is the difference between the descriptions of the two events?

……………………………………………………………………………………………………

9. In the left pane, click *Status Overview*. This table provides an overview of events on all managed systems and links to the events themselves.



Status Overview

An overview of system and uncleared event status

System Status

	Servers	Clusters	Clients	Networking	Printers	Other	TOTAL
⊗ Critical	0	0	0	0	0	0	0
▼ Major	1	0	0	0	0	0	1
⚠ Minor	0	0	0	0	0	0	0
✓ Normal	0	0	0	0	0	0	0
? Unknown	0	0	0	0	0	0	0
TOTAL	**1**	**0**	**0**	**0**	**0**	**0**	**1**

Uncleared Event Status

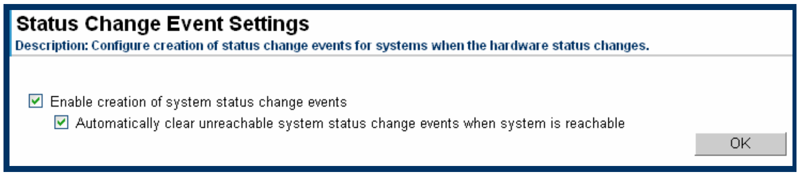
	Servers	Clusters	Clients	Networking	Printers	Other	TOTAL
⊗ Critical	0	0	0	0	0	0	0
▼ Major	2	0	0	0	0	0	2
⚠ Minor	0	0	0	0	0	0	0
✓ Normal	2	0	0	0	0	0	2
ℹ Informational	14	0	0	0	0	0	14
TOTAL	**18**	**0**	**0**	**0**	**0**	**0**	**18**

Last Update: Wed, 17-Sep-2003, 9:18 AM BST

Configuring SNMP trap settings

In this exercise you will configure SNMP trap settings.

1. On the Systems Insight Manager Home page, select *Options* → *Events* → *Status Change Event Settings*.

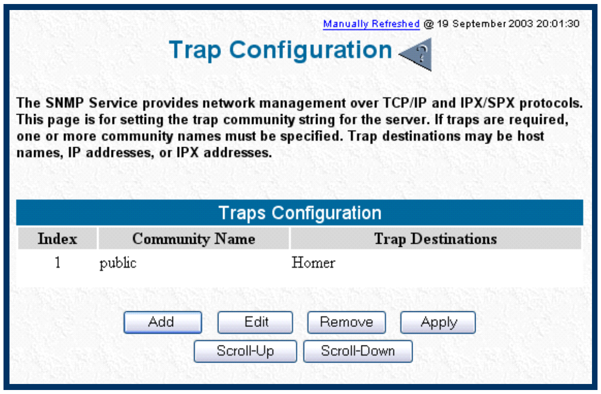


Status Change Event Settings

Description: Configure creation of status change events for systems when the hardware status changes.

☑ Enable creation of system status change events
  ☑ Automatically clear unreachable system status change events when system is reachable

2. This screen enables you to configure the behavior of the system in case of a hardware status change.
3. From the HP Systems Management Home page, select *Tools* → *System Information* → *System Page*.
4. Ensure that your system is the target system and click *Run Now*. Click the *Links* tab and then the *Insight Management Agents* link.
5. In the left-hand pane, click *SNMP Configuration*. In the SNMP Configuration pane, click the *Trap* link.



Manually Refreshed @ 19 September 2003 20:01:30

Trap Configuration

The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. This page is for setting the trap community string for the server. If traps are required, one or more community names must be specified. Trap destinations may be host names, IP addresses, or IPX addresses.

Traps Configuration

Index	Community Name	Trap Destinations
1	public	Homer

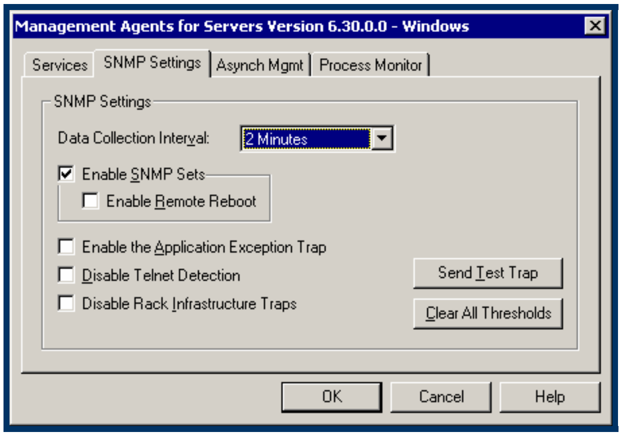
6. On the Trap Configuration page, click *public* in the Community Name column and then click *Edit*.
7. In the Trap Destinations box, enter the IP address of the CMS and the other server in your student set separated by a semicolon. Click *Apply*.
8. On the Trap Configuration page, click *Apply* and then close the Insight Management Agents browser.
9. On the Systems Insight Manager Home page, what is the number of major events in the Uncleared Event Status area?

....

10. On the Systems Insight Manager server, click *Start* → *Settings* → *Control Panel*.

11. Double-click the *HP Management Agents* icon and then click the *SNMP Settings* tab.

12. Click the *Send Test Trap* button and then click *OK* in the confirmation box.



Management Agents for Servers Version 6.30.0.0 - Windows

SNMP Settings

Data Collection Interval: 2 Minutes

☑ Enable SNMP Sets
☐ Enable Remote Reboot
☐ Enable the Application Exception Trap
☐ Disable Telnet Detection
☐ Disable Rack Infrastructure Traps

13. On the Systems Insight Manager Home page, what is the number of major events in the Uncleared Event Status area?

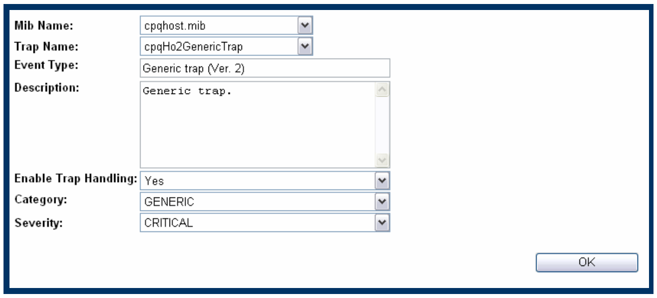
....

14. Click the number link underneath the major icon to open the *Major Uncleared Events* list.

15. Click the link for the trap that was just sent, *Generic trap (Ver. 2)*. Notice the information in the trap details, especially the associated MIB name.

16. On the Systems Insight Manager Home page, click *Options* → *Events* → *SNMP Trap Settings*.

17. On the SNMP Trap Settings page, select *cpqhost.mib* for the MIB Name, *cpqHo2GenericTrap* for the Trap Name, and change the Severity from *Major* to *Critical*. Click *OK*.



Mib Name: cpqhost.mib
Trap Name: cpqHo2GenericTrap
Event Type: Generic trap (Ver. 2)
Description: Generic trap.
Enable Trap Handling: Yes
Category: GENERIC
Severity: CRITICAL

18. Resend the test trap. What is different about the received trap?

....

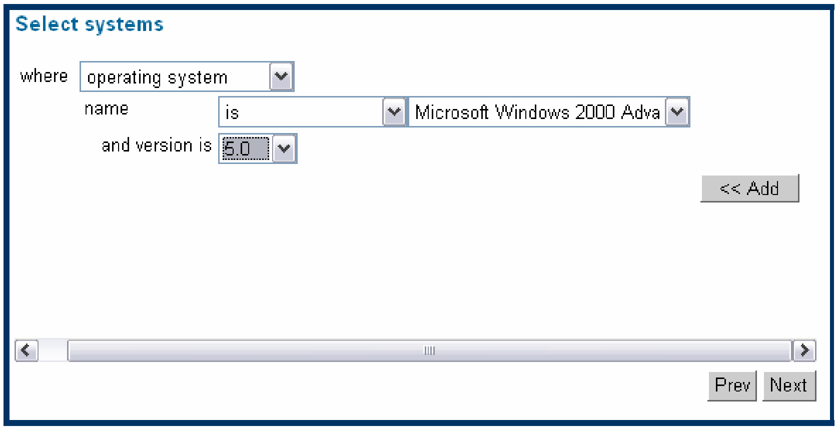
Configuring automatic event handling

In this exercise, you will configure the system to notify a member of the network administration team if a Windows 2000 Advanced Server experiences a critical event on a Monday, Wednesday, or Friday evening. You will then configure the system to notify the network infrastructure administrator if a router reports a problem at any time.

1. From the HP Systems Insight Manager Home page, select *Options* → *Security* → *Users and Authorizations*. Select the *Users* tab. Click *New*.
2. Enter the details for Kathy Morgan, filling in pager information and giving her limited rights. Click *OK*.
3. From the Systems Insight Manager Home page, select *Options* → *Events* → *Automatic Event Handling* → *New Task*. The Automatic Event Handling – New Task page displays.
4. In the Task name box, enter *Critical Event Notification MWF*. Click *Next*.
5. In the Select events section, select *where severity is Critical*. Click *Next*.
6. Configure the *Select systems* section so that events from Windows 2000 Advanced Server machines are forwarded. Click *Next*.

Note

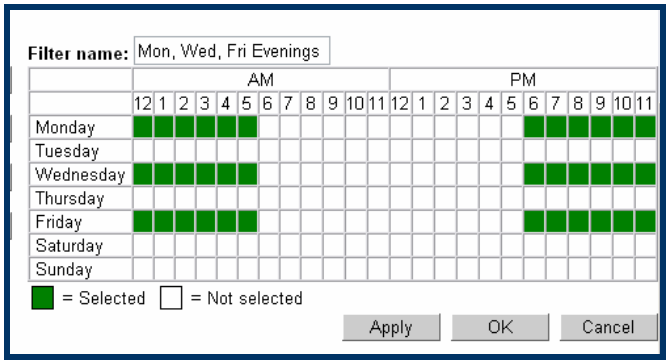
When associating a task with a list, keep the list as simple as possible to minimize the performance impacts.



where operating system
name is Microsoft Windows 2000 Adva
and version is 5.0

7. In the *Select actions* section, select *Send page, Assign* and *Write to system log*. Select *Kathy Morgan* to receive pager messages and to also have the event assigned to her. Click *Next*.

8. On the Select time filter page, select the box to use a Time Filter and click *Manage Filters*. Click *New*. For the Filter name, enter *Mon Wed Fri Evenings*. Select the times shown in the following screen image and then click *OK*. Click *Next*.

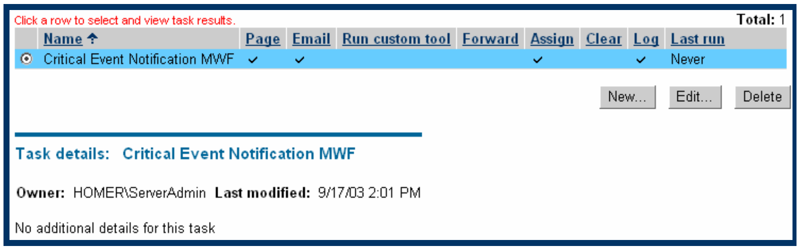


Filter name: Mon, Wed, Fri Evenings

	AM												PM											
	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11
Monday	🟩	🟩	🟩	🟩	🟩	🟩													🟩	🟩	🟩	🟩	🟩	🟩
Tuesday																								
Wednesday	🟩	🟩	🟩	🟩	🟩	🟩													🟩	🟩	🟩	🟩	🟩	🟩
Thursday																								
Friday	🟩	🟩	🟩	🟩	🟩	🟩													🟩	🟩	🟩	🟩	🟩	🟩
Saturday																								
Sunday																								

🟩 = Selected ☐ = Not selected

9. Review the summary page and then click *Finish*. The Automatic Event Handling list displays with the new event handling rule.



Click a row to select and view task results. **Total:** 1

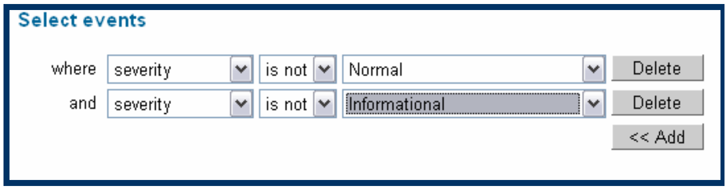
	Name ↑	Page	Email	Run custom tool	Forward	Assign	Clear	Log	Last run
●	Critical Event Notification MWF	✓	✓			✓		✓	Never

Task details: Critical Event Notification MWF

Owner: HOMER\ServerAdmin **Last modified:** 9/17/03 2:01 PM

No additional details for this task

10. From the HP Systems Insight Manager Home page, select *Options* → *Security* → *Users and Authorizations*. Select the *Users* tab. Click *New*.
11. Enter the details for Brandon Parker, filling in pager information and giving him limited rights. Click *OK*.
12. Select *Options* → *Events* → *Automatic Event Handling* → *New Task*. Name the task *Router Events* and then click *Next*.
13. In the Select events section, configure the rule so that it responds only to critical, major, and minor events. Use the *Add* button to add additional rules. Click *Next*.

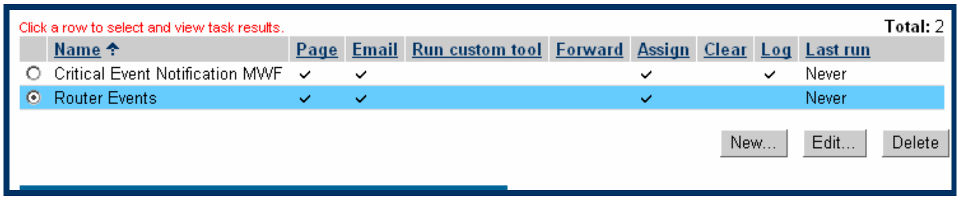


Select events

where severity is not Normal

and severity is not Informational

14. In the *Select systems* section, select *where system type is router*. Click *Next*.
15. In the *Select actions* section, configure the *Send e-mail* and *Assign* fields for Brandon Parker. Click *Next*.
16. Do not select a time filter. Click *Next*, review the summary page, and click *Finish*. The new event handling rule displays in the Automatic Event Handling list.



Click a row to select and view task results.

Total: 2

	Name	Page	Email	Run custom tool	Forward	Assign	Clear	Log	Last run
○	Critical Event Notification MWF	✓	✓			✓		✓	Never
●	Router Events	✓	✓			✓			Never

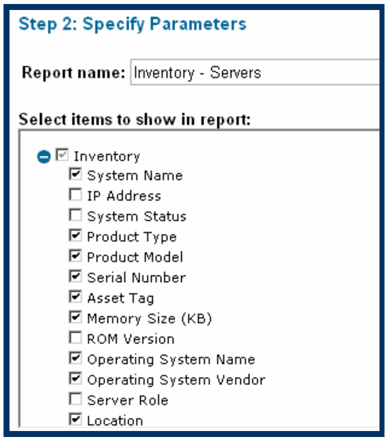
Exercise 4 — Running reports

Systems Insight Manager provides predefined reports that are accessible to any user. In addition, new reports can be created or existing reports can be modified.

Running available reports

In this exercise you will view and run reports in Systems Insight Manager.

1. On the Systems Insight Manager Home page, select *Reports* → *Manage Reports*. The Manage Reports page displays.
2. Select the *Inventory – Servers* report and click *Edit*.
3. The Verify Target Systems interface displays. Select *All Servers* and click *Next*.



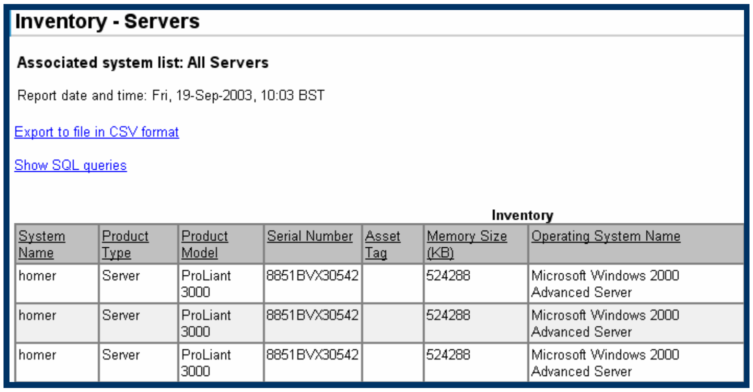
Step 2: Specify Parameters

Report name: Inventory - Servers

Select items to show in report:

- ☑ Inventory
  - ☑ System Name
  - ☐ IP Address
  - ☐ System Status
  - ☑ Product Type
  - ☑ Product Model
  - ☑ Serial Number
  - ☑ Asset Tag
  - ☑ Memory Size (KB)
  - ☐ ROM Version
  - ☑ Operating System Name
  - ☑ Operating System Vendor
  - ☐ Server Role
  - ☑ Location

4. In the Edit Report section, notice the data that is collected to comprise the report. Notice that you can change the report contents. Click *Run Report*.



Inventory - Servers

Associated system list: All Servers

Report date and time: Fri, 19-Sep-2003, 10:03 BST

Export to file in CSV format

Show SQL queries

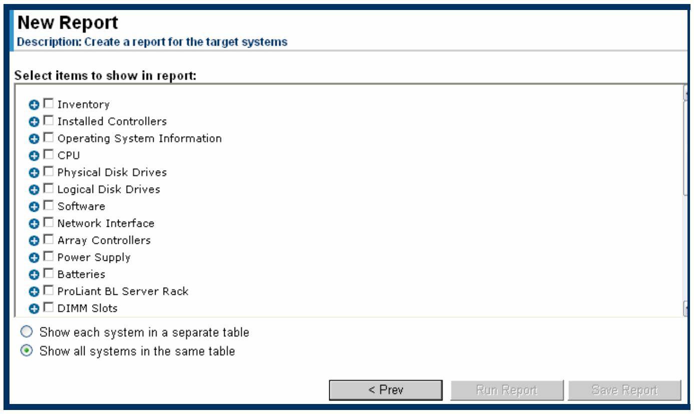
Inventory						
System Name	Product Type	Product Model	Serial Number	Asset Tag	Memory Size (KB)	Operating System Name
homer	Server	ProLiant 3000	8851BVX30542		524288	Microsoft Windows 2000 Advanced Server
homer	Server	ProLiant 3000	8851BVX30542		524288	Microsoft Windows 2000 Advanced Server
homer	Server	ProLiant 3000	8851BVX30542		524288	Microsoft Windows 2000 Advanced Server

5. The report displays in a new browser. To export the report to a CSV format, click the link in the top-left hand corner. To display the SQL queries made to the database, click *Show SQL queries*.

Creating new reports

In this exercise, you will create a new report.

1. On the Systems Insight Manager Home page, select *Reports* → *New Report*.
2. Verify that the target is *All Systems* and click *Next*. A list of possible data to include in the report displays.



New Report

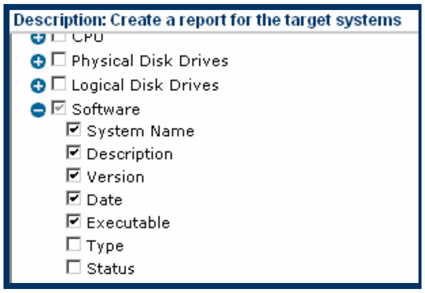
Description: Create a report for the target systems

Select items to show in report:

- ☐ Inventory
- ☐ Installed Controllers
- ☐ Operating System Information
- ☐ CPU
- ☐ Physical Disk Drives
- ☐ Logical Disk Drives
- ☐ Software
- ☐ Network Interface
- ☐ Array Controllers
- ☐ Power Supply
- ☐ Batteries
- ☐ ProLiant BL Server Rack
- ☐ DIMM Slots

○ Show each system in a separate table
● Show all systems in the same table

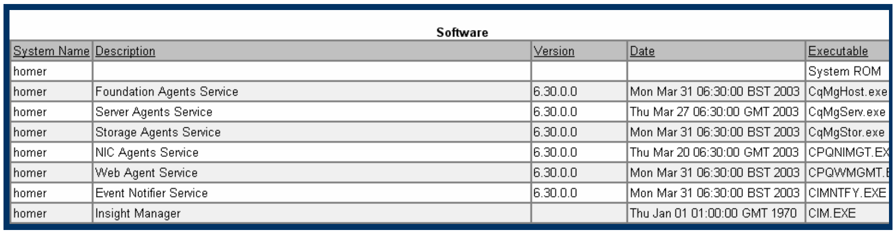
3. Expand the section headings and review the data available. Select some data to add into your report. Give the report a name and click *Run Report*.



Description: Create a report for the target systems

- ☐ CPU
- ☐ Physical Disk Drives
- ☐ Logical Disk Drives
- ☑ Software
  - ☑ System Name
  - ☑ Description
  - ☑ Version
  - ☑ Date
  - ☑ Executable
  - ☐ Type
  - ☐ Status

4. The report runs and returns the requested information. Click the link to create a CSV file from the report. This enables you to import the report into a spreadsheet. Close the report browser.



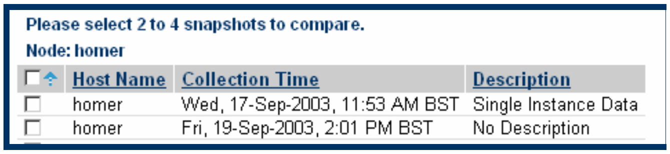
Software

System Name	Description	Version	Date	Executable
homer				System ROM
homer	Foundation Agents Service	6.30.0.0	Mon Mar 31 06:30:00 BST 2003	CqMgHost.exe
homer	Server Agents Service	6.30.0.0	Thu Mar 27 06:30:00 GMT 2003	CqMgServ.exe
homer	Storage Agents Service	6.30.0.0	Mon Mar 31 06:30:00 BST 2003	CqMgStor.exe
homer	NIC Agents Service	6.30.0.0	Thu Mar 20 06:30:00 GMT 2003	CPQNIMGT.EX
homer	Web Agent Service	6.30.0.0	Mon Mar 31 06:30:00 BST 2003	CPQWMGMT.E
homer	Event Notifier Service	6.30.0.0	Mon Mar 31 06:30:00 BST 2003	CIMNTFY.EXE
homer	Insight Manager		Thu Jan 01 01:00:00 GMT 1970	CIM.EXE

Comparing the snapshots of managed systems

In this exercise you will compare data collection snapshots for a system.

1. On the Systems Insight Manager Home page, select *Reports* → *Snapshot Comparison*. Make sure your system is the target and click *Next*.
2. The Snapshot Comparison page opens with a list of data collection snapshots. You can choose between a minimum of two to a maximum of four snapshots to compare. Select some snapshots and click *Next*. The Select categories and baseline page opens.

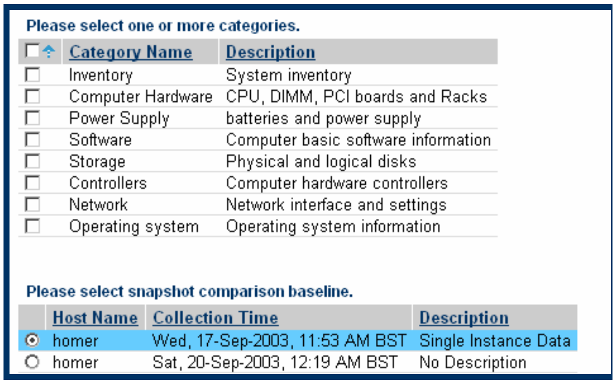


Please select 2 to 4 snapshots to compare.

Node: homer

☐	Host Name	Collection Time	Description
☐	homer	Wed, 17-Sep-2003, 11:53 AM BST	Single Instance Data
☐	homer	Fri, 19-Sep-2003, 2:01 PM BST	No Description

3. Select the snapshot content you would like to view and select one of the snapshots to use as a baseline. Then click *Run Reports*.



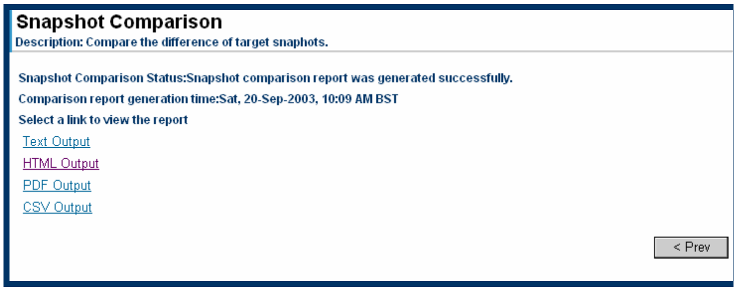
Please select one or more categories.

☐	Category Name	Description
☐	Inventory	System inventory
☐	Computer Hardware	CPU, DIMM, PCI boards and Racks
☐	Power Supply	batteries and power supply
☐	Software	Computer basic software information
☐	Storage	Physical and logical disks
☐	Controllers	Computer hardware controllers
☐	Network	Network interface and settings
☐	Operating system	Operating system information

Please select snapshot comparison baseline.

	Host Name	Collection Time	Description
●	homer	Wed, 17-Sep-2003, 11:53 AM BST	Single Instance Data
○	homer	Sat, 20-Sep-2003, 12:19 AM BST	No Description

4. The comparison process runs and offers the choice of format to view the report. Choose the *HTML Output* link. The comparison report opens in another browser. Review the report and close the browser when finished.



Snapshot Comparison

Description: Compare the difference of target snaphots.

Snapshot Comparison Status:Snapshot comparison report was generated successfully.

Comparison report generation time:Sat, 20-Sep-2003, 10:09 AM BST

Select a link to view the report

Text Output

HTML Output

PDF Output

CSV Output

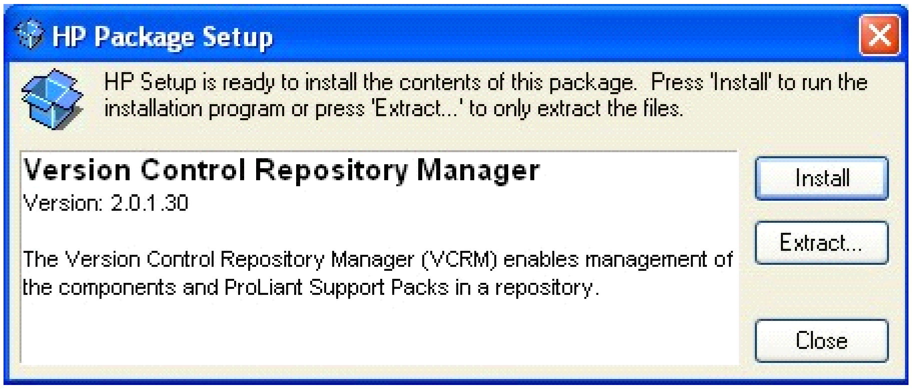
Exercise 5 — Deploying software to managed systems

You can configure software updates such as HP ProLiant Support Packs (PSPs) to deploy to multiple systems managed by Systems Insight Manager. This requires installing Version Control Repository Manager (VCRM) on a network server and specifying the repository that stores the PSPs within Systems Insight Manager.

Installing VCRM on the CMS

To install VCRM:

1. Insert the HP Management CD into the CD-ROM drive of your server. If the CD does not autorun, navigate to the VCRep directory and execute the package file.
2. Click *Version Control Repository Manager* in the left-hand pane and then *Install Version Control Repository Manager* at the bottom of the left-hand pane. Alternatively, use the soft pack provided by your instructor.
3. The HP Package Setup dialog box displays the Version Control Repository Manager version number. Click *Install*.



HP Setup is ready to install the contents of this package. Press 'Install' to run the installation program or press 'Extract...' to only extract the files.

Version Control Repository Manager

Version: 2.0.1.30

The Version Control Repository Manager (VCRM) enables management of the components and ProLiant Support Packs in a repository.

4. Accept the End-User License Agreement and click *Next*.
5. On the Version Control Repository Manager Setup Repository Directory dialog box, accept the default repository location and click *Next*.
6. On the Automatic Updates dialog box, do not select *Enable Automatic Update*. Click *Finish*.
7. A dialog box displays confirming the installation was successful. Click *Close*.

Configuring VCRM and updating the catalog

In this exercise, you will add software to the repository so that it is available for deployment tasks.

1. On the Systems Insight Manager Home page, select *Options* → *Version Control Repository*. At this point there are no available repositories.
2. Click the *Configure* link in the Trusted? column of the list of repositories. The Options page opens.

Note

If a pop-up message indicates that the page is only supported in the integrated user interface, click *OK*. The System Management Homepage for the device displays. Then click the *Settings* tab and the *Options* link under HTTP Server.

---

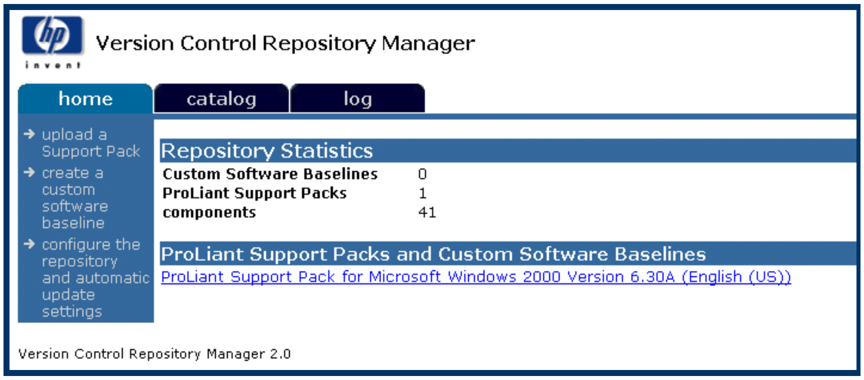
3. Scroll down the page and view the options available. This page allows the configuration of access to the local console, IP restrictions, trust modes, and certificate management.
4. Ensure that *Trust All* is selected and close the *Options* window.

Note

Configuring *Trust All* is not an appropriate setting for a production environment.

---

5. On the Systems Insight Manager Home page, select *Tools* → *System Information* → *System Page*.
6. Verify that your machine is the target and click *Run Now*.
7. Click the *Links* tab and then the *Version Control Repository Manager* link. The Version Control Repository Manager page opens.


invent
Version Control Repository Manager
home
catalog
log
upload a Support Pack
create a custom software baseline
configure the repository and automatic update settings

Repository Statistics

Custom Software Baselines	0
ProLiant Support Packs	1
components	41

ProLiant Support Packs and Custom Software Baselines

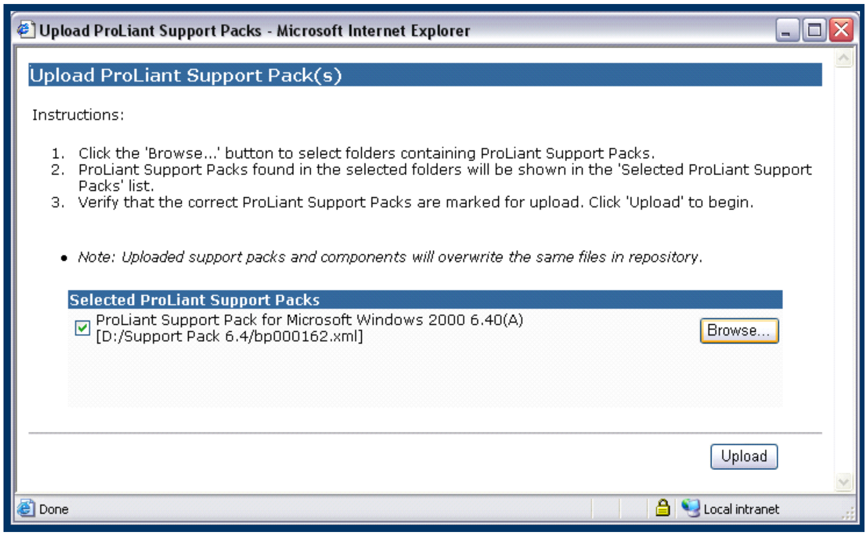
ProLiant Support Pack for Microsoft Windows 2000 Version 6.30A (English (US))

Version Control Repository Manager 2.0

Populate the repository

After a repository has been created, it must be populated with PSPs and components before deploying software to the target HP systems.

1. Insert the SmartStart CD into the CD-ROM drive on the CMS. If the autorun application starts, close the window.
2. Click the *upload a Support Pack* link on the Version Control Repository Manager page.
3. A security warning prompts you to install the support pack upload control. Click *Yes*.
4. On the *Upload ProLiant Support Pack(s)* page, click *Browse* and navigate to the Support Pack (*D:\Compaq\csp\NT* in Smart Start 7.0). Select the check box to identify the support pack to be uploaded and click *OK*. The support pack displays in the Selected ProLiant Support Packs list.



Upload ProLiant Support Pack(s)

Instructions:

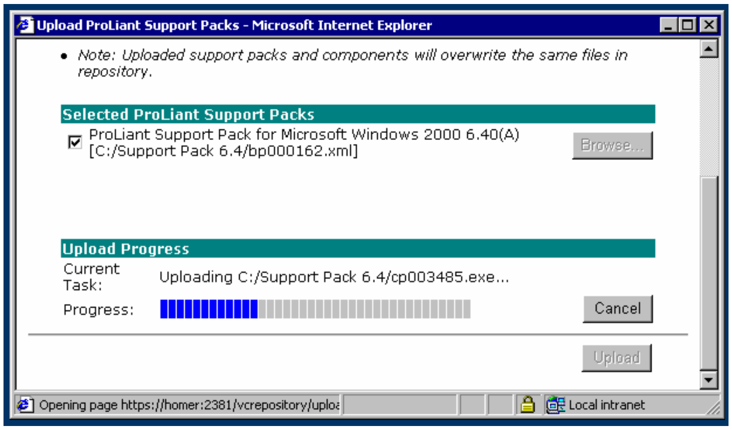
1. Click the 'Browse...' button to select folders containing ProLiant Support Packs.
2. ProLiant Support Packs found in the selected folders will be shown in the 'Selected ProLiant Support Packs' list.
3. Verify that the correct ProLiant Support Packs are marked for upload. Click 'Upload' to begin.

- *Note: Uploaded support packs and components will overwrite the same files in repository.*

Selected ProLiant Support Packs

☑ ProLiant Support Pack for Microsoft Windows 2000 6.40(A)
[D:/Support Pack 6.4/bp000162.xml]

5. Click the *Upload* button to upload the support pack. When the support pack upload is finished, click *Close*.



Upload ProLiant Support Packs - Microsoft Internet Explorer

- *Note: Uploaded support packs and components will overwrite the same files in repository.*

Selected ProLiant Support Packs

☑ ProLiant Support Pack for Microsoft Windows 2000 6.40(A) [C:/Support Pack 6.4/bp000162.xml]

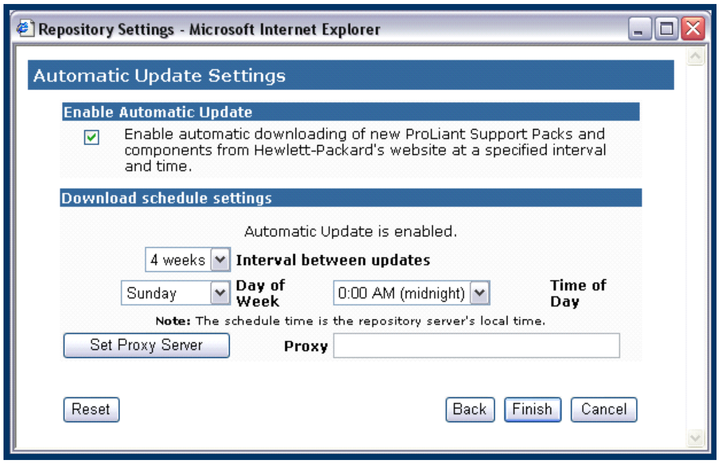
Upload Progress

Current Task: Uploading C:/Support Pack 6.4/cp003485.exe...

Progress:

Opening page https://homer:2381/vcrepository/uploa

6. On the Version Control Repository Manager page, click the *Catalog* tab. Click *Rescan the repository and rebuild the catalog*. Click *Yes* in the confirmation box. Notice that the new support pack is included in the support pack list.
7. Click the *Home* tab. Click *configure the repository and automatic update settings*. Then click *Next*.
8. Select the *Enable Automatic Update* checkbox. This screen displays the current settings used for automatic repository updates.



Repository Settings - Microsoft Internet Explorer

Automatic Update Settings

Enable Automatic Update

☑ Enable automatic downloading of new ProLiant Support Packs and components from Hewlett-Packard's website at a specified interval and time.

Download schedule settings

Automatic Update is enabled.

Interval between updates: 4 weeks

Day of Week: Sunday

Time of Day: 0:00 AM (midnight)

Note: The schedule time is the repository server's local time.

Proxy:

9. Change the interval between updates to once per week and schedule each update for Sunday at 3:00 AM local time.
10. Notice that you can configure automatic downloads of support packs from the HP website. Click *Finish*.
11. Close the Version Control Repository Manager window.

Creating a new software status polling task

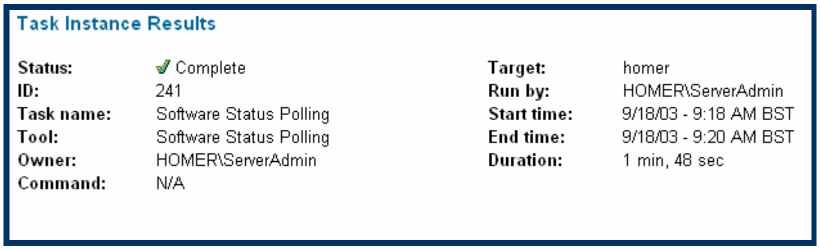
In this exercise, you will configure a software status polling task to retrieve the version numbers of the installed HP software from the Version Control Agent (VCA) on the specified devices.

Note

This process is performed automatically at discovery time and when a Data Collection task or Software Status Polling task runs against the device. There is a predefined Software Version Status Polling task that runs on all discovered servers weekly.

---

1. On the Systems Insight Manager Home page, select *Options* → *Status Polling* → *Software Status Polling*.
2. Ensure that your server is the target system (if it is not the target system, click *Change Targets* and select your system).
3. Click *Run Now*. Review the *Task Results* list to ensure that the task completed successfully. (This task might take a minute to complete.)



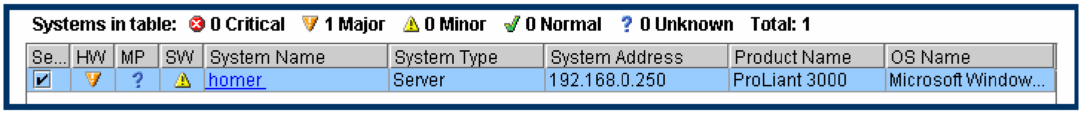
Task Instance Results

Status:	✓ Complete	**Target:**	homer
ID:	241	**Run by:**	HOMER\ServerAdmin
Task name:	Software Status Polling	**Start time:**	9/18/03 - 9:18 AM BST
Tool:	Software Status Polling	**End time:**	9/18/03 - 9:20 AM BST
Owner:	HOMER\ServerAdmin	**Duration:**	1 min, 48 sec
Command:	N/A		

4. Select *Tools* → *System Information* → *System Page*.
5. Click *Run Now* if your system is the target system, or click *Change Targets* and select your system.
6. On the System Page, click the *Links* tab and then the *Version Control Agent* link. The Version Control Agent page displays. Take note of the version number for the Management Agents for Windows.

....

7. To view the software status of all systems, click the *All Systems* link in *System Lists*. The SW column shows the status of software on the system. Click the icon in the SW column to see details.



Systems in table: ⊗ 0 Critical ▼ 1 Major ⚠ 0 Minor ✓ 0 Normal ? 0 Unknown Total: 1

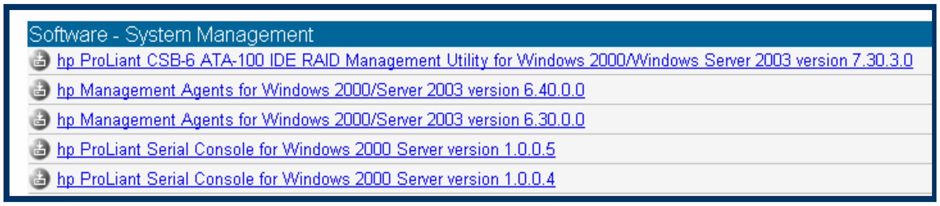
Se...	HW	MP	SW	System Name	System Type	System Address	Product Name	OS Name
☑	▼	?	⚠	homer	Server	192.168.0.250	ProLiant 3000	Microsoft Window...

8. Close all VCA browsers when finished.

Using the VCA to upgrade the HP Management Agents

In this exercise, you will use the VCA to upgrade the version of the HP Management Agents installed on the system.

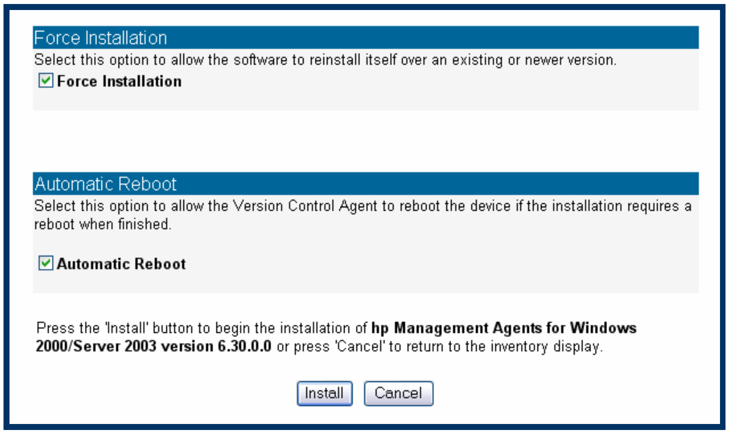
1. Click the *All Systems* list and then the *SW* icon for your server. The Version Control Agent page displays showing a list of installed software.
2. Click *Show additional items available in the Repository*.
3. Scroll down the page to the Available Software. This is a list of software available on the VCRM. Scroll down the list to the Software – System Management section. Click the link for the slightly newer version of the HP Management Agents and review the information available. Then click the *Back* button in your browser.



Software - System Management

- hp ProLiant CSB-6 ATA-100 IDE RAID Management Utility for Windows 2000/Windows Server 2003 version 7.30.3.0
- hp Management Agents for Windows 2000/Server 2003 version 6.40.0.0
- hp Management Agents for Windows 2000/Server 2003 version 6.30.0.0
- hp ProLiant Serial Console for Windows 2000 Server version 1.0.0.5
- hp ProLiant Serial Console for Windows 2000 Server version 1.0.0.4

4. To begin the installation, click the gray *install/update* icon to the left of the HP Management Agents for Windows 2000 server link.
5. Select *Force Installation* and *Automatic Reboot*. Click *Install*.



Force Installation

Select this option to allow the software to reinstall itself over an existing or newer version.

☑ **Force Installation**

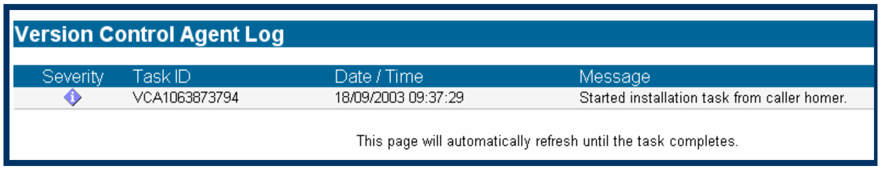
Automatic Reboot

Select this option to allow the Version Control Agent to reboot the device if the installation requires a reboot when finished.

☑ **Automatic Reboot**

Press the 'Install' button to begin the installation of **hp Management Agents for Windows 2000/Server 2003 version 6.30.0.0** or press 'Cancel' to return to the inventory display.

6. Notice the messages that display. The Version Control Agent Log page automatically tracks the installation process and updates messages. When the installation is complete, click the *Details* link and review the information provided.



Version Control Agent Log

Severity	Task ID	Date / Time	Message
ℹ	VCA1063873794	18/09/2003 09:37:29	Started installation task from caller homer.

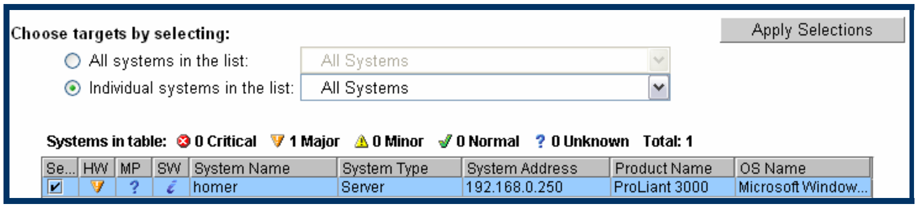
This page will automatically refresh until the task completes.

7. Return to the Version Control Agent page and refresh the browser. Review the version number for the HP Management Agents. It should now be the new version. Close the VCA browser when you are finished.

Deploying a PSP with a task

In this exercise, you will configure Systems Insight Manager to deploy a PSP for Windows 2000. This method is used primarily for systems not running the VCA.

1. From the Systems Insight Manager Home page, click *Deploy* → *Deploy Drivers, Firmware and Agents* → *Initial ProLiant Support Pack Install*. Ensure that your system is the target.
2. On the Install ProLiant Support Pack page, select *Individual systems in the list* and then select *All Servers* from the drop-down list. Highlight your partner’s server in the list and click *Apply Selections*. Then click *Next*.



Choose targets by selecting:

○ All systems in the list: All Systems

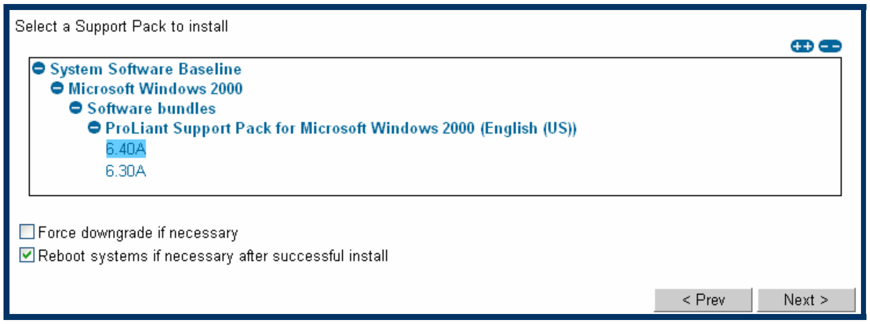
● Individual systems in the list: All Systems

Systems in table: 0 Critical 1 Major 0 Minor 0 Normal 0 Unknown Total: 1

Se...	HW	MP	SW	System Name	System Type	System Address	Product Name	OS Name
☑	▽	?	ℹ	homer	Server	192.168.0.250	ProLiant 3000	Microsoft Window...

3. Enter *ServerAdmin* and *password* on the Enter Windows Logon Credentials page. Click *Next*.

4. On the Select a Support Pack to install page, select a Version Control Repository other than your own, expand the list of available software, and select the slightly newer *ProLiant Support Pack for Microsoft Windows 2000 (English (US))*. Click *Next*.



Select a Support Pack to install

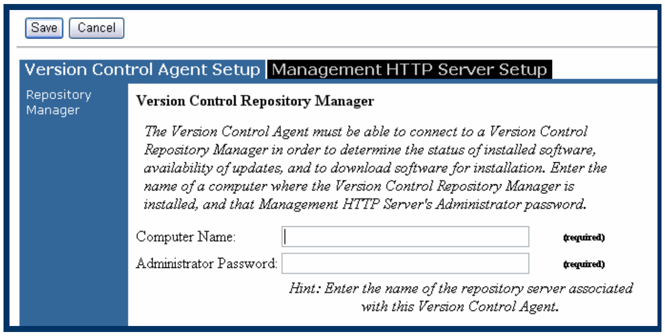
- System Software Baseline
  - Microsoft Windows 2000
    - Software bundles
      - ProLiant Support Pack for Microsoft Windows 2000 (English (US))
        - 6.40A
        - 6.30A

☐ Force downgrade if necessary

☑ Reboot systems if necessary after successful install

5. On the Configure Support Pack page, click *Configure Support Pack*. The Version Control Agent Setup box displays.

6. Enter the name of your machine in the Computer Name field and *password* in the Administrator Password field. Click *Save*.



Version Control Repository Manager

The Version Control Agent must be able to connect to a Version Control Repository Manager in order to determine the status of installed software, availability of updates, and to download software for installation. Enter the name of a computer where the Version Control Repository Manager is installed, and that Management HTTP Server's Administrator password.

Computer Name: (required)

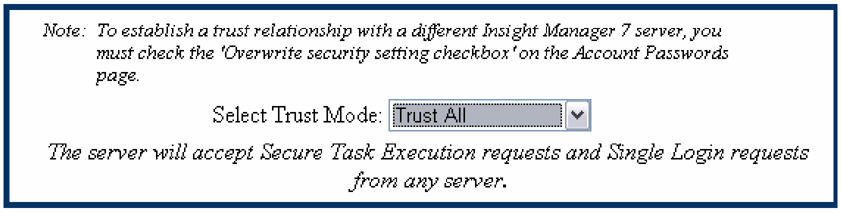
Administrator Password: (required)

Hint: Enter the name of the repository server associated with this Version Control Agent.

7. If a message displays indicating that the HTTP Management password is not set, click *OK*. The Management HTTP Server Setup box displays.

8. Enter *password* as the administrator password and leave the other fields blank. Click *Save*.

9. If a message regarding a trust certificate displays, click *OK*.
10. In the Trust Relationship box, select *Trust All* and then click *Save*.

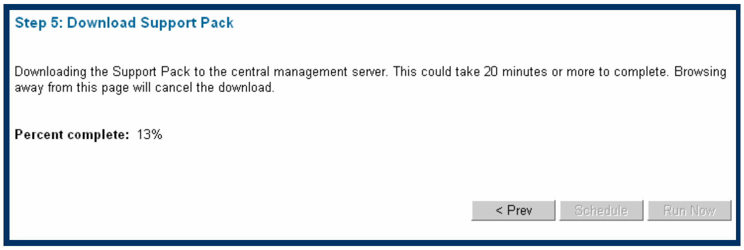


Note: To establish a trust relationship with a different Insight Manager 7 server, you must check the 'Overwrite security setting checkbox' on the Account Passwords page.

Select Trust Mode: Trust All

The server will accept Secure Task Execution requests and Single Login requests from any server.

11. The Component Configuration box displays. Click *Close*.
12. The Support Pack begins downloading. Notice the Percent complete figure. Also notice the message regarding browsing away from the page.

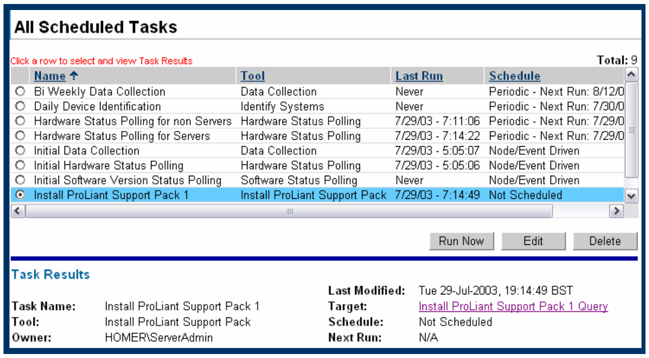


Step 5: Download Support Pack

Downloading the Support Pack to the central management server. This could take 20 minutes or more to complete. Browsing away from this page will cancel the download.

Percent complete: 13%

13. After the download is finished, you can schedule the deployment for a later time or click *Run Now*.
14. For this exercise, click *Run Now* and then click *Done*. The All Scheduled Tasks page displays information about the task.



All Scheduled Tasks

Click a row to select and view Task Results

Total: 9

	Name	Tool	Last Run	Schedule
○	Bi Weekly Data Collection	Data Collection	Never	Periodic - Next Run: 8/12/0
○	Daily Device Identification	Identify Systems	Never	Periodic - Next Run: 7/30/0
○	Hardware Status Polling for non Servers	Hardware Status Polling	7/29/03 - 7:11:06	Periodic - Next Run: 7/29/0
○	Hardware Status Polling for Servers	Hardware Status Polling	7/29/03 - 7:14:22	Periodic - Next Run: 7/29/0
○	Initial Data Collection	Data Collection	7/29/03 - 5:05:07	Node/Event Driven
○	Initial Hardware Status Polling	Hardware Status Polling	7/29/03 - 5:05:06	Node/Event Driven
○	Initial Software Version Status Polling	Software Status Polling	Never	Node/Event Driven
●	Install ProLiant Support Pack 1	Install ProLiant Support Pack	7/29/03 - 7:14:49	Not Scheduled

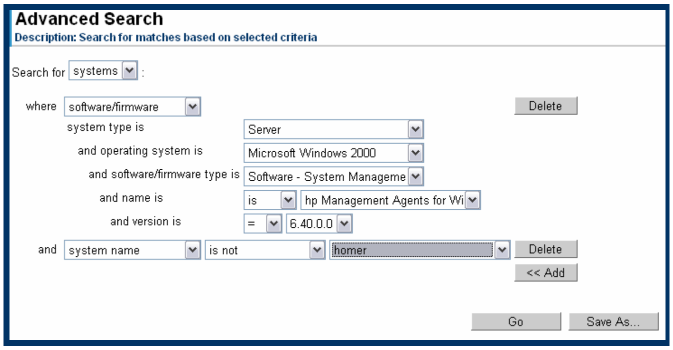
Task Results

Last Modified: Tue 29-Jul-2003, 19:14:49 BST
Task Name: Install ProLiant Support Pack 1
Target: Install ProLiant Support Pack 1 Query
Tool: Install ProLiant Support Pack
Schedule: Not Scheduled
Owner: HOMER\ServerAdmin
Next Run: N/A

Deploying software to multiple systems

In this exercise, you will create a query that will include multiple servers dynamically and upgrade the software on each server automatically.

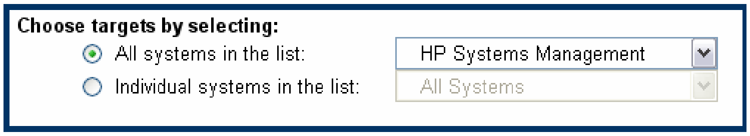
1. On the Systems Insight Manager Home page, click *Advanced Search*. Create a search for systems with the new version of the management agents, but only include your own system. Then click *Save As*.



Advanced Search
Description: Search for matches based on selected criteria

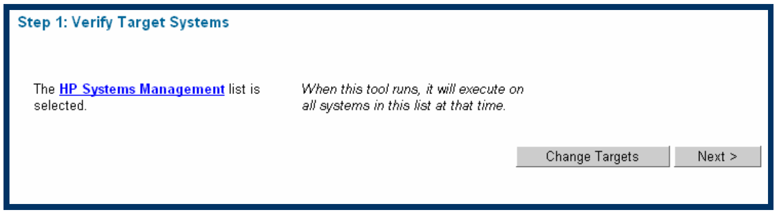
Search for systems :
where software/firmware
system type is Server
and operating system is Microsoft Windows 2000
and software/firmware type is Software - System Manageme
and name is is hp Management Agents for Wi
and version is = 6.40.0.0
and system name is not homer

2. In the Save As List section, enter *HP Systems Management* as the name for the list. Select the *New Folder* radio button and name the new folder *Software*. Click *OK*.
3. Select *Deploy* → *Deploy Drivers, Firmware and Agents* → *Install Software and Firmware*.
4. On the Select Target Systems page, select the *All systems in the list* radio button and then select the *HP Systems Management* list.



Choose targets by selecting:
● All systems in the list: HP Systems Management
○ Individual systems in the list: All Systems

5. Click *Apply Selections*. The Verify Target Systems page indicates that the *HP Systems Management* list is selected. Click *Next*.



Step 1: Verify Target Systems

The HP Systems Management list is selected.

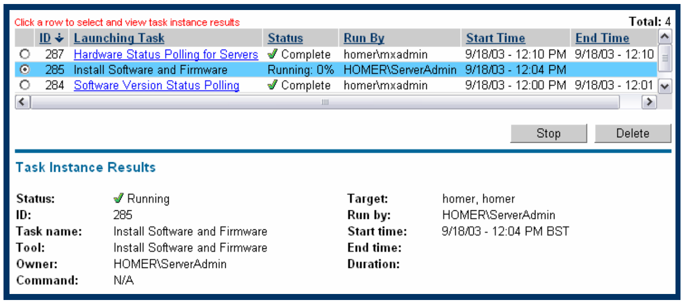
When this tool runs, it will execute on all systems in this list at that time.

6. On the *Select Items to Install* screen, select a Version Control Repository other than your own, then select *Server* → *Microsoft Windows 2000* → *Software — Systems Management* and select the newest management agents. Click *Next*.
7. On the *Select Install Options* screen, select the management agents in the list and click *Run Now*. The Task List displays with the task running.

Verifying software deployment

In this exercise, you will view the task list to verify the results of the software deployment performed in the previous exercise.

1. Select *Logs* → *View Task Results*.



Click a row to select and view task instance results

Total: 4

	ID	Launching Task	Status	Run By	Start Time	End Time
○	287	Hardware Status Polling for Servers	✓ Complete	homer\mxadmin	9/18/03 - 12:10 PM	9/18/03 - 12:10
●	285	Install Software and Firmware	Running: 0%	HOMER\ServerAdmin	9/18/03 - 12:04 PM	
○	284	Software Version Status Polling	✓ Complete	homer\mxadmin	9/18/03 - 12:00 PM	9/18/03 - 12:01

Task Instance Results

Status:	✓ Running	**Target:**	homer, homer
ID:	285	**Run by:**	HOMER\ServerAdmin
Task name:	Install Software and Firmware	**Start time:**	9/18/03 - 12:04 PM BST
Tool:	Install Software and Firmware	**End time:**	
Owner:	HOMER\ServerAdmin	**Duration:**	
Command:	N/A		

2. Highlight the task in the list and view the results that display below the table. You should see that the task status is complete with a start and end time. You have now installed the latest management agents to both machines.

Security

Lab 3

Objectives

After completing this lab, you should be able to:

- Determine the most secure location for a server
- Perform a risk analysis
- Configure the HP Systems Insight Manager security and replicate agent settings

Requirements

To perform this lab, you need an HP ProLiant server with the following components installed:

- Microsoft Windows 2000 Server or Advanced Server SP3 or later with Systems Insight Manager
- TCP/IP and Simple Network Management Protocol (SNMP)
- Microsoft Internet Explorer 6.0 or later
- Monitor capable of supporting a resolution of 1024 x 768 with 16-bit colors
- One crossover network cable

Introduction

Security must be one of an enterprise's most dependable policies. As an HP Accredited Systems Engineer (ASE), you possess the expertise to help RC Engineering implement the appropriate security measures, helping to ensure the company's data integrity and privacy.

RC Engineering is shipping servers and other networking equipment from their Silicon Valley location to corporate headquarters in Houston, Texas. Bob, the CEO, has asked for your help determining the most secure location for this equipment. After surveying the Houston site with Jackie, the IT manager, you make your recommendations based on HP and industry best practices.

After determining where to place the servers, you work with Jackie to evaluate the risks the company remains vulnerable to. Based on her answers to the questions you ask, Jackie will be able to formulate an approach to minimizing the company's exposure to risk. The results of both these sessions will be documented and will become part of the RC Engineering information security policy.

You will then use Systems Insight Manager to configure security for the company's network. First you will configure web agent settings. Then you will import the Systems Insight Manager certificate, change the trust mode, and replicate the agent settings.

Exercise 1 — Determining the most secure location for a server

! **Important**

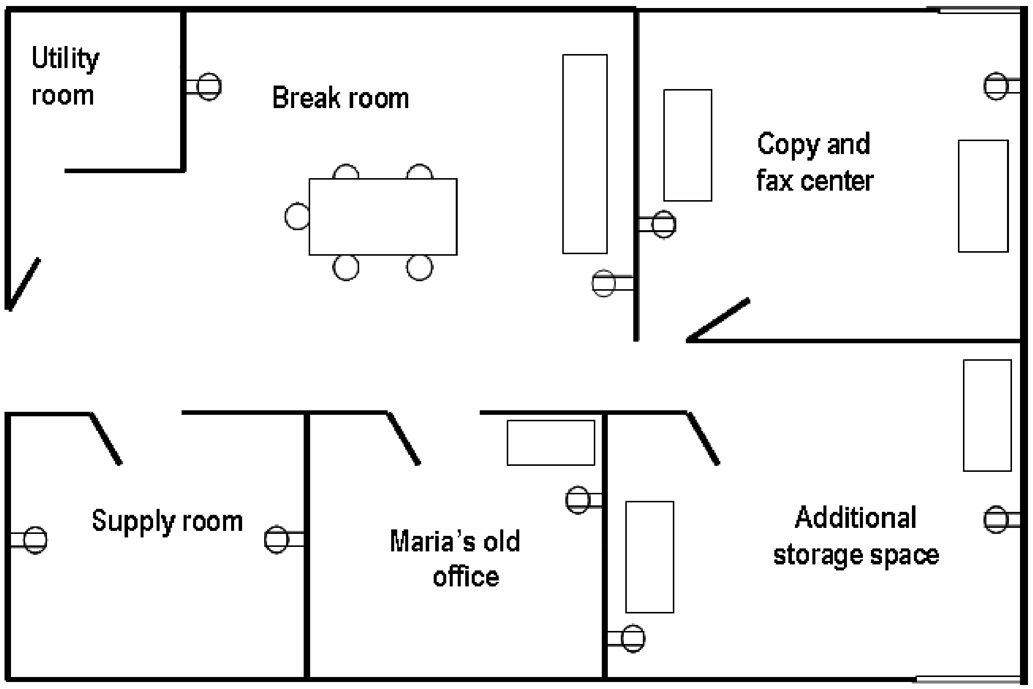
In order to assume the role of Bob, your instructor or another student must read Synopsis 1 — RC Engineering's headquarters in the Interview Guide in Appendix C before beginning this exercise.

The primary goal for secure placement of networking equipment should be to control access to all areas containing servers, website hardware, firewalls, and other equipment. After touring the site where RC Engineering plans to house its essential networking equipment, you make a note of any security vulnerabilities that impact placement of the equipment. These vulnerabilities can include:

- Uninformed and noncompliant employees
- Users who are unaware of their surroundings and allow their passwords to be "shoulder surfed"
- Using cell phones and text pagers to distribute passwords or other sensitive information

Jackie informs you that her company does not have formal information security policy documentation. Usually, security related issues are communicated to employees through informal email memos. The lack of security policy documentation amplifies security vulnerabilities, as new employees—unaware of the previously communicated security issues—join the company.

RC E



The preceding graphic illustrates the layout of the RC Engineering offices in the Houston headquarters. After your instructor or another student has read the Interview Guide, you must create a list of questions for Bob. The following questions are examples of the kind of questions you might want to ask.

1. How is access to the building controlled?

   ....

2. Are there guards at building entrances?

   ....

3. Are badges worn by employees?

   ....

4. What is the procedure for visitor sign-in?

   ....

5. Is any security training offered to employees, including secretaries and receptionists?

   ....

6. Are the rooms which contain high-level equipment such as servers, workstations, tapes, and hard drives kept locked at all times?

   ....

7. Are coat tags or swipe cards required for entry into secure rooms?

   ....

8. Who has access to the server room?

   ....

9. Are there any public computers or computers that do not require a password at the facility?

   ....

10. Is there a way to access any office without using a door or window?

    ....

What additional questions would you ask Bob?

....

....

....

....

....

Based on the information you have received, what recommendations and considerations would you present to Bob for improving security?

....

....

....

....

....

....

....

Exercise 2 — Performing a risk analysis

! **Important**

In order to assume the role of Jackie, your instructor or another student must read Synopsis 2 — RC Engineering's security practices in the Interview Guide in Appendix C before beginning this exercise.

Your next step in implementing a security plan at RC Engineering is to perform a risk analysis. In order to do this, you must interview Jackie, the IT manager. Possible questions to ask Jackie include:

1. What IT security policies does RC Engineering currently document?

   ....

2. What roles do the key stakeholders play in ensuring compliance?

   ....

3. What resources are committed to securing the enterprise?

   ....

4. How would a security breach impact the business?

   ....

5. What type of Information Security Policy, if any, is presently in place?

   ....

6. Have any authorizing documents been issued from management?

   ....

7. What type of federal, state, or local statutory regulations affect RC Engineering?

   ....

8. How often are passwords changed?

   ....

9. What are the restrictions regarding passwords (length, special characters, and so forth)?

   ....

10. What security failure would cause the most harm?

    ....

11. Have security probes or intrusion tests ever been performed on the enterprise?

    ....

12. Describe the users that access RC Engineering systems and their access privileges.

    ....

13. How are security awareness and compliance measured?

    ....

14. Does the IT staff routinely perform audits of the enterprise and all of its systems?

    ....

15. How are the results analyzed and who performs the analysis?

    ....

16. Does RC Engineering use any forms of encryption?

    ....

17. Do contractors have access to the company intranet?

    ....

18. Is there any type of written and signed security policy in place with contractors?

    ....

19. What file systems are used in the enterprise?

    ....

List five additional questions that would assist you in performing a detailed risk analysis.

....

....

....

....

....

Based on this information, what would be your recommendations for Jackie?

....

....

....

....

....

....

Exercise 3 — Configuring security for Systems Insight Manager

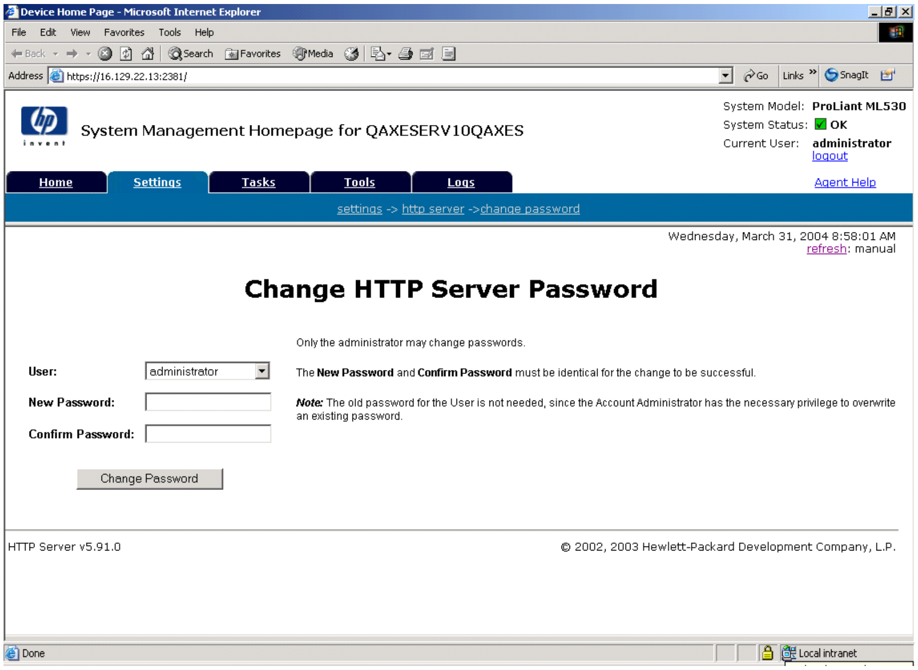
A typical enterprise environment has numerous devices. It is easier to manage those devices by sharing common passwords, configuration information, and certificates of trusted Systems Insight Manager servers. After configuring agent settings on your central management server (CMS), you will replicate these settings to the remote server in your student set.

Configuring web agent settings

To access the agent settings on the CMS, you must access the System Management Homepage on the server.

1. Open a browser window on the CMS and enter *https://machine:2381* in the address bar, where *machine* is the IP address of the target server or the computer Domain Name Service (DNS) name.
2. From the Systems Management Homepage, click the *Settings* tab.
3. From the HTTP Server section, click *Change Password*. The Change HTTP Server Password screen displays. In an enterprise environment, the web agent password should be consistent for managed systems to facilitate management of multiple systems.

   In the New Password and Confirm Password fields, enter *password123*. Click *Change Password* to save your new password.


Device Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links SnagIt
Home Settings Tasks Tools Logs
Agent Help
Done
Local intranet

https://16.129.22.13:2381/

System Management Homepage for QAXESERV10QAXES

System Model: **ProLiant ML530**
System Status: **OK**
Current User: **administrator**
logout

settings -> http server ->change password

Wednesday, March 31, 2004 8:58:01 AM
refresh: manual

Change HTTP Server Password

Only the administrator may change passwords.

The **New Password** and **Confirm Password** must be identical for the change to be successful.

Note: The old password for the User is not needed, since the Account Administrator has the necessary privilege to overwrite an existing password.

User: administrator
New Password:
Confirm Password:

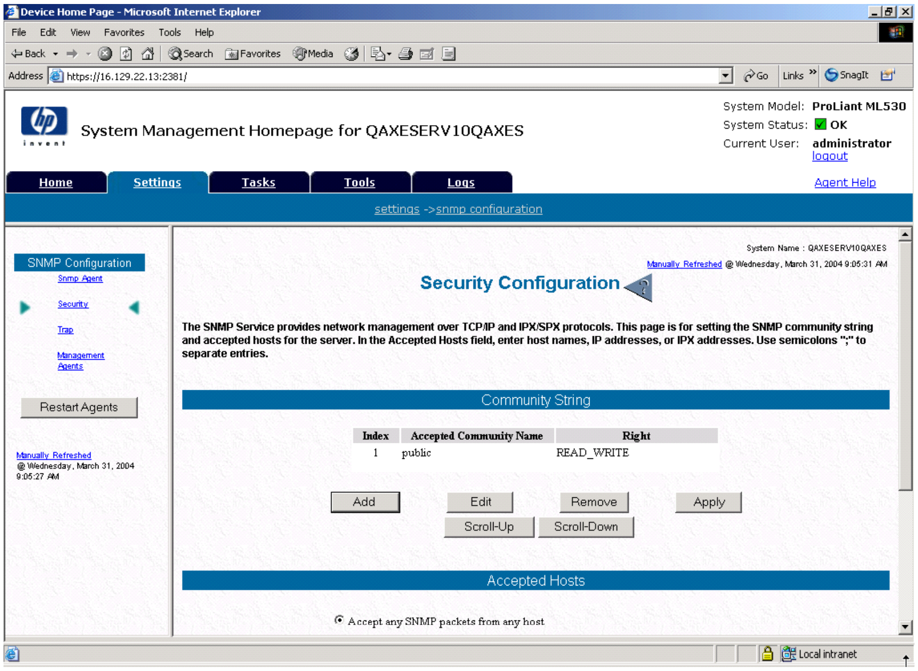
Change Password

HTTP Server v5.91.0

© 2002, 2003 Hewlett-Packard Development Company, L.P.

4. Click the *Settings* tab. Because you changed the password, the community string must be modified to have consistency in the environment. Click *SNMP Configuration*. From the SNMP Configuration section, click *Security*.

5. From the Security Configuration screen, click *Add*. The HP Group Configuration GUI window displays.


Device Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://16.129.22.13:2381/
Go Links SnagIt
System Management Homepage for QAXESERV10QAXES
Home Settings Tasks Tools Logs
Agent Help
settings ->snmp configuration
SNMP Configuration
Snmp Agent
Security
Trap
Management Agents
Restart Agents
Community String
Add Edit Remove Apply
Scroll-Up Scroll-Down
Accepted Hosts
Local intranet

System Model: **ProLiant ML530**
System Status: ✓ **OK**
Current User: **administrator**
logout

Manually Refreshed @ Wednesday, March 31, 2004 9:05:27 AM

System Name : QAXESERV10QAXES
Manually Refreshed @ Wednesday, March 31, 2004 9:05:31 AM

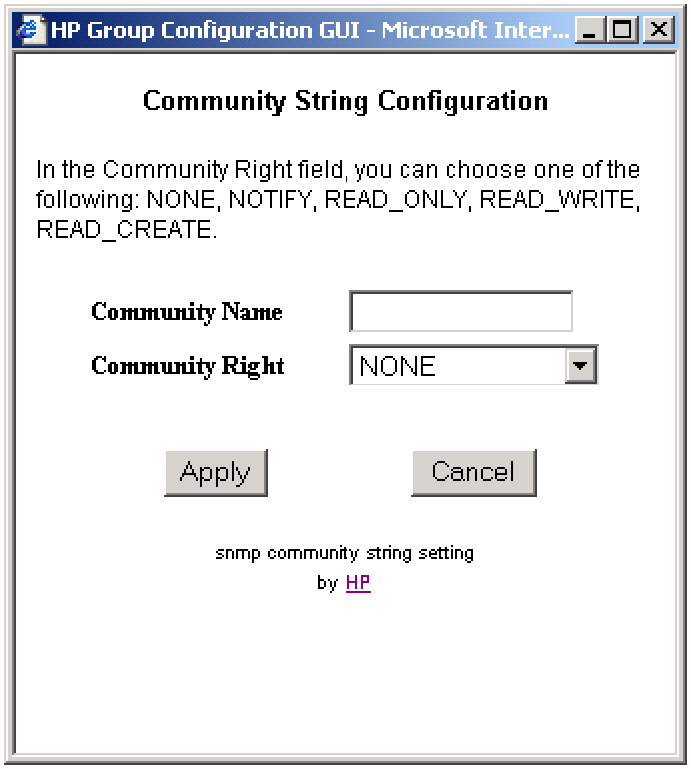
Security Configuration

The SNMP Service provides network management over TCP/IP and IPX/SPX protocols. This page is for setting the SNMP community string and accepted hosts for the server. In the Accepted Hosts field, enter host names, IP addresses, or IPX addresses. Use semicolons ";" to separate entries.

Index	Accepted Community Name	Right
1	public	READ_WRITE

● Accept any SNMP packets from any host

6. In the Community Name field, enter *public1*. From the Community Right drop-down menu, select *READ_ONLY*. Click *Apply* to confirm your changes.



Community String Configuration

In the Community Right field, you can choose one of the following: NONE, NOTIFY, READ_ONLY, READ_WRITE, READ_CREATE.

Community Name

Community Right NONE

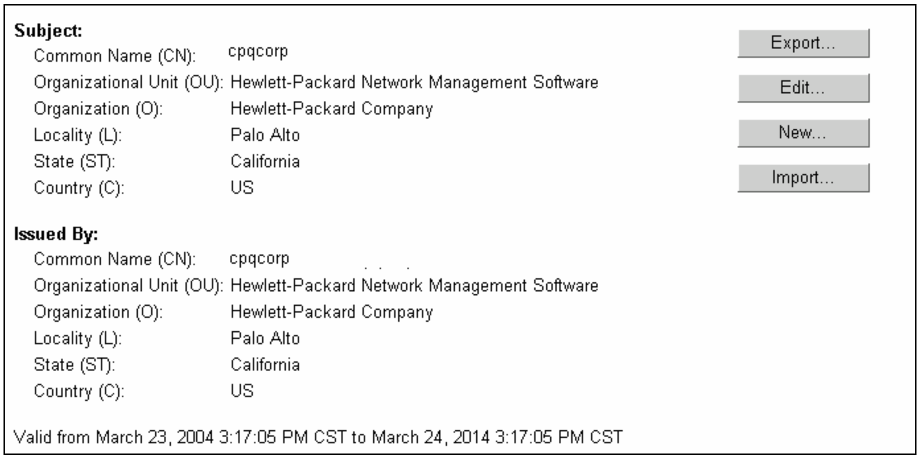
snmp community string setting
by HP

7. Return to the Security Configuration screen. Click *Apply* in the Community String section to save your changes.
8. Click *logout* and exit the browser window.

Importing the Systems Insight Manager certificate

To view the certificate for your server and use the enable the Trust by Certificate option, perform the following steps:

1. Launch Systems Insight Manager.
2. From the HP Systems Insight Manager Home page, click *Options* → *Security* → *Certificates* → *Server Certificate*. The Server Certificate screen displays. From this window, you can view and manage the information for the Secure Sockets Layer (SSL) server certificate.



Subject:

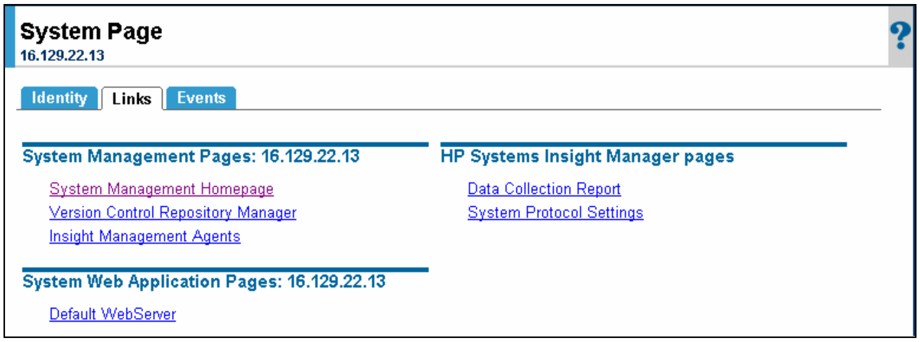
Common Name (CN): cpqcorp
Organizational Unit (OU): Hewlett-Packard Network Management Software
Organization (O): Hewlett-Packard Company
Locality (L): Palo Alto
State (ST): California
Country (C): US

Issued By:

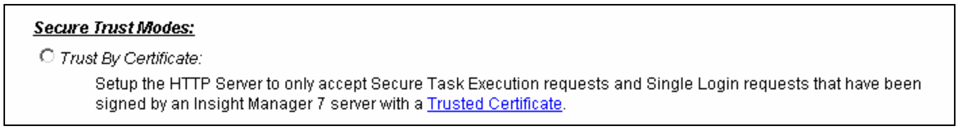
Common Name (CN): cpqcorp
Organizational Unit (OU): Hewlett-Packard Network Management Software
Organization (O): Hewlett-Packard Company
Locality (L): Palo Alto
State (ST): California
Country (C): US

Valid from March 23, 2004 3:17:05 PM CST to March 24, 2014 3:17:05 PM CST

3. From the menu bar, select *Tools* → *System Information* → *System Page*. Ensure that your system is the target device and click *Run Now*. Review the detailed information.
4. From the System Page, click the *Links* tab and select the *Systems Management Homepage* link. The Device Home Page window displays.


System Page
16.129.22.13
?
Identity
Links
Events
System Management Pages: 16.129.22.13
System Management Homepage
Version Control Repository Manager
Insight Management Agents
System Web Application Pages: 16.129.22.13
Default WebServer
HP Systems Insight Manager pages
Data Collection Report
System Protocol Settings

5. From the Systems Management Homepage, click the *Settings* tab.
6. In the HTTP server section, click *Options*.
7. From the Options screen, locate the Trust Mode options. In the Secure Trust Modes section, select the *Trust By Certificate* radio button.

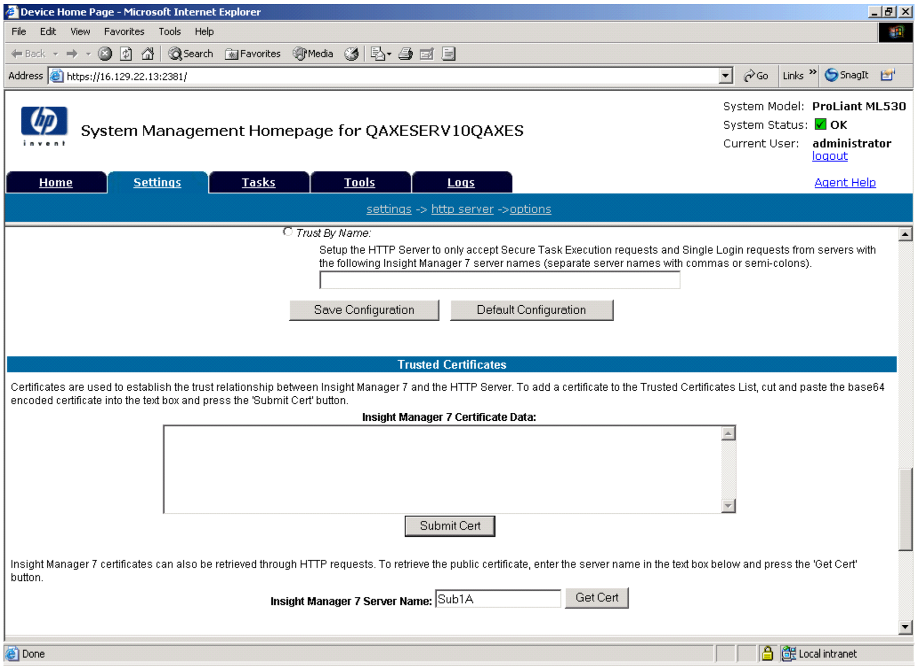


Secure Trust Modes:

○ *Trust By Certificate:*

Setup the HTTP Server to only accept Secure Task Execution requests and Single Login requests that have been signed by an Insight Manager 7 server with a Trusted Certificate.

8. From the Options screen, locate the *Trusted Certificates* section. In the Insight Manager 7 Server Name field, enter the name of the CMS. Click *Get Cert*.



Address: https://16.129.22.13:2381/

System Management Homepage for QAXESERV10QAXES

System Model: ProLiant ML530
System Status: OK
Current User: administrator

settings -> http server ->options

○ *Trust By Name:*

Setup the HTTP Server to only accept Secure Task Execution requests and Single Login requests from servers with the following Insight Manager 7 server names (separate server names with commas or semi-colons).

Trusted Certificates

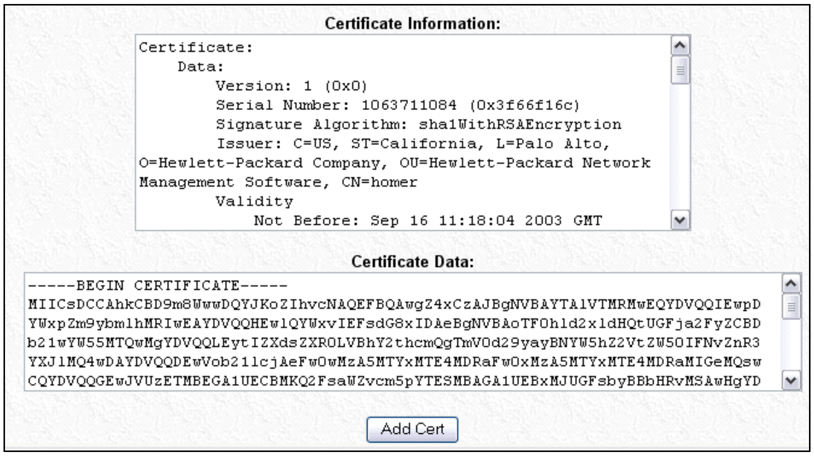
Certificates are used to establish the trust relationship between Insight Manager 7 and the HTTP Server. To add a certificate to the Trusted Certificates List, cut and paste the base64 encoded certificate into the text box and press the 'Submit Cert' button.

Insight Manager 7 Certificate Data:

Insight Manager 7 certificates can also be retrieved through HTTP requests. To retrieve the public certificate, enter the server name in the text box below and press the 'Get Cert' button.

Insight Manager 7 Server Name: Sub1A

9. The *Certificate Information* screen displays. This screen displays the version, serial number, signature name, and base64 encoding of the certificate.



```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1063711084 (0x3f66f16c)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=California, L=Palo Alto,
O=Hewlett-Packard Company, OU=Hewlett-Packard Network
Management Software, CN=homer
        Validity
            Not Before: Sep 16 11:18:04 2003 GMT
```

```
-----BEGIN CERTIFICATE-----
MIICsDCCAhkCBD9m8WwwDQYJKoZIhvcNAQEFBQAwgZ4xCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpD
YWxpZm9ybmlhMRIwEAYDVQQHEwlQYWxvIEFsdG8xIDAeBgNVBAoTF0hld2xldHQtUGFja2FyZCBD
b21wYW55MTQwMgYDVQQLEytIZXdsZXR0LVBhY2thcmQgTmV0d29yayBNYW5hZ2VtZW50IFNvZnR3
YXJlMQ4wDAYDVQQDEwVob21lcjAeFw0wMzA5MTYxMTE4MDRaFw0xMzA5MTYxMTE4MDRaMIGeMQsw
CQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJUGFsbyBBbHRvMSAwHgYD
```

10. Click *Add Cert*. A confirmation page displays stating that the certificate has been added to the trusted list. Close the browser.

Changing the trust mode

1. From the managed server, display the browser window and enter **http://localhost:2381** in the address bar.
2. From the Systems Management Homepage, click the *Settings* tab.
3. From the HTTP Server section, click *Options*.
4. From the Options screen, click *Configuration Options*.
5. Scroll down to the Secure Trust Modes section. Select the *Trust by Certificate* radio button to accept only Secure Task Execution requests and single login requests that have been signed by a Systems Insight Manager server with a Trusted Certificate.

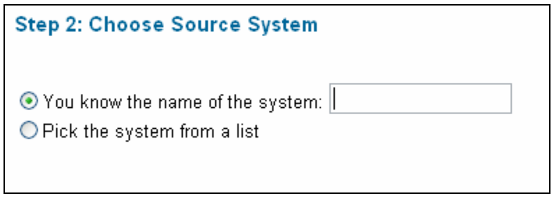
Replicating the agent settings

Systems Insight Manager allows you to copy configuration settings from one server to groups of systems. To replicate agent settings, perform the following steps:

1. From the menu bar of the Systems Insight Manager Home page, select *Configure → Replicate Agent Settings*.
2. From the Replicate Agent Settings screen, verify that your partner's system is the target server. Click *Next*.

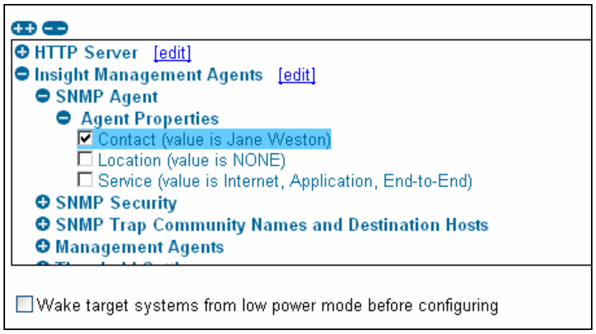
> **Note**
> If your partner's system is not specified, click *Change Targets* and select your partner's system. Locate the Change target by selecting section. Click the *Individual systems in the list* radio button and select *All System* in the drop-down menu. Locate your partner's system and select it. Click the *Apply Changes* button.

3. The Choose Source System section displays. In the You know the name of the system field, enter the name of your server. Click *Next* to continue.


Step 2: Choose Source System
● You know the name of the system:
○ Pick the system from a list

> **Note**
> The target for the replication can be a single system or list.

4. The Choose Source Configuration Settings screen displays an expandable list of possible settings. Expand *Insight Management Agents* → *SNMP Agent* → *Agent Properties* and select the setting you just configured. Click *Run Now*.



HTTP Server [edit]
Insight Management Agents [edit]
  SNMP Agent
    Agent Properties
      ☑ Contact (value is Jane Weston)
      ☐ Location (value is NONE)
      ☐ Service (value is Internet, Application, End-to-End)
  SNMP Security
  SNMP Trap Community Names and Destination Hosts
  Management Agents

☐ Wake target systems from low power mode before configuring

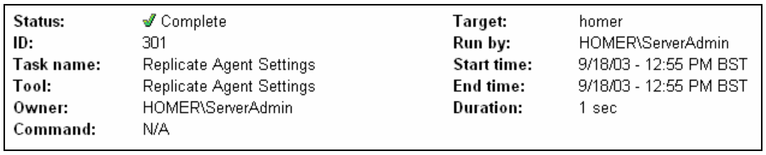
Note

Other useful agent settings to replicate include:

- *HTTP Server → Settings → all Passwords Properties*
- *Configuration Option Properties → Trust Mode*
- *Trusted Certificate Properties → Trusted Certificate*

---

5. The Task List displays confirming that your replication task was successful.



Status:	✓ Complete	**Target:**	homer
ID:	301	**Run by:**	HOMER\ServerAdmin
Task name:	Replicate Agent Settings	**Start time:**	9/18/03 - 12:55 PM BST
Tool:	Replicate Agent Settings	**End time:**	9/18/03 - 12:55 PM BST
Owner:	HOMER\ServerAdmin	**Duration:**	1 sec
Command:	N/A		

Performance management

Lab 4

Objectives

After completing this lab, you should be able to:

- Demonstrate how to use the HP ProLiant Essentials Performance Management Pack (PMP) 2.1, including:
  - Updating the HP Management Agents and the PMP software
  - Licensing monitored servers
  - Configuring the monitoring behavior of PMP
  - Performing static analysis
  - Detecting, analyzing, and resolving performance bottlenecks
  - Logging and manipulating data
  - Configuring performance-based alerts
  - Comparing current performance with baseline performance
  - Removing PMP
- Monitor and tune a database server for the highest performance at the lowest-cost configuration. Specifically, you should be able to:
  - Prepare the network environment by installing the database software and the benchmark suite
  - Monitor and tune the network
- Install the HP Resource Partitioning Manager (RPM) and use it to:
  - Create a resource partition
  - Add a new process to the resource partition
  - Assign rules for a resource partition
  - Capture a non-RPM job object
  - Activate and deactivate a resource partition
  - Remove a resource partition
  - Remotely connect to a target computer

Requirements

To complete the first exercise, you must have HP Insight Manager 7 and PMP 2.1 installed on a server that is part of your lab network.

Note

Although there are plans for future compatibility, PMP currently is not compatible with HP Systems Insight Manager.

The server hosting Insight Manager 7 and PMP must meet the minimum hardware and operating system requirements described in the HP ProLiant Essentials Performance Management Pack Support Matrix. The servers to be monitored must also meet the minimum hardware and operating system requirements described in the HP ProLiant Essentials Performance Management Pack Support Matrix.

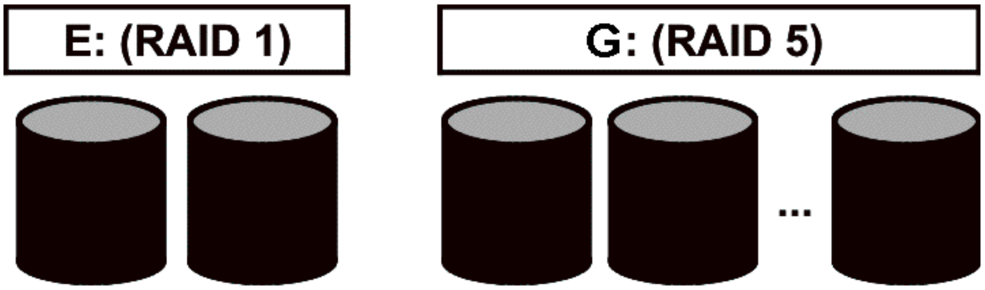
To complete the second exercise, you must have a Microsoft SQL Server 7.0 CD, a TPC-B benchmark kit, and at least one workstation and one server that meet the following requirements:

- Workstation — Any Intel-based workstation with:
  - One 400MHz or faster processor
  - 256MB or more memory
  - 2.1GB or larger hard drive
  - Microsoft Windows 2000 with the latest service pack
  - TCP/IP-based connectivity to the server
  - Microsoft Excel
- Server — Any ProLiant server with:
  - At least two 400MHz or faster processors
  - 512MB or more memory
  - An HP Smart Array controller
  - Five or more 4.3GB hard drives
  - Windows 2000 Advanced Server with the latest service pack

To complete the third exercise, you must have two servers running RPM, with at least one server that meets the following requirements:

- HP Workload Management Pack 2.0 CD
- HP Survey Utility installed

Configuration



Configure the storage subsystem as shown in the preceding graphic. The available space requirements are:

- Drive E: — 1.5GB (250MB for SQL Server binaries and 1.25GB for database files)
- Drive G: — 500MB

> **Note**
> The drive lettering might change according to the configuration of the hardware in your classroom. Ask your instructor for the correct drive assignments.

Introduction

Before you can address the performance issues at RC Engineering, you must determine the management agent version and, if necessary, perform the necessary management agent updates. You also must show Jackie how to license the target servers and configure the performance monitoring infrastructure. After you change the PMP mode of operation to any of the monitoring options, you can begin monitoring performance.

To solve system health and performance issues, you will apply the HP Troubleshooting Methodology. You will perform a static analysis and demonstrate how to create reports based on logged performance statistics. You also must configure performance-based alerts to prevent similar issues in the future.

Exercise 1 — Using PMP

These lab exercises enable you to practice different aspects of PMP functionality. They complement the presentation material as well as the associated self-running or instructor-led demonstrations.

INTERNET For more information about PMP, refer to:
http://www.hp.com/servers/proliantessentials/pmp

Updating HP Management Agents and software

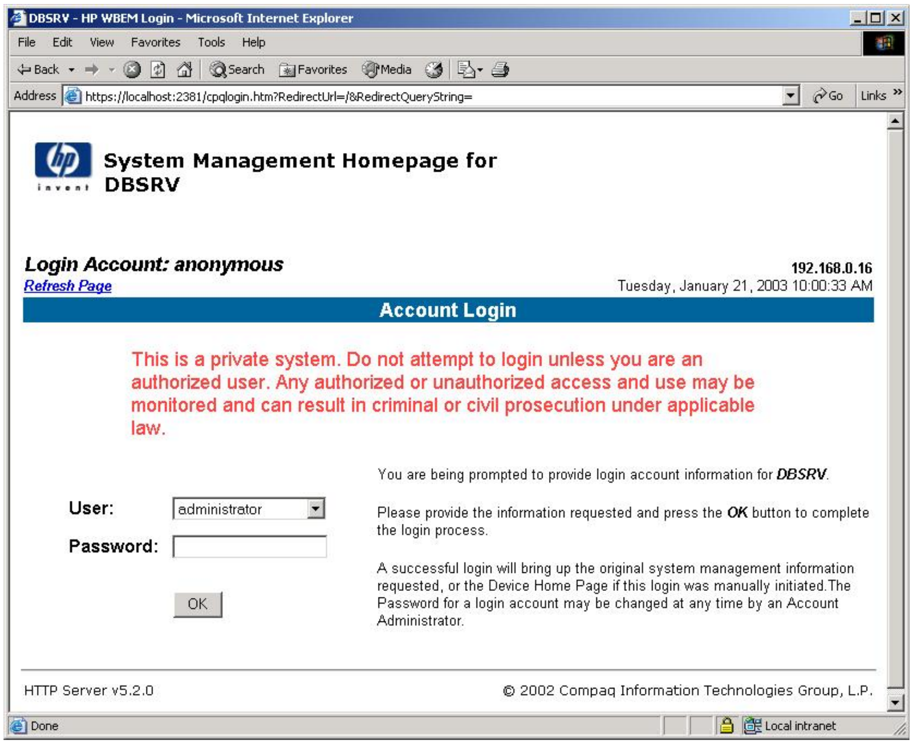
PMP 2.1 requires a minimum version of the HP Management Agents to be running on the supported ProLiant servers. This minimum version is dependent on the host operating system.

Operating system	Minimum agent version
Microsoft Windows NT 4.0	6.10.01
Microsoft Windows 2000	6.20
Microsoft Windows Server 2003	6.31

Determining the HP Management Agent version

To determine the installed version of the HP Management Agents using the System Management Homepage, complete these steps at the monitored server:

1. Open Internet Explorer and access the *https://localhost:2381* website.
2. At the login screen for the System Management Homepage for <server name>, log in as *administrator* using a valid password. (The administrator password was set up during the SmartStart installation and will be provided by your instructor.)


DBSRV - HP WBEM Login - Microsoft Internet Explorer
File
Edit
View
Favorites
Tools
Help
Back
Search
Favorites
Media
Address
https://localhost:2381/cpqlogin.htm?RedirectUrl=/&RedirectQueryString=
Go
Links
invent
Done
Local intranet

System Management Homepage for DBSRV

Login Account: anonymous

Refresh Page

192.168.0.16

Tuesday, January 21, 2003 10:00:33 AM

Account Login

This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.

User: administrator

Password:

OK

You are being prompted to provide login account information for ***DBSRV***.

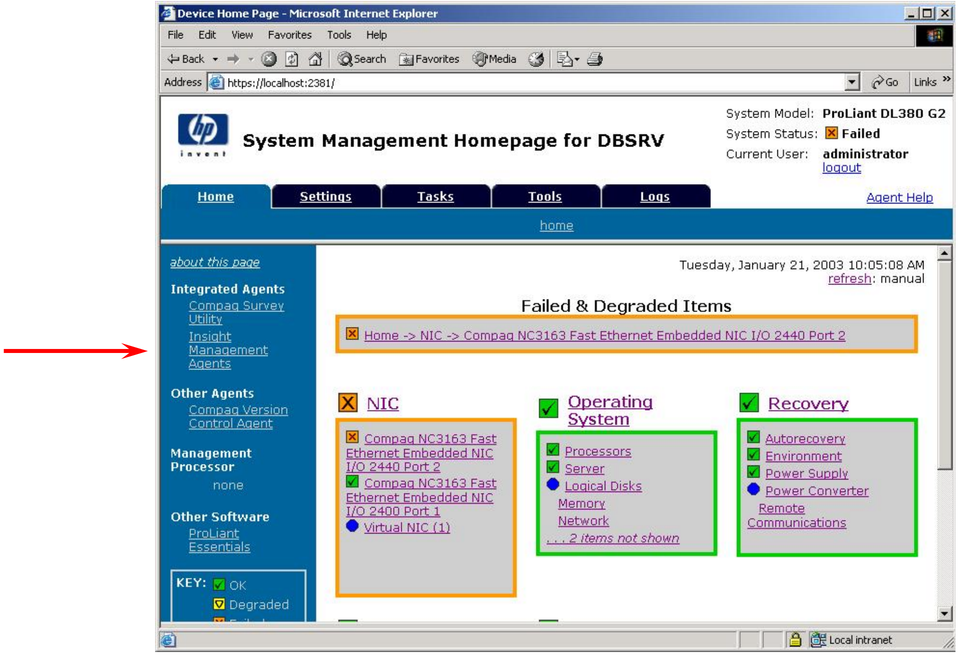
Please provide the information requested and press the ***OK*** button to complete the login process.

A successful login will bring up the original system management information requested, or the Device Home Page if this login was manually initiated.The Password for a login account may be changed at any time by an Account Administrator.

HTTP Server v5.2.0

© 2002 Compaq Information Technologies Group, L.P.

3. At the System Management Homepage for <server name>, click *Insight Management Agents*.


Device Home Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://localhost:2381/
Go Links
Home Settings Tasks Tools Logs
Agent Help
home
about this page
Integrated Agents
Compaq Survey Utility
Insight Management Agents
Other Agents
Compaq Version Control Agent
Management Processor
none
Other Software
ProLiant Essentials
KEY: OK Degraded
Local intranet

System Management Homepage for DBSRV

System Model: **ProLiant DL380 G2**
System Status: ☒ **Failed**
Current User: **administrator** logout

Tuesday, January 21, 2003 10:05:08 AM
refresh: manual

Failed & Degraded Items

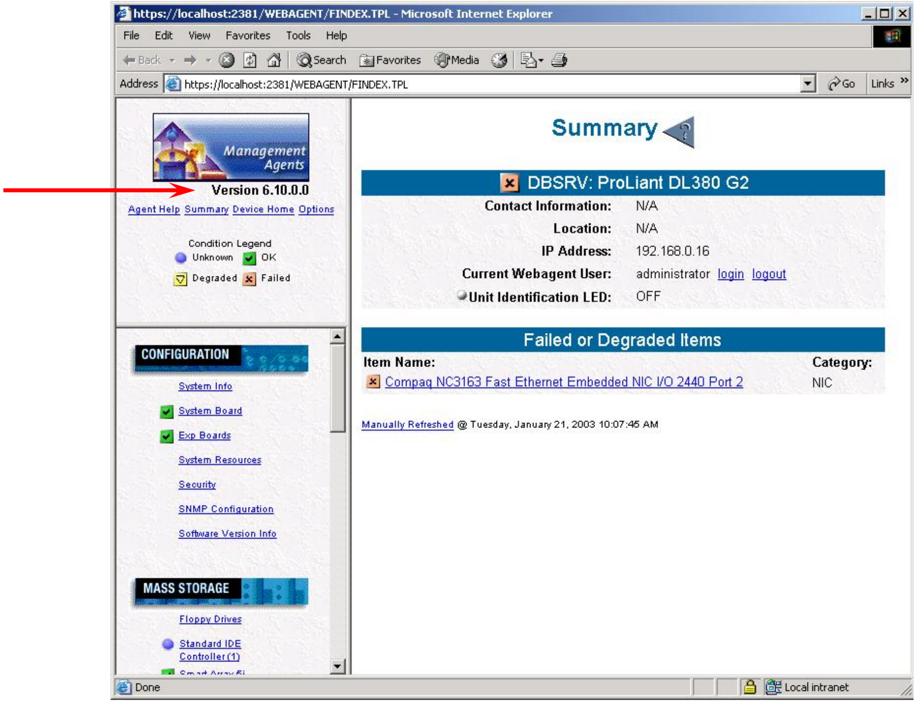
☒ Home -> NIC -> Compaq NC3163 Fast Ethernet Embedded NIC I/O 2440 Port 2

☒ NIC
- ☒ Compaq NC3163 Fast Ethernet Embedded NIC I/O 2440 Port 2
- ☑ Compaq NC3163 Fast Ethernet Embedded NIC I/O 2400 Port 1
- ● Virtual NIC (1)

☑ Operating System
- ☑ Processors
- ☑ Server
- ● Logical Disks
- Memory
- Network
- . . . 2 items not shown

☑ Recovery
- ☑ Autorecovery
- ☑ Environment
- ☑ Power Supply
- ● Power Converter
- Remote Communications

4. At the Management Agents screen, note that the HP Management Agents version displays in the top left pane; then close the window.


https://localhost:2381/WEBAGENT/FINDEX.TPL - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://localhost:2381/WEBAGENT/FINDEX.TPL
Go Links
Management Agents
Agent Help Summary Device Home Options
Condition Legend
Unknown OK
Degraded Failed
CONFIGURATION
System Info
System Board
Exp Boards
System Resources
Security
SNMP Configuration
Software Version Info
MASS STORAGE
Floppy Drives
Standard IDE Controller (1)
Done
Local intranet

Version 6.10.0.0

Summary

☒ DBSRV: ProLiant DL380 G2

Contact Information:	N/A
Location:	N/A
IP Address:	192.168.0.16
Current Webagent User:	administrator login logout
Unit Identification LED:	OFF

Failed or Degraded Items

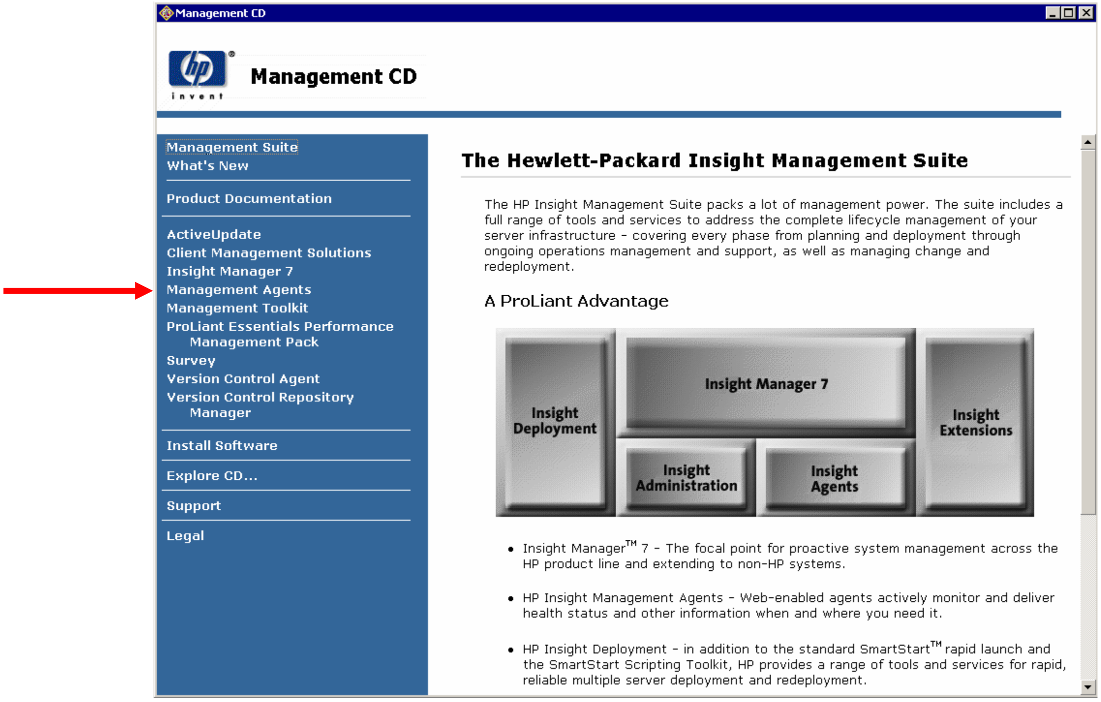
Item Name:	**Category:**
☒ Compaq NC3163 Fast Ethernet Embedded NIC I/O 2440 Port 2	NIC

Manually Refreshed @ Tuesday, January 21, 2003 10:07:45 AM

Updating the HP Management Agents

If the currently installed version of the HP Management Agents does not meet the minimum version requirements, you must update the agents. To update the agents:

1. Execute *autorun.exe*. This file is located on the Management CD or in a location specified by your instructor.
2. At the End-user license agreement screen, click *Agree*.
3. At the Hewlett-Packard Insight Management Suite screen, click *Management Agents*.



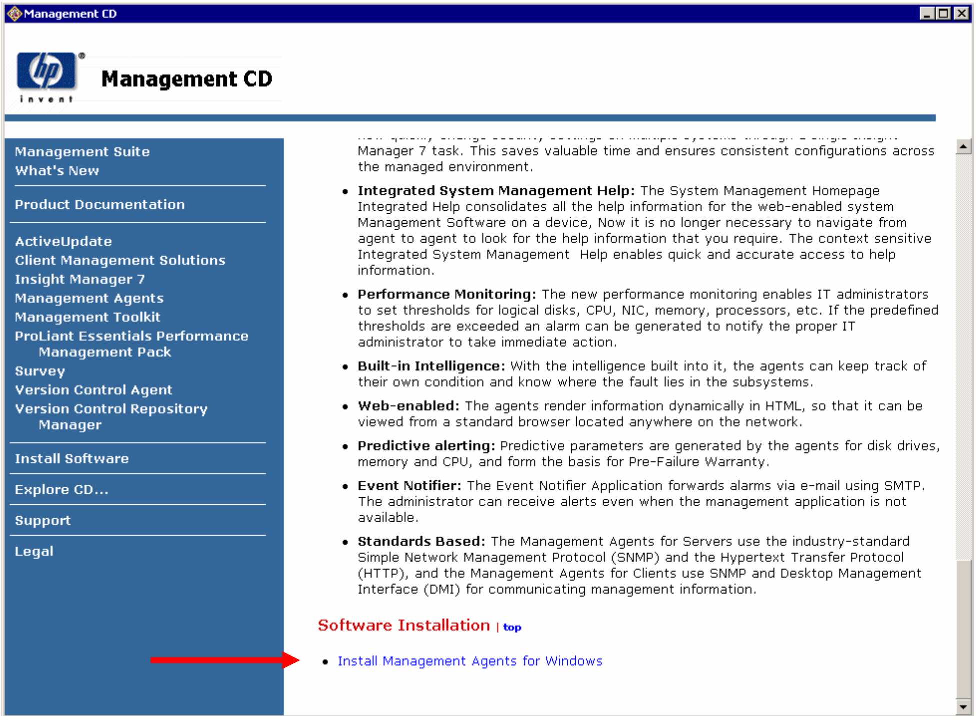
The Hewlett-Packard Insight Management Suite

The HP Insight Management Suite packs a lot of management power. The suite includes a full range of tools and services to address the complete lifecycle management of your server infrastructure - covering every phase from planning and deployment through ongoing operations management and support, as well as managing change and redeployment.

A ProLiant Advantage

- Insight Manager™ 7 - The focal point for proactive system management across the HP product line and extending to non-HP systems.
- HP Insight Management Agents - Web-enabled agents actively monitor and deliver health status and other information when and where you need it.
- HP Insight Deployment - in addition to the standard SmartStart™ rapid launch and the SmartStart Scripting Toolkit, HP provides a range of tools and services for rapid, reliable multiple server deployment and redeployment.

4. At the Management Agents screen, click *Install* → *Install Management Agents for Windows*.



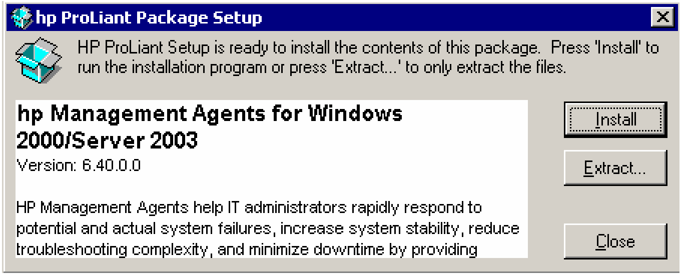
Manager 7 task. This saves valuable time and ensures consistent configurations across the managed environment.

- **Integrated System Management Help:** The System Management Homepage Integrated Help consolidates all the help information for the web-enabled system Management Software on a device, Now it is no longer necessary to navigate from agent to agent to look for the help information that you require. The context sensitive Integrated System Management Help enables quick and accurate access to help information.
- **Performance Monitoring:** The new performance monitoring enables IT administrators to set thresholds for logical disks, CPU, NIC, memory, processors, etc. If the predefined thresholds are exceeded an alarm can be generated to notify the proper IT administrator to take immediate action.
- **Built-in Intelligence:** With the intelligence built into it, the agents can keep track of their own condition and know where the fault lies in the subsystems.
- **Web-enabled:** The agents render information dynamically in HTML, so that it can be viewed from a standard browser located anywhere on the network.
- **Predictive alerting:** Predictive parameters are generated by the agents for disk drives, memory and CPU, and form the basis for Pre-Failure Warranty.
- **Event Notifier:** The Event Notifier Application forwards alarms via e-mail using SMTP. The administrator can receive alerts even when the management application is not available.
- **Standards Based:** The Management Agents for Servers use the industry-standard Simple Network Management Protocol (SNMP) and the Hypertext Transfer Protocol (HTTP), and the Management Agents for Clients use SNMP and Desktop Management Interface (DMI) for communicating management information.

Software Installation | top

- Install Management Agents for Windows

5. At the hp ProLiant Package Setup screen, click *Install*.

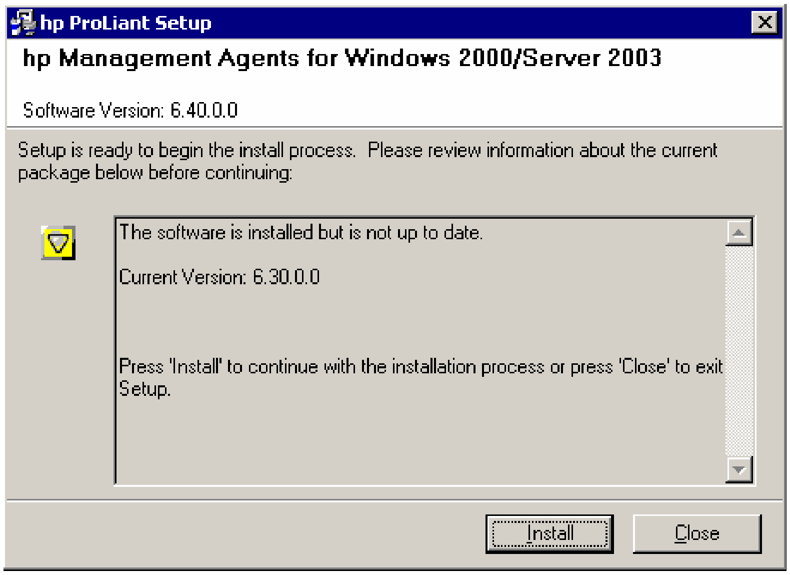


HP ProLiant Setup is ready to install the contents of this package. Press 'Install' to run the installation program or press 'Extract...' to only extract the files.

hp Management Agents for Windows 2000/Server 2003
Version: 6.40.0.0

HP Management Agents help IT administrators rapidly respond to potential and actual system failures, increase system stability, reduce troubleshooting complexity, and minimize downtime by providing

6. At the hp Management Agents for Windows 2000/Server 2003 screen, click *Install*.



hp ProLiant Setup

hp Management Agents for Windows 2000/Server 2003

Software Version: 6.40.0.0

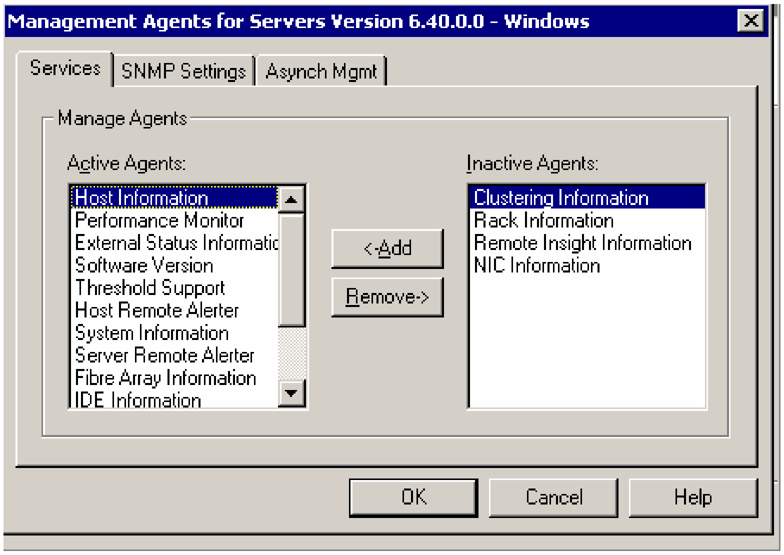
Setup is ready to begin the install process. Please review information about the current package below before continuing:

The software is installed but is not up to date.

Current Version: 6.30.0.0

Press 'Install' to continue with the installation process or press 'Close' to exit Setup.

7. At the Management Agents for Servers Version 6.40.0.0 – Windows screen, click *OK*.

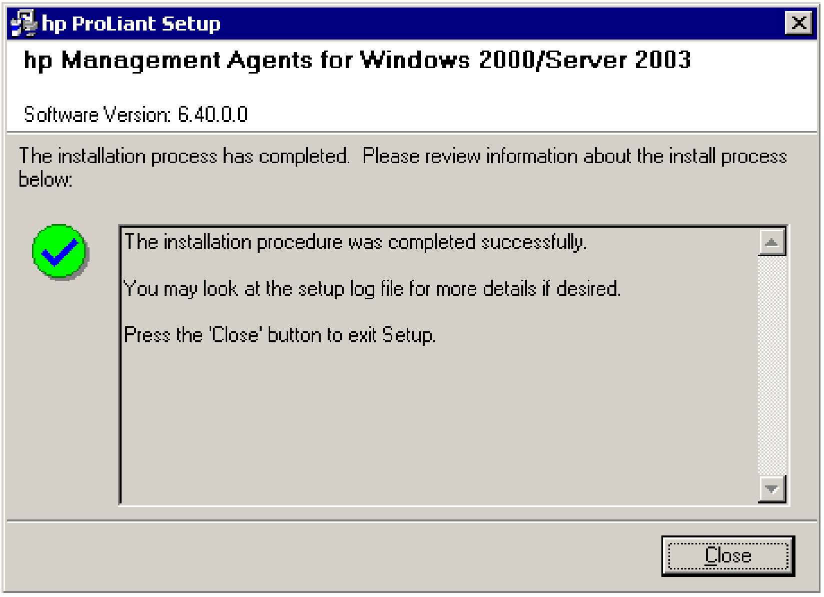


Management Agents for Servers Version 6.40.0.0 - Windows

Active Agents:
- Host Information
- Performance Monitor
- External Status Informatic
- Software Version
- Threshold Support
- Host Remote Alerter
- System Information
- Server Remote Alerter
- Fibre Array Information
- IDE Information

Inactive Agents:
- Clustering Information
- Rack Information
- Remote Insight Information
- NIC Information

8. At the following screen, click *Close*.



hp Management Agents for Windows 2000/Server 2003

Software Version: 6.40.0.0

The installation process has completed. Please review information about the install process below:

The installation procedure was completed successfully.

You may look at the setup log file for more details if desired.

Press the 'Close' button to exit Setup.

9. Use the steps described in the previous section, “Determining the HP Management Agent version,” to determine whether the agents have been updated to the desired version.

Updating PMP

If a PMP update is necessary, complete these steps at the middle-tier server:

1. Obtain the SP24900.exe file from your instructor and copy it to the local drive of your performance analysis server.
2. Close all windows and applications.
3. Execute the file and follow the prompts to install the update.
4. Restart the computer to complete the installation.

Licensing monitored servers

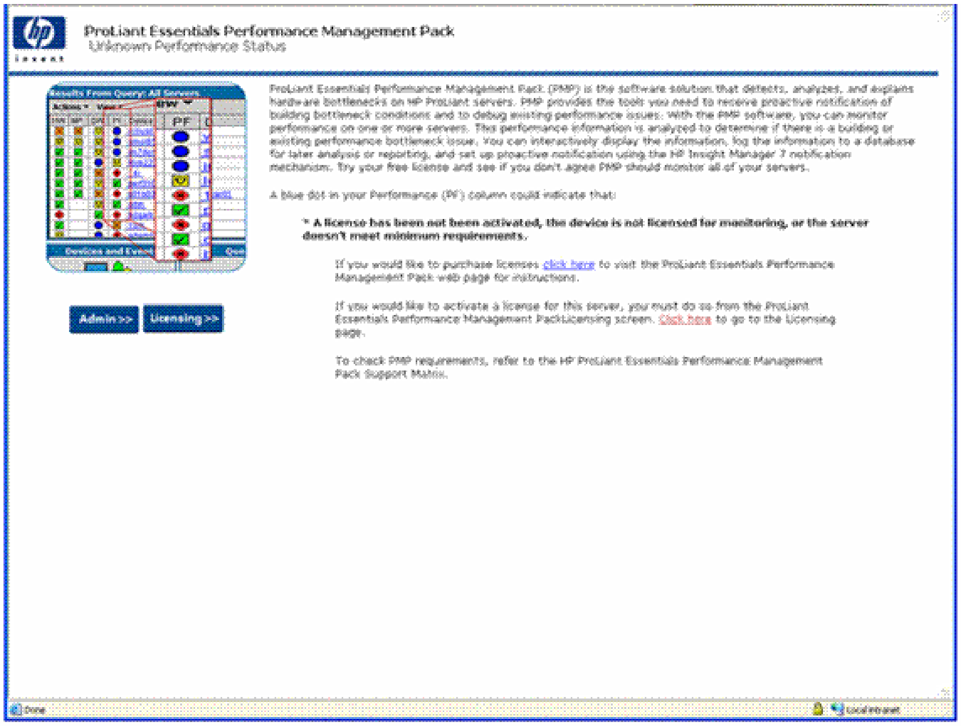
Complete this exercise to:

- Import new PMP licenses.
- Apply licenses to select servers.
- Retire demo licenses.

Importing new PMP licenses

To import purchased or demo licenses, perform these steps:

5. At the Insight Manager 7 Home page, click the blue dot corresponding to the appropriate server entry to display the ProLiant Essentials Performance Management Pack page. Then click *Licensing*.


ProLiant Essentials Performance Management Pack
Unknown Performance Status
Results From Query: All Servers
PF
Admin >>
Licensing >>
Done
Local intranet

ProLiant Essentials Performance Management Pack (PMP) is the software solution that detects, analyzes, and explains hardware bottlenecks on HP ProLiant servers. PMP provides the tools you need to receive proactive notification of building bottleneck conditions and to debug existing performance issues. With the PMP software, you can monitor performance on one or more servers. This performance information is analyzed to determine if there is a building or existing performance bottleneck issue. You can interactively display the information, log the information to a database for later analysis or reporting, and set up proactive notification using the HP Insight Manager 7 notification mechanism. Try your free license and see if you don't agree PMP should monitor all of your servers.

A blue dot in your Performance (PF) column could indicate that:

*** A license has been not been activated, the device is not licensed for monitoring, or the server doesn't meet minimum requirements.**

If you would like to purchase licenses click here to visit the ProLiant Essentials Performance Management Pack web page for instructions.

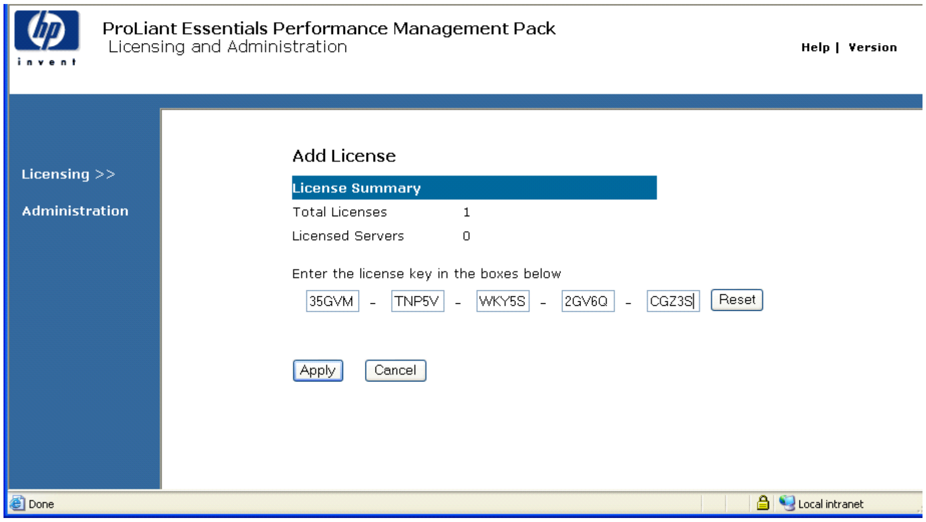
If you would like to activate a license for this server, you must do so from the ProLiant Essentials Performance Management PackLicensing screen. Click here to go to the Licensing page.

To check PMP requirements, refer to the HP ProLiant Essentials Performance Management Pack Support Matrix.

6. At the Licensing page, click *Update Server List* if the list of displayed servers does not include all servers displayed on the Insight Manager 7 Home page.
7. Click *Add License* to display the Add License page.

8. At the Add License page, enter the following 5-server 30-day demo license number and click *Apply*:

   35GVM-TNP5V-WKY5S-2GV6Q-CGZ3S



Add License

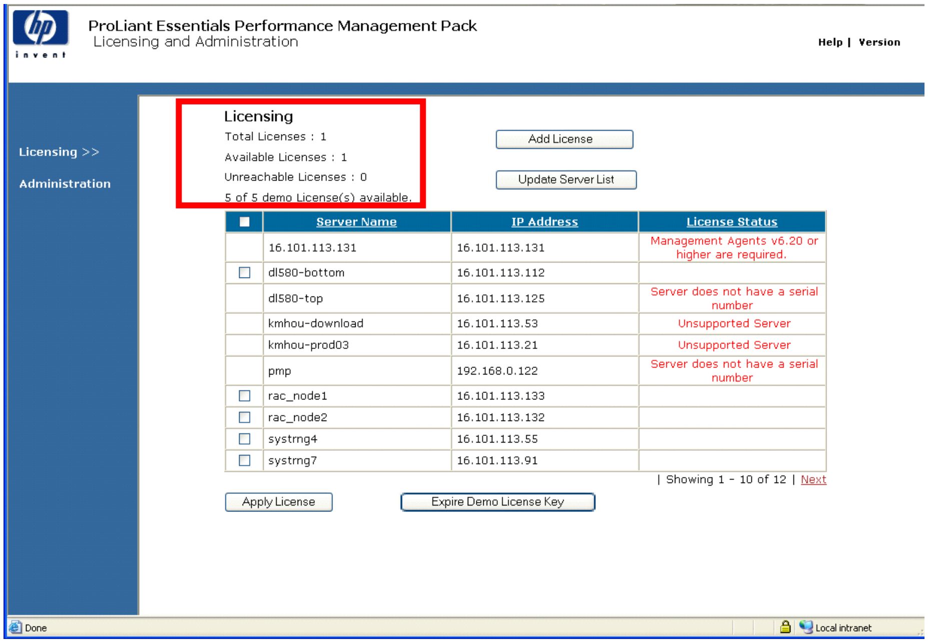
License Summary

Total Licenses	1
Licensed Servers	0

Enter the license key in the boxes below

35GVM - TNP5V - WKY5S - 2GV6Q - CGZ3S

9. At the Licensing page, verify that the licenses were added correctly.



Licensing

Total Licenses : 1

Available Licenses : 1

Unreachable Licenses : 0

5 of 5 demo License(s) available.

■	Server Name	IP Address	License Status
	16.101.113.131	16.101.113.131	Management Agents v6.20 or higher are required.
☐	dl580-bottom	16.101.113.112	
	dl580-top	16.101.113.125	Server does not have a serial number
	kmhou-download	16.101.113.53	Unsupported Server
	kmhou-prod03	16.101.113.21	Unsupported Server
	pmp	192.168.0.122	Server does not have a serial number
☐	rac_node1	16.101.113.133	
☐	rac_node2	16.101.113.132	
☐	systrng4	16.101.113.55	
☐	systrng7	16.101.113.91	

| Showing 1 - 10 of 12 | Next

Applying licenses to selected servers

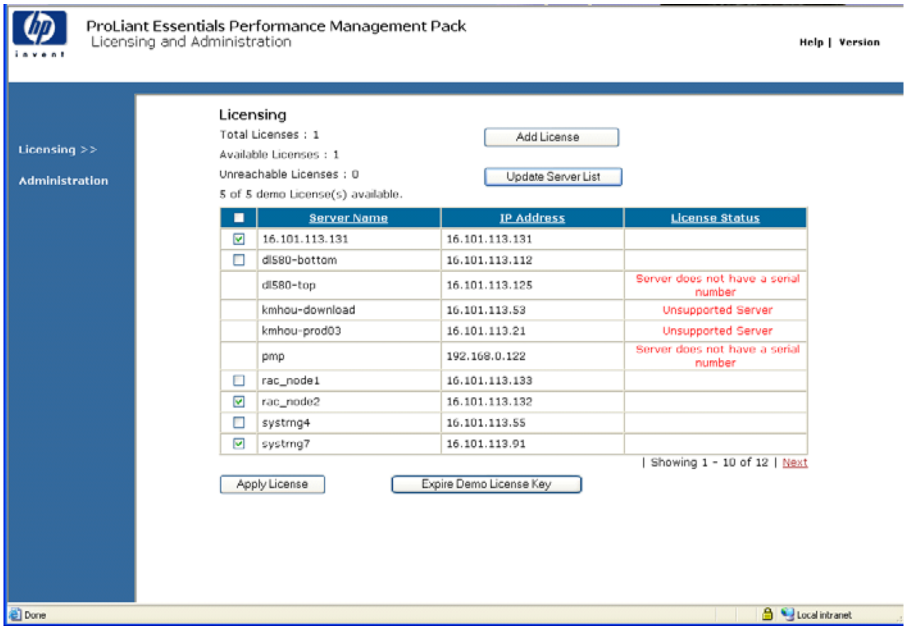
To license desired servers for monitoring, follow these steps:

Note

During licensing, PMP 2.1 uses available purchased licenses first, and then uses demo licenses if they are available.

---

1. At the Licensing page, select the desired servers to be licensed and click *Apply License*. You will be allowed to select only those servers meeting the PMP 2.1 requirements. An explanation displays in the License Status column for those servers not meeting the requirements.



Licensing

Total Licenses : 1

Available Licenses : 1

Unreachable Licenses : 0

5 of 5 demo License(s) available.

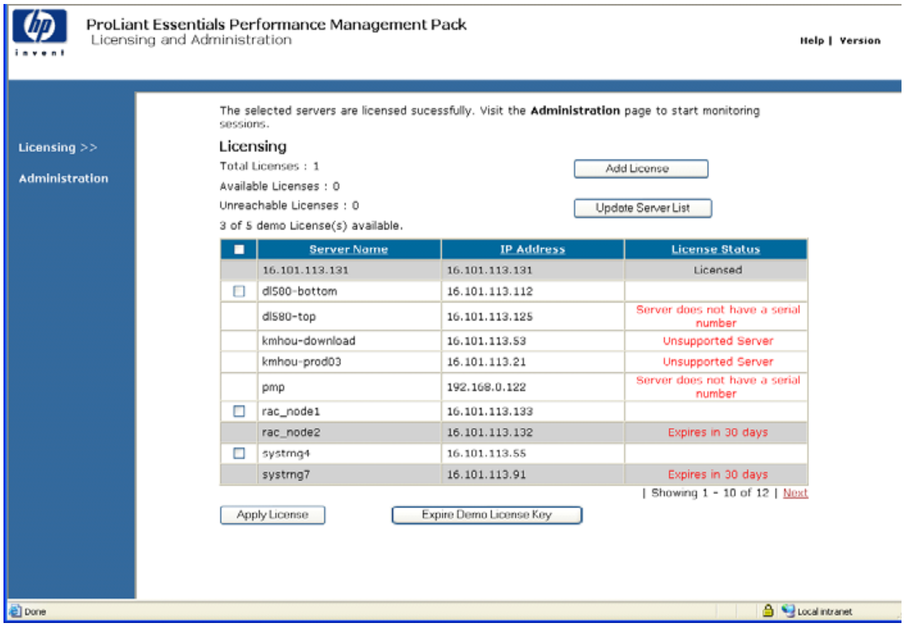
☐	Server Name	IP Address	License Status
☑	16.101.113.131	16.101.113.131	
☐	dl580-bottom	16.101.113.112	
	dl580-top	16.101.113.125	Server does not have a serial number
	kmhou-download	16.101.113.53	Unsupported Server
	kmhou-prod03	16.101.113.21	Unsupported Server
	pmp	192.168.0.122	Server does not have a serial number
☐	rac_node1	16.101.113.133	
☑	rac_node2	16.101.113.132	
☐	systmg4	16.101.113.55	
☑	systmg7	16.101.113.91	

| Showing 1 - 10 of 12 | Next

2. At the Licensing page, verify that the licenses were applied correctly. The License Status column displays whether the server was licensed with a purchased license (*Licensed*) or with a demo license (*Expires in 30 days*).

Note

If the free license was available, it was used as a purchased license, in addition to the available demo licenses.



The selected servers are licensed sucessfully. Visit the **Administration** page to start monitoring sessions.

Licensing

Total Licenses : 1

Available Licenses : 0

Unreachable Licenses : 0

3 of 5 demo License(s) available.

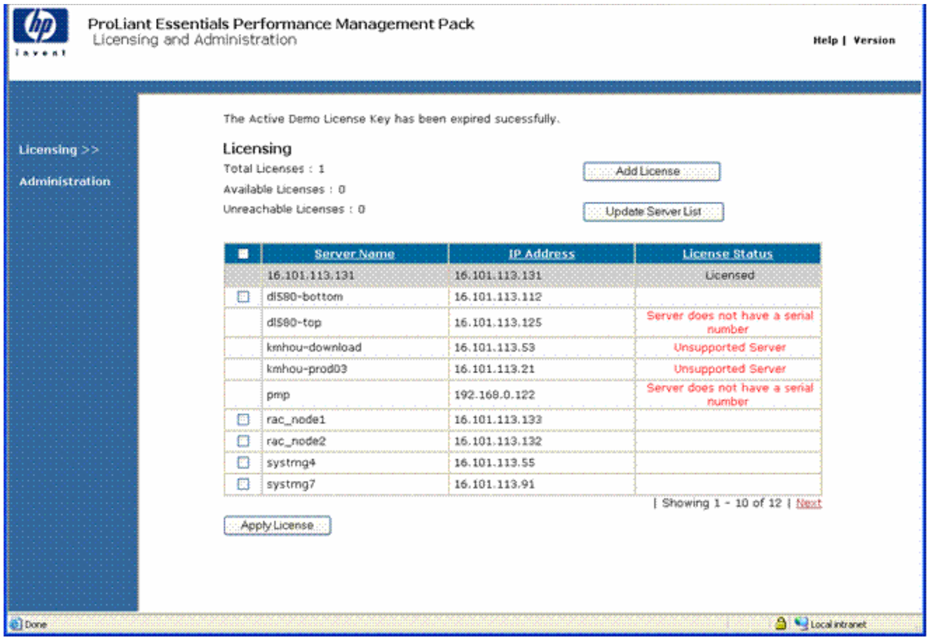
■	Server Name	IP Address	License Status
	16.101.113.131	16.101.113.131	Licensed
☐	dl580-bottom	16.101.113.112	
	dl580-top	16.101.113.125	Server does not have a serial number
	kmhou-download	16.101.113.53	Unsupported Server
	kmhou-prod03	16.101.113.21	Unsupported Server
	pmp	192.168.0.122	Server does not have a serial number
☐	rac_node1	16.101.113.133	
	rac_node2	16.101.113.132	Expires in 30 days
☐	systmg4	16.101.113.55	
	systmg7	16.101.113.91	Expires in 30 days

| Showing 1 - 10 of 12 | Next

Retiring demo licenses

Demo licenses are retired when you apply a purchased license to a monitored server that is licensed with a valid demo license. Retiring this demo license frees the server to be licensed with a purchased license. If a demo license key contains a certain number of licenses, all such licenses expire. If any such licenses were unused, they expire also.

1. At the Licensing page, click *Expire Demo License Key*. All demo licenses that belonged to the demo license key, whether applied to servers or still available, are expired. The servers are now available to be licensed with a purchased license.
2. At the Licensing page, verify that the licenses were applied correctly.



The Active Demo License Key has been expired sucessfully.

Licensing

Total Licenses : 1

Available Licenses : 0

Unreachable Licenses : 0

■	Server Name	IP Address	License Status
	16.101.113.131	16.101.113.131	Licensed
☐	dl580-bottom	16.101.113.112	
	dl580-top	16.101.113.125	Server does not have a serial number
	kmhou-download	16.101.113.53	Unsupported Server
	kmhou-prod03	16.101.113.21	Unsupported Server
	pmp	192.168.0.122	Server does not have a serial number
☐	rac_node1	16.101.113.133	
☐	rac_node2	16.101.113.132	
☐	systmg4	16.101.113.55	
☐	systmg7	16.101.113.91	

| Showing 1 - 10 of 12 | Next

3. Attempt to apply the same 5-server 30-day demo license key as in step 4:

   35GVM-TNP5V-WKY5S-2GV6Q-CGZ3S

   What was the result?

   ....

4. Enter the following 10-server 30-day demo license key and apply one of the demo licenses to the server you want to monitor (if applicable):

   332Q4-MH78T-JH9MV-RXVCN-6KD23

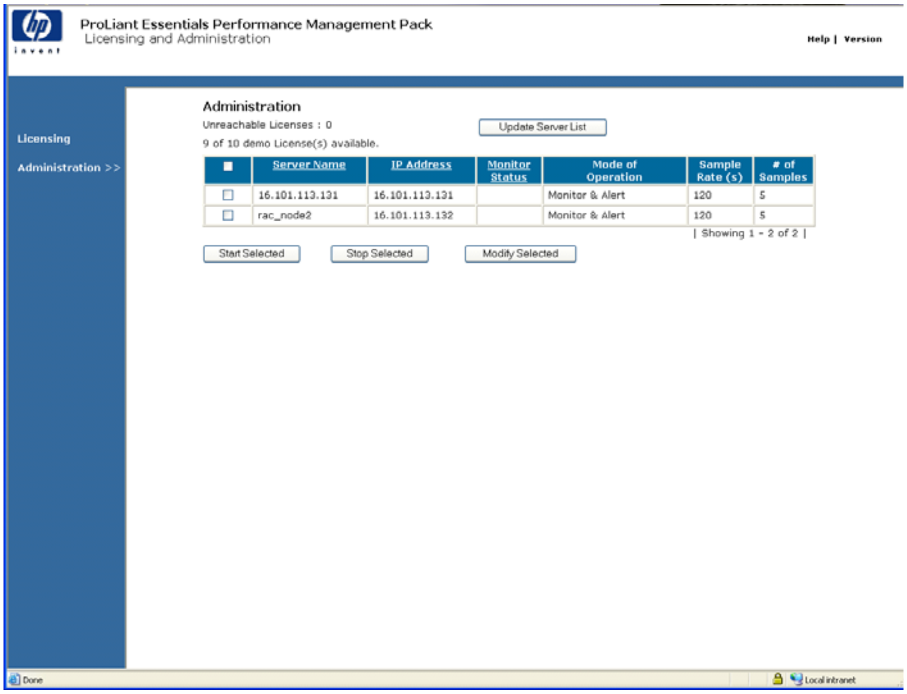
Configuring monitoring behavior

Monitoring PMP behavior depends primarily on its internal administration settings, such as the mode of operation, sample rate, and number of samples, which are configured at the PMP Administration page. The rate at which PMP collects performance information defaults to the data collection interval of the individual Management Agents at the monitored server.

Administering PMP

To administer PMP, use the Administration page. This page is accessible from the Licensing page, Unknown Performance Status page, or the PMP Home page.

1. At the Licensing page, click *Administration*.
2. At the Administration page, verify that the appropriate licensed servers are listed. Click *Update Server List* if necessary.



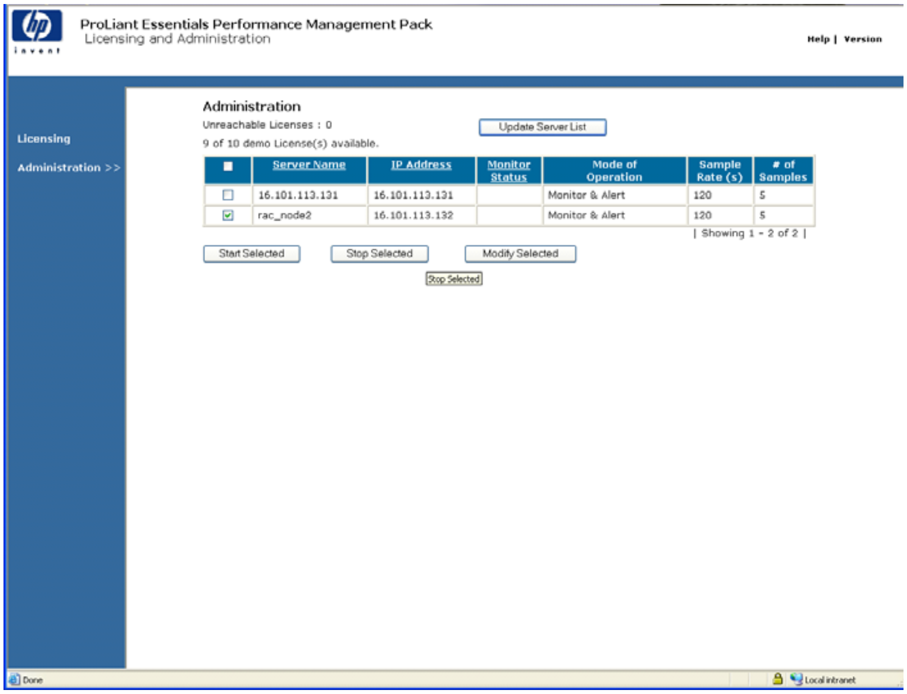
Unreachable Licenses : 0

9 of 10 demo License(s) available.

■	Server Name	IP Address	Monitor Status	Mode of Operation	Sample Rate (s)	# of Samples
☐	16.101.113.131	16.101.113.131		Monitor & Alert	120	5
☐	rac_node2	16.101.113.132		Monitor & Alert	120	5

| Showing 1 - 2 of 2 |

3. If you are satisfied with the monitoring settings, such as the mode of operation, sample rate, and number of samples, select the desired server and click *Start Selected*. Otherwise, select the desired server and click *Modify Selected*.



Administration

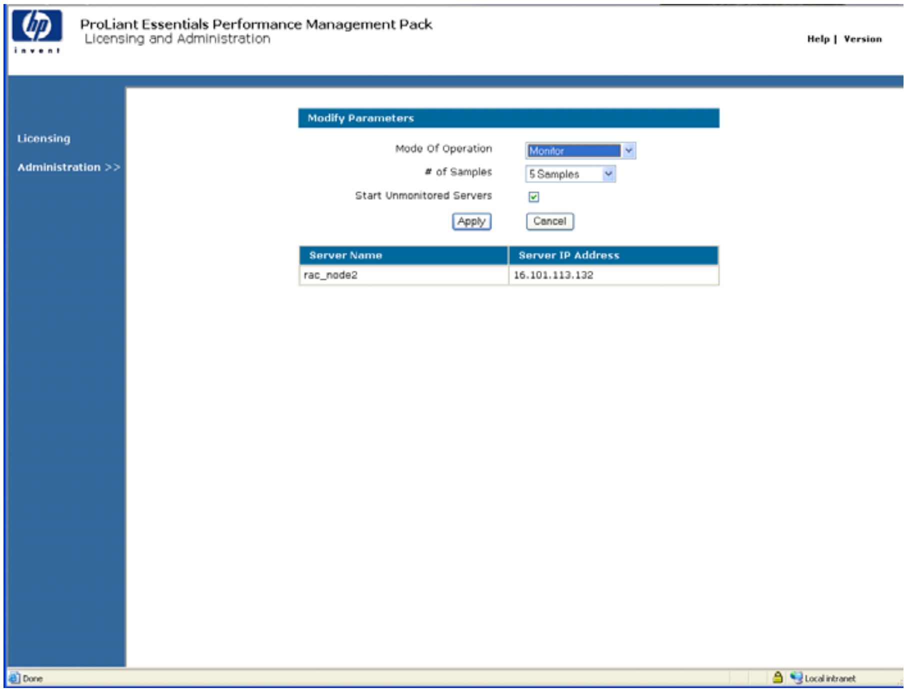
Unreachable Licenses : 0

9 of 10 demo License(s) available.

■	Server Name	IP Address	Monitor Status	Mode of Operation	Sample Rate (s)	# of Samples
☐	16.101.113.131	16.101.113.131		Monitor & Alert	120	5
☑	rac_node2	16.101.113.132		Monitor & Alert	120	5

| Showing 1 - 2 of 2 |

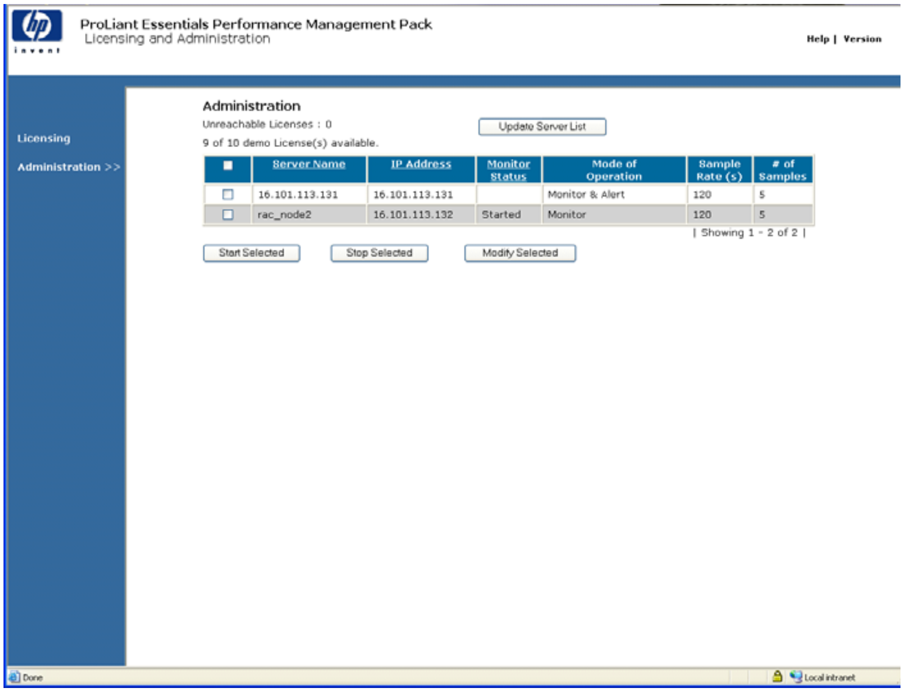
4. At the Modify Parameters page, modify the operational parameters as desired and click *Apply*. If you select the Start Unmonitored Servers option, PMP 2.1 begins monitoring those servers automatically.



Mode Of Operation: Monitor
# of Samples: 5 Samples
Start Unmonitored Servers: ☑

Server Name	Server IP Address
rac_node2	16.101.113.132

5. At the Administration page, verify that the monitoring status for the desired servers displays *Started* and close the window.



Administration

Unreachable Licenses : 0

9 of 10 demo License(s) available.

☐	Server Name	IP Address	Monitor Status	Mode of Operation	Sample Rate (s)	# of Samples
☐	16.101.113.131	16.101.113.131		Monitor & Alert	120	5
☐	rac_node2	16.101.113.132	Started	Monitor	120	5

| Showing 1 - 2 of 2 |

Modifying the data collection sample rate

The sample rate (the rate at which PMP collects performance-related statistics from the monitored server agents) is no longer user-configurable through PMP administration. Instead, it defaults to the data collection interval set by the HP Management Agents at the monitored server. By default, this interval is set to two minutes. Although this setting is valid for most environments, it can be changed to a value ranging from five seconds to 60 minutes.

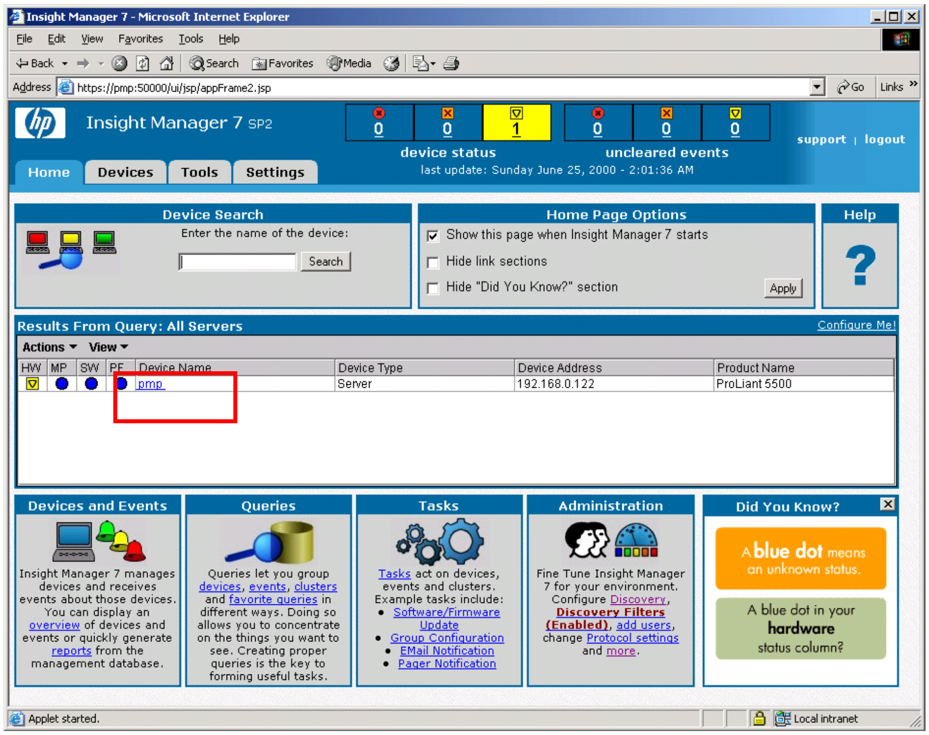
! **Important**

In the classroom setting, change the data collection interval and the number of samples to lower than default values. Otherwise, it might be several minutes before you can see visible results in PMP. However, avoid setting these parameters to the minimum values to avoid problems with collecting performance data.

To change the data collection interval for the Management Agents, perform these steps:

Using Insight Manager 7

1. At the Insight Manager 7 home page, click the Device Name entry for the desired server.


Insight Manager 7 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://pmp:50000/ui/jsp/appFrame2.jsp
Go Links
Insight Manager 7 SP2
0 0 1 0 0 0
device status
uncleared events
last update: Sunday June 25, 2000 - 2:01:36 AM
support | logout
Home Devices Tools Settings
Device Search
Search
Home Page Options
Help
Apply
Results From Query: All Servers
Configure Me!
Actions View
Devices and Events
Queries
Tasks
Administration
Did You Know?
A blue dot means an unknown status.
A blue dot in your hardware status column?
Applet started.
Local intranet

Enter the name of the device:

☑ Show this page when Insight Manager 7 starts

☐ Hide link sections

☐ Hide "Did You Know?" section

HW	MP	SW	PF	Device Name	Device Type	Device Address	Product Name
▽	●	●	●	pmp	Server	192.168.0.122	ProLiant 5500

Insight Manager 7 manages devices and receives events about those devices. You can display an overview of devices and events or quickly generate reports from the management database.

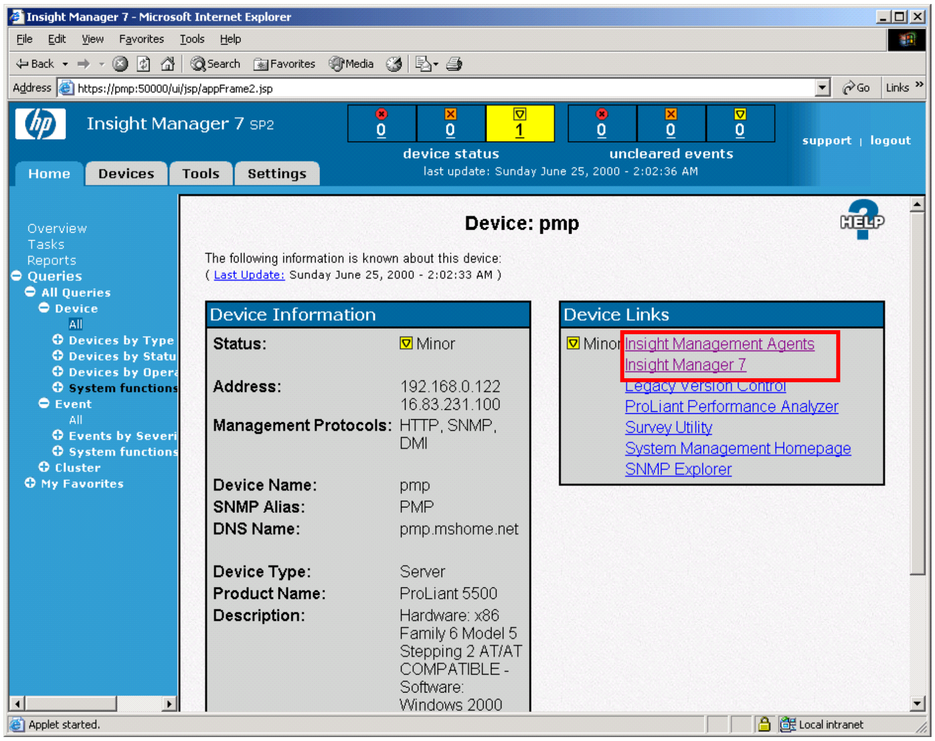
Queries let you group devices, events, clusters and favorite queries in different ways. Doing so allows you to concentrate on the things you want to see. Creating proper queries is the key to forming useful tasks.

Tasks act on devices, events and clusters. Example tasks include:

- Software/Firmware Update
- Group Configuration
- EMail Notification
- Pager Notification

Fine Tune Insight Manager 7 for your environment. Configure Discovery, **Discovery Filters (Enabled)**, add users, change Protocol settings and more.

2. At the Device: PMP screen, click *Insight Management Agents* in the Device Links section.



Device: pmp

The following information is known about this device:
(Last Update: Sunday June 25, 2000 - 2:02:33 AM)

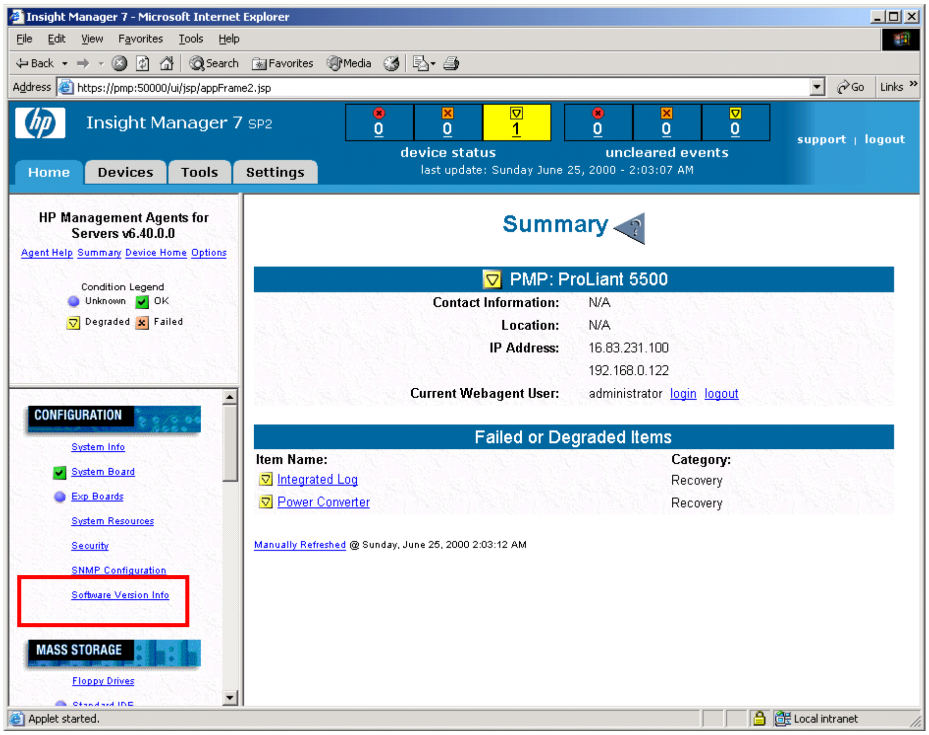
Device Information

Status:	Minor
Address:	192.168.0.122 16.83.231.100
Management Protocols:	HTTP, SNMP, DMI
Device Name:	pmp
SNMP Alias:	PMP
DNS Name:	pmp.mshome.net
Device Type:	Server
Product Name:	ProLiant 5500
Description:	Hardware: x86 Family 6 Model 5 Stepping 2 AT/AT COMPATIBLE - Software: Windows 2000

Device Links

Minor Insight Management Agents
Insight Manager 7
Legacy Version Control
ProLiant Performance Analyzer
Survey Utility
System Management Homepage
SNMP Explorer

3. At the Summary screen, click *SNMP Configuration* in the left pane.


Insight Manager 7 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://pmp:50000/ui/jsp/appFrame2.jsp
Go Links
Insight Manager 7 SP2
0 0 1 0 0 0
device status
uncleared events
last update: Sunday June 25, 2000 - 2:03:07 AM
support | logout
Home Devices Tools Settings
HP Management Agents for Servers v6.40.0.0
Agent Help Summary Device Home Options
Condition Legend
Unknown OK
Degraded Failed
CONFIGURATION
System Info
System Board
Exp Boards
System Resources
Security
SNMP Configuration
Software Version Info
MASS STORAGE
Floppy Drives
Standard IDE
Applet started.
Local intranet

Summary

PMP: ProLiant 5500

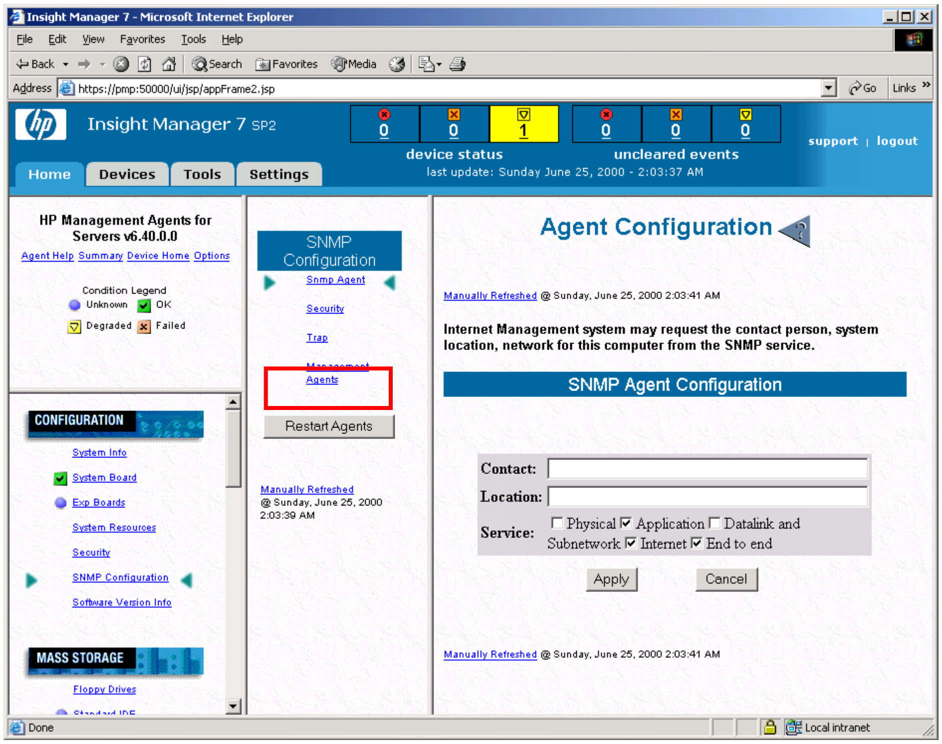
Contact Information:	N/A
Location:	N/A
IP Address:	16.83.231.100 192.168.0.122
Current Webagent User:	administrator login logout

Failed or Degraded Items

Item Name:	Category:
Integrated Log	Recovery
Power Converter	Recovery

Manually Refreshed @ Sunday, June 25, 2000 2:03:12 AM

4. At the Agent Configuration screen, click *Management Agents*.


Insight Manager 7 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://pmp:50000/ui/jsp/appFrame2.jsp
Go Links
Insight Manager 7 SP2
0 0 1 0 0 0
device status
uncleared events
last update: Sunday June 25, 2000 - 2:03:37 AM
support | logout
Home Devices Tools Settings
HP Management Agents for Servers v6.40.0.0
Agent Help Summary Device Home Options
Condition Legend
Unknown OK Degraded Failed
CONFIGURATION
System Info
System Board
Exp Boards
System Resources
Security
SNMP Configuration
Software Version Info
MASS STORAGE
Floppy Drives
Standard IDE
SNMP Configuration
Snmp Agent
Security
Trap
Management Agents
Restart Agents
Manually Refreshed @ Sunday, June 25, 2000 2:03:39 AM
Agent Configuration
Manually Refreshed @ Sunday, June 25, 2000 2:03:41 AM
SNMP Agent Configuration
Apply
Cancel
Manually Refreshed @ Sunday, June 25, 2000 2:03:41 AM
Done
Local intranet

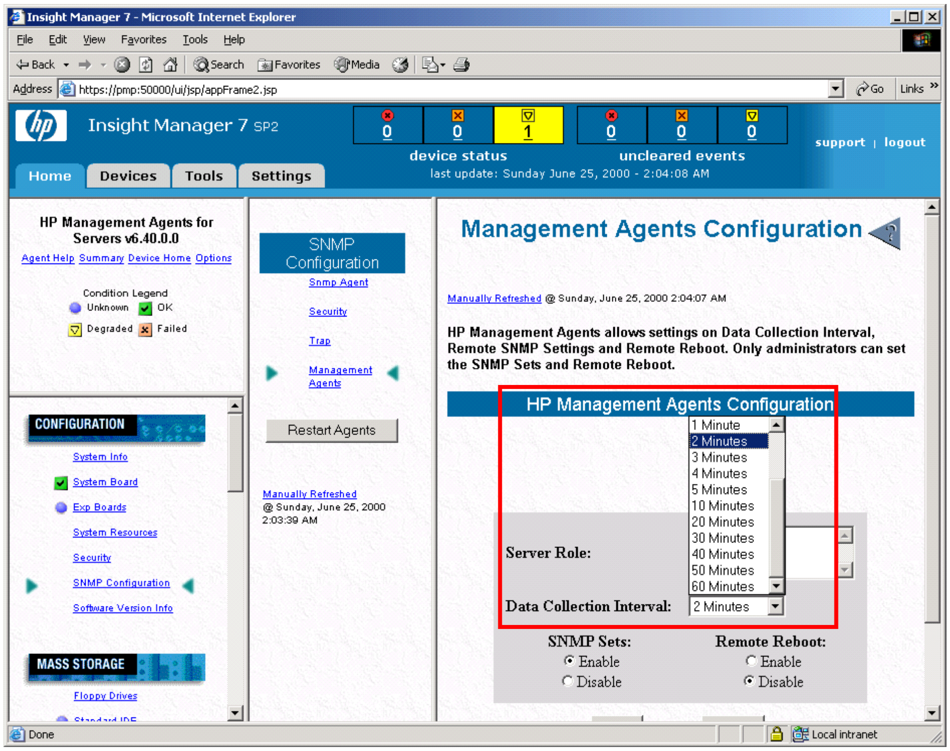
Internet Management system may request the contact person, system location, network for this computer from the SNMP service.

Contact:

Location:

Service: ☐ Physical ☑ Application ☐ Datalink and Subnetwork ☑ Internet ☑ End to end

5. At the Management Agents Configuration screen, select the desired data collection interval and then click *Apply*.


Insight Manager 7 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://pmp:50000/ui/jsp/appFrame2.jsp
Go Links
Insight Manager 7 SP2
0 0 1 0 0 0
device status
uncleared events
last update: Sunday June 25, 2000 - 2:04:08 AM
support | logout
Home Devices Tools Settings
HP Management Agents for Servers v6.40.0.0
Agent Help Summary Device Home Options
Condition Legend
Unknown OK Degraded Failed
CONFIGURATION
System Info
System Board
Exp Boards
System Resources
Security
SNMP Configuration
Software Version Info
MASS STORAGE
Floppy Drives
Standard IDE
SNMP Configuration
Snmp Agent
Security
Trap
Management Agents
Restart Agents
Manually Refreshed @ Sunday, June 25, 2000 2:03:39 AM
Management Agents Configuration
Manually Refreshed @ Sunday, June 25, 2000 2:04:07 AM
HP Management Agents Configuration
1 Minute
2 Minutes
3 Minutes
4 Minutes
5 Minutes
10 Minutes
20 Minutes
30 Minutes
40 Minutes
50 Minutes
60 Minutes
Done
Local intranet

HP Management Agents allows settings on Data Collection Interval, Remote SNMP Settings and Remote Reboot. Only administrators can set the SNMP Sets and Remote Reboot.

Server Role:

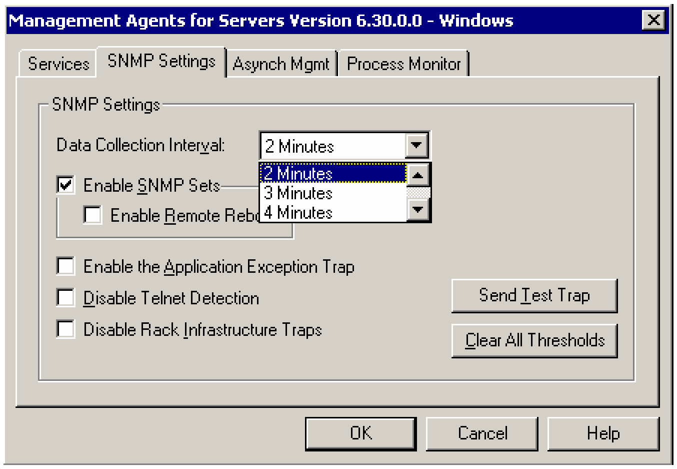
Data Collection Interval: 2 Minutes

SNMP Sets: ● Enable ○ Disable

Remote Reboot: ○ Enable ● Disable

Using Windows Control Panel

1. At the target server, click *Start* → *Settings* → *Control Panel* → *HP Management Agents*.
2. At the Management Agents for Servers window, change the Data Collection Interval to a desired value. Then click *OK*.



Management Agents for Servers Version 6.30.0.0 - Windows

SNMP Settings

Data Collection Interval: 2 Minutes

☑ Enable SNMP Sets

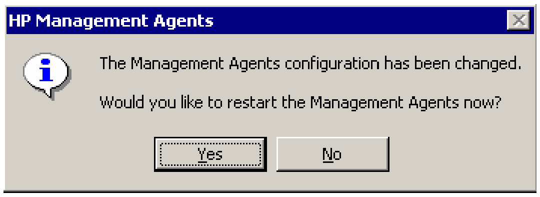
☐ Enable Remote Rebo

☐ Enable the Application Exception Trap

☐ Disable Telnet Detection

☐ Disable Rack Infrastructure Traps

3. At the following window, click *Yes* to restart the Management Agents.



HP Management Agents

The Management Agents configuration has been changed.

Would you like to restart the Management Agents now?

Performing static analysis

Static analysis refers to configuration validation of the target server. PMP ensures that the hardware configuration of the server does not create a performance problem at a later time.

Use the appropriate PMP areas to determine if there are any configuration problem areas in the monitored server.

Example 1

Smart Array 5i Controller configuration problems:

- Drives with different performance (SCSI speeds) detected in Array A
- Physical drives not assigned to an array

Example 2

Host bus configuration problems:

- PCI Devices are not evenly distributed among the available PCI buses.

Note any configuration problems with your system.

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

Detecting, analyzing, and resolving performance bottlenecks

Performance monitoring starts as soon as you license the target server and change the PMP mode of operation to any of the monitoring options. You might have to wait a few minutes for PMP to collect sufficient data points.

The main features of PMP are:

- Server inventory
- Static analysis
- Monitoring and performance analysis of major server subsystems
  - Processors
  - Memory
  - Disk subsystem
  - Network connections
  - Host buses

The current version of PMP is designed to monitor nonclustered servers.

As you explore these features, you will notice that detailed instructions are omitted. Because PMP is so easy to use, only guidelines and tasks to complete are provided.

! **Important**

Any changes to the monitored server hardware and software must be completed before monitoring the server. These changes include:

- Disabling a NIC
- Changing the IP address
- Updating the Management Agents

If you must make changes, stop the monitoring of the server from the Administration page. Then use the Insight Manager 7 Settings page to add the IP address of the modified server to the inclusion range and rediscover the server.

Reviewing the server inventory

The server inventory displays information about the hardware and software components, including their description, version, and condition.

Use the appropriate PMP areas to determine:

Server model: ....

Number of processors: ....

Type of processors: ....

Amount of memory:...

Number of network interface controllers: ....

Number and type of array controllers: ....

Number of host buses: ....

Operating system type and version: ....

Applied service packs, if any: ....

Number of Windows physical disks and their location: ....

....

....

....

Note

Windows 2000 logical disks that are mounted instead of assigned a drive letter will not be included in the PMP Inventory tab under the Windows logical drives.

IP addresses of the configured network controllers: ....

....

Operating mode of the network controllers: ....

....

Operating speed of the network controllers: ....

....

Type and size of the logical disk volumes: ....

....

....

....

Number, type, and size of arrays configured on the first array controller: ....
....
....
....
....

Striping factor of the first array configured on the first array controller: ....
....

The size and type of the connected disk drives: ....
....
....

The types of expansion boards connected to the primary bus: ....
....
....
....

The types of expansion boards connected to the secondary bus: ....
....
....
....

The types of expansion boards connected to the tertiary bus: ....
....
....
....

Monitoring processor utilization

To monitor processor utilization, follow these steps:

1. At the monitored server, induce high processor utilization by using a stress tool of your choice.

   Note

   For recommended stress tools, refer to Appendix B, “Stress Tools.”

2. At the performance analysis server, use the appropriate PMP areas to determine the levels of processor utilization. Focus on the following areas:

   Average Processor Busy %: ....

   Processor Queue: ....

   Context Switches/Sec: ....

   Interrupts/Sec: ....

   Analysis Explanation: ....

   ....

   Recommendation: ....

   ....

3. To assess the monitored server, answer the following questions.

   Which subsystem is the most stressed? ....

   ....

   What is the level of utilization of this subsystem? ....

   ....

   ....

   If this were a customer system, what would you recommend? ....

   ....

   ....

   ....

Monitoring memory utilization

To monitor memory utilization, follow these steps:

1. At the monitored server, induce high memory utilization by using a stress tool of your choice.

> **Note**
> For recommended stress tools, refer to Appendix B, "Stress Tools."

2. At the performance analysis server, use the appropriate PMP areas to determine the levels of memory utilization. Focus on the following areas:

   Available KBytes: ....

   Page Reads/Sec: ....

   Pages Input/Sec: ....

   Page Faults/Sec: ....

   % Hard Page Faults: ....

   Analysis Explanation: ....

   ....

   Recommendation: ....

   ....

3. To assess the monitored server, answer the following questions.

   Which subsystem is the most stressed? ....

   ....

   What is the level of utilization of this subsystem? ....

   ....

   ....

   If this were a customer system, what would you recommend? ....

   ....

   ....

   ....

Monitoring disk subsystem utilization

To monitor disk subsystem utilization:

1. At the monitored server, induce high disk subsystem utilization by using a stress tool of your choice.

Note
For recommended stress tools, refer to Appendix B, "Stress Tools."

2. At the performance analysis server, use the appropriate PMP areas to determine the levels of disk subsystem utilization. Focus on the following areas:

Storage Transfers/Sec: ....
Storage Bytes/Sec: ....

Array Controller Transfers/Sec:...
Array Controller Sec/Transfer: ....
Array Controller Queue Length: ....

Array ___ Disk Reads/Sec: ....
Array ___ Disk Writes/Sec: ....
Array ___ Disk Sec/Read: ....
Array ___ Disk Sec/Write: ....
Array ___ Disk Queue Length: ....

Array ___ Disk Reads/Sec: ....
Array ___ Disk Writes/Sec: ....
Array ___ Disk Sec/Read: ....
Array ___ Disk Sec/Write: ....
Array ___ Disk Queue Length: ....

Disk ID ___ Disk Reads/Sec: ....
Disk ID ___ Disk Writes/Sec: ....
Disk ID ___ Disk Sec/Read: ....
Disk ID ___ Disk Sec/Write: ....
Disk ID ___ Disk Queue Length: ....

Disk ID ___ Disk Reads/Sec: ....
Disk ID ___ Disk Writes/Sec: ....
Disk ID ___ Disk Sec/Read: ....
Disk ID ___ Disk Sec/Write: ....
Disk ID ___ Disk Queue Length: ....

Analysis Explanation: ....
....
....
....
Recommendation: ....
....
....

3. To assess the monitored server, answer the following questions.

   Which subsystem is the most stressed? ....
   ....
   What is the level of utilization of this subsystem? ....
   ....
   ....
   If this were a customer system, what would you recommend? ....
   ....
   ....

Note

The SCSI Utilization Percentage metric might display a value greater than 100% when sequential writes are issued to logical drives configured with RAID 5 or Advanced Data Guarding (ADG).

Monitoring network utilization

To monitor network utilization:

1. At the monitored server, induce high network utilization by using a stress tool of your choice.

> **Note**
> For recommended stress tools, refer to Appendix B, “Stress Tools.”

2. At the performance analysis server, use the appropriate PMP areas to determine the levels of network utilization. Focus on the following areas:

Network Bytes/Sec: ....

Bytes Sent/Sec: ....

Bytes Received/Sec: ....

NIC ___ Bytes Sent/Sec: ....

NIC ___ Bytes Received/Sec: ....

Port ___ Bytes Sent/Sec: ....

Port ___ Bytes Received/Sec: ....

Port ___ Send Utilization %: ....

Port ___ Receive Utilization %: ....

Analysis Explanation: ....

....

Recommendation: ....

....

3. To assess the monitored server, answer the following questions.

   Which subsystem is the most stressed? ....

   ....

   What is the level of utilization of this subsystem? ....

   ....

   ....

   If this were a customer system, what would you recommend? ....

   ....

   ....

Monitoring host buses

To monitor host bus utilization:

1. At the monitored server, induce high disk subsystem utilization by using a stress tool of your choice.

> **Note**
> For recommended stress tools, refer to Appendix B, "Stress Tools."

2. At the performance analysis server, use the appropriate PMP areas to determine the levels of host bus utilization. Focus on the following areas:

   PCI Bytes/Sec: ....

   Primary Bus Bytes/Sec: ....
   Primary Bus Utilization %: ....

   Secondary Bus Bytes/Sec: ....
   Secondary Bus Utilization %: ....

   Tertiary Bus Bytes/Sec: ....
   Tertiary Bus Utilization: ....

   Analysis Explanation: ....
   ....
   Recommendation: ....
   ....

3. To assess the monitored server, answer the following questions.

   Which subsystem is the most stressed? ....
   ....
   What is the level of utilization of this subsystem? ....
   ....
   ....
   If this were a customer system, what would you recommend? ....
   ....
   ....
   ....

Logging and manipulating data

When logging is enabled, PMP stores performance data gathered from monitored servers in a database repository. PMP provides powerful performance analysis tools to help manipulate the stored performance data.

Note

Although logging can be enabled remotely, logged data manipulation such as data extraction, log deletion, offline analysis, and report generation must be performed at the performance analysis server.

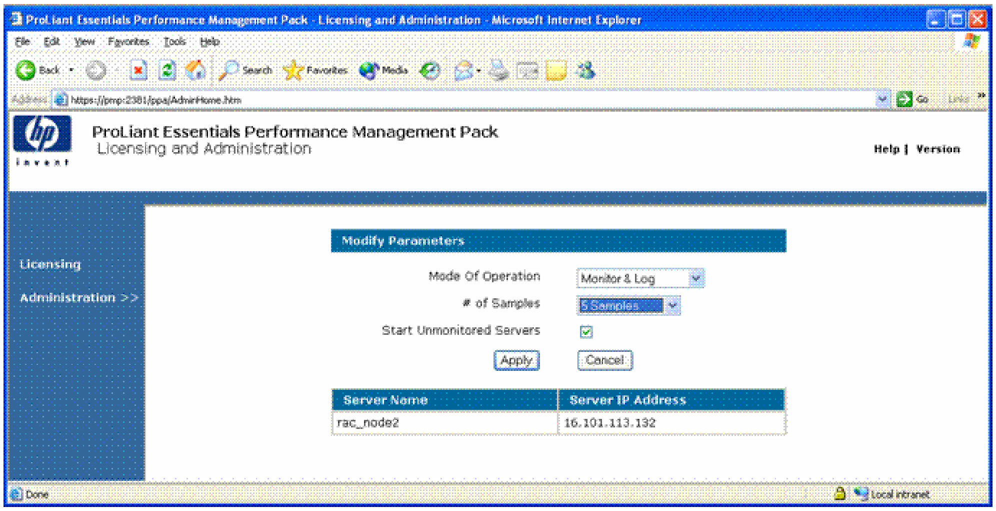
Logging

Logging enables PMP to collect performance information and store it in the performance database. You can then extract the data for offline analysis or generate reports to be imported into desktop data analysis tools.

1. At the Administration page, select the desired target server and click *Modify Selected*.
2. At the Modify Parameters screen, select the *Monitor & Log* mode of operation to enable logging for a selected target server. Adjust the number of samples option to the desired setting (for example, *5 Samples*) and click *Apply*.

Note

The sampling frequency is set at the monitored servers by the HP Management Agents.


ProLiant Essentials Performance Management Pack - Licensing and Administration - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://pmp:2381/ppa/AdminHome.htm
Go Links
invent
Help | Version
Licensing
Administration >>
Apply
Cancel
Done
Local intranet

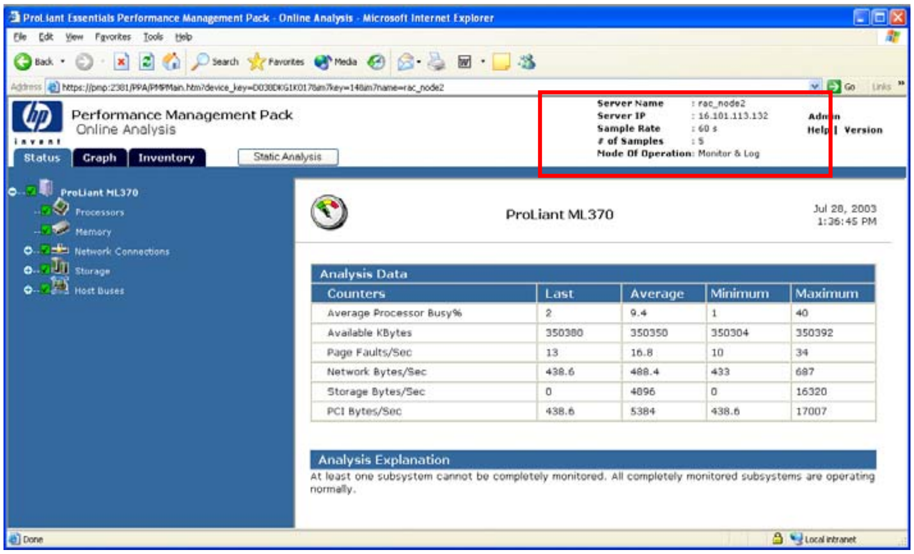
ProLiant Essentials Performance Management Pack
Licensing and Administration

Modify Parameters

Mode Of Operation: Monitor & Log
# of Samples: 5 Samples
Start Unmonitored Servers ☑

Server Name	Server IP Address
rac_node2	16.101.113.132

3. Close the Administration page.
4. At the PMP Online Analysis page, verify your logging settings.


ProLiant Essentials Performance Management Pack - Online Analysis - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://pmp:2381/PPA/PMPMain.htm?device_key=D030DKG1K0178am?key=148am?name=rac_node2
Go Links
Performance Management Pack
Online Analysis
Status
Graph
Inventory
Static Analysis
Admin
Help | Version
ProLiant ML370
Processors
Memory
Network Connections
Storage
Host Buses
Done
Local intranet

Server Name : rac_node2
Server IP : 16.101.113.132
Sample Rate : 60 s
# of Samples : 5
Mode Of Operation: Monitor & Log

ProLiant ML370

Jul 28, 2003
1:36:45 PM

Analysis Data

Counters	Last	Average	Minimum	Maximum
Average Processor Busy%	2	9.4	1	40
Available KBytes	350380	350350	350304	350392
Page Faults/Sec	13	16.8	10	34
Network Bytes/Sec	438.6	488.4	433	687
Storage Bytes/Sec	0	4896	0	16320
PCI Bytes/Sec	438.6	5384	438.6	17007

Analysis Explanation

At least one subsystem cannot be completely monitored. All completely monitored subsystems are operating normally.

5. Apply a workload using instructor supplied tools such as *cpustres.exe*, *eatmem.exe*, *leakyapp.exe*, *ttcp.exe*, or *iometer*, or by applying and previewing an OpenGL screen saver to the monitored server for 10 to 15 minutes. At the PMP Home page, monitor how the workload affects the target server.
6. To disable logging, set the mode of operation to the *Monitor* option.

Extracting data

Before data can be analyzed offline, it must be extracted from the performance database. Data is extracted from the database in XML format. To perform data extraction, use the data extraction tool.

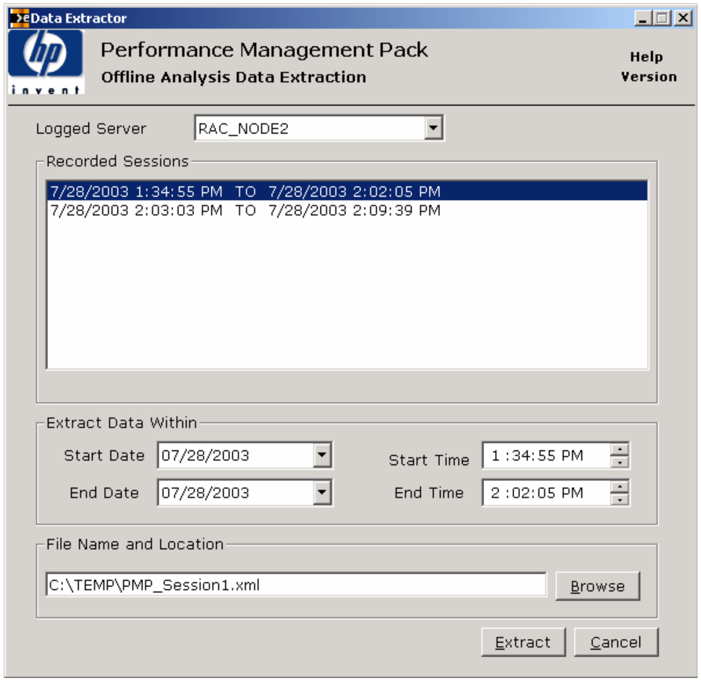
You can extract statistics from desired servers, selected recorded sessions, and specified data/time ranges. The statistical output is an XML file that is used for offline analysis.

1. Select *Start* → *Programs* → *Performance Management Pack* → *Data Extractor* to launch the data extraction tool.
2. At the Offline Analysis Data Extraction window, select the desired options and click *Extract*.
   - **Logged Server** — Select the desired target server.
   - **Recorded Sessions** — Select the desired recorded session.
   - **Start Date and Start Time** — Select a starting date and time.
   - **End Date and End Time** — Select an ending date and time.

   Note

   The Start Date, Start Time, End Date, and End Time parameters **must** fall within the data and time of the recorded session.

   - **File Name and Location** — Enter the location and the file name of the output. With PMP 2.1, you can enter an output file name with or without the XML extension.



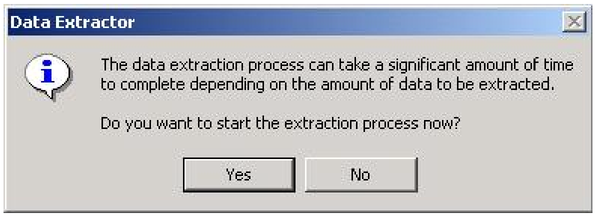
Logged Server: RAC_NODE2

7/28/2003 1:34:55 PM TO 7/28/2003 2:02:05 PM
7/28/2003 2:03:03 PM TO 7/28/2003 2:09:39 PM

Start Date: 07/28/2003
Start Time: 1 :34:55 PM
End Date: 07/28/2003
End Time: 2 :02:05 PM

C:\TEMP\PMP_Session1.xml

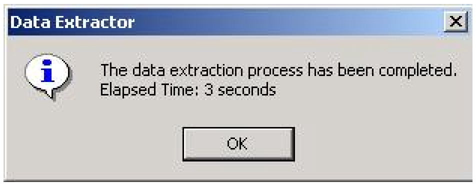
3. At the following Data Extractor message window, click *Yes*.



The data extraction process can take a significant amount of time to complete depending on the amount of data to be extracted.

Do you want to start the extraction process now?

4. When the extraction completes, the following Data Extractor message window displays. Click *OK* → *Cancel*.



The data extraction process has been completed.
Elapsed Time: 3 seconds

Using the Offline Analysis tool

To view recorded data sessions, use the Offline Analysis tool.

Note

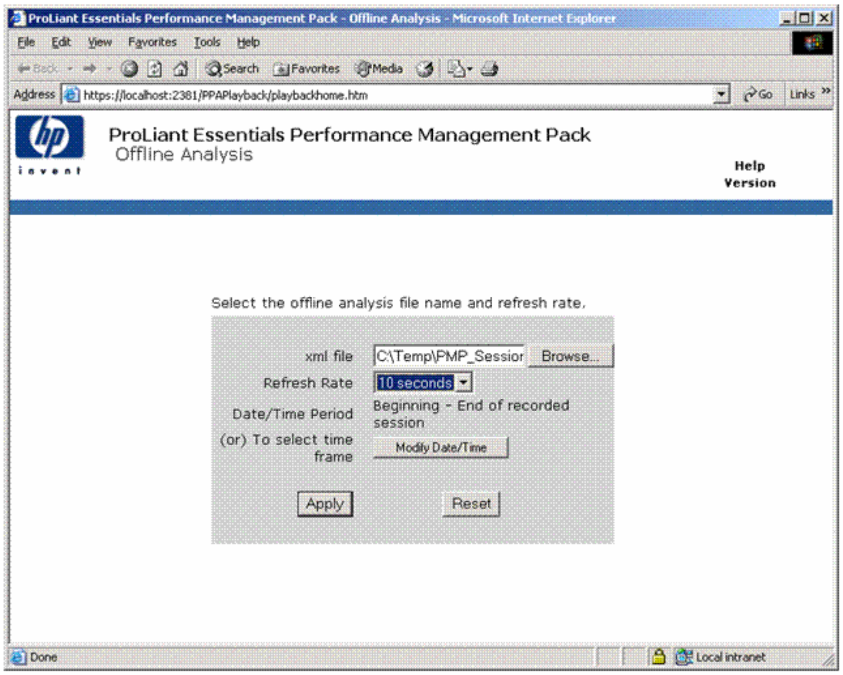
The Offline Analysis tool is also helpful when analyzing performance trends. It enables playback of any performance session that is recorded in the database repository.

You must have an XML-formatted file available for offline analysis.

1. To launch the Offline Analysis tool, select *Start* → *Programs* → *Performance Management Pack* → *Offline Analysis*.
2. At the Offline Analysis screen, select the desired options and click *Apply*.
   - **xml file** — The XML file generated by the data extractor tool.
   - **Refresh Rate** — The playback rate. If set to 30 seconds, the playback data is refreshed every 30 seconds.
   - **Start date and time** — The starting date and time of the playback.
   - **End date and time** — The ending date and time of the playback.

Note

The start and end dates and times **must** fall within the range of collected data. Click *Modify Date/Time* to display a page where you can adjust the start and end date/time.


ProLiant Essentials Performance Management Pack - Offline Analysis - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://localhost:2381/PPAPlayback/playbackhome.htm
Go Links
ProLiant Essentials Performance Management Pack
Offline Analysis
invent
Help
Version
Browse...
Modify Date/Time
Apply
Reset
Done
Local intranet

Select the offline analysis file name and refresh rate.

xml file C:\Temp\PMP_Sessior

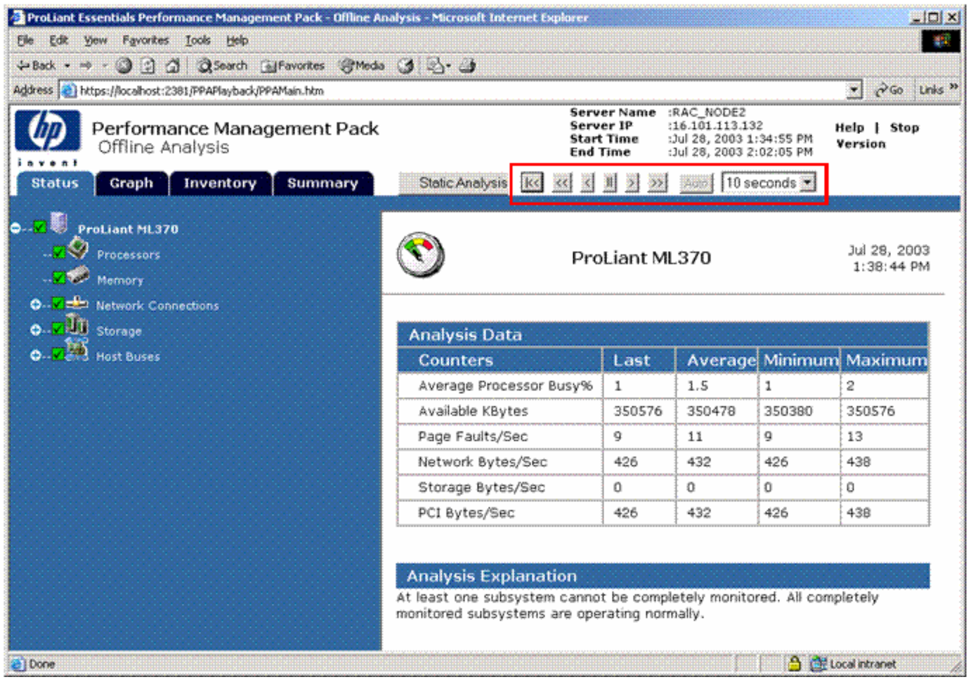
Refresh Rate 10 seconds

Date/Time Period Beginning - End of recorded session

(or) To select time frame

3. You can control the offline analysis using the control buttons near the top of the Offline Analysis window.

    - **|<<, <<, <, ||, >, and** >> — Click these buttons to manually navigate through the collected samples.
    - **Auto** — Click this button to advance automatically through the collected samples at the refresh rate.



Server Name :RAC_NODE2
Server IP :16.101.113.132
Start Time :Jul 28, 2003 1:34:55 PM
End Time :Jul 28, 2003 2:02:05 PM

ProLiant ML370

Jul 28, 2003
1:38:44 PM

Analysis Data

Counters	Last	Average	Minimum	Maximum
Average Processor Busy%	1	1.5	1	2
Available KBytes	350576	350478	350380	350576
Page Faults/Sec	9	11	9	13
Network Bytes/Sec	426	432	426	438
Storage Bytes/Sec	0	0	0	0
PCI Bytes/Sec	426	432	426	438

Analysis Explanation

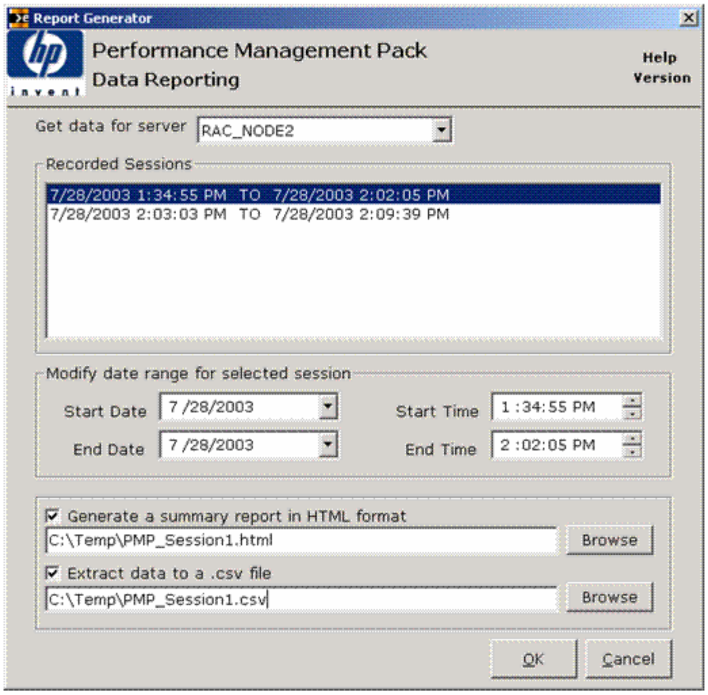
At least one subsystem cannot be completely monitored. All completely monitored subsystems are operating normally.

4. When you have completed the playback, click *Stop* and close the window.

Reporting

The data reporting tool creates reports that show the percentage of time the server was in a bottleneck state and the overall performance utilization for a server, categorized by its subsystems. These summary reports can be generated from the performance database and then stored in either an HTML or a comma-separated-value (CSV) file for import into desktop analysis or reporting tools.

1. Click *Start* → *Programs* → *Performance Management Pack* → *Report Generator* to launch the data reporting tool.
2. At the Data Reporting screen, select the desired options and click *OK*.
    - **Get data for server** — If the performance database contains data for multiple target servers, select the appropriate server.
    - **Recorded Sessions** — If the performance database contains multiple recorded sessions for the selected server, select the desired recorded session from this list.
    - **Modify date range for selected session** — Specify the date and time ranges for the report.
    - **Generate a summary report in HTML format** — Select this option if the HTML format is desired, and then enter the appropriate path and file name.
    - **Extract data to a .csv file** — If the CSV format is desired, select this option, and then enter the appropriate path and file name.



Get data for server: RAC_NODE2

Recorded Sessions:
7/28/2003 1:34:55 PM TO 7/28/2003 2:02:05 PM
7/28/2003 2:03:03 PM TO 7/28/2003 2:09:39 PM

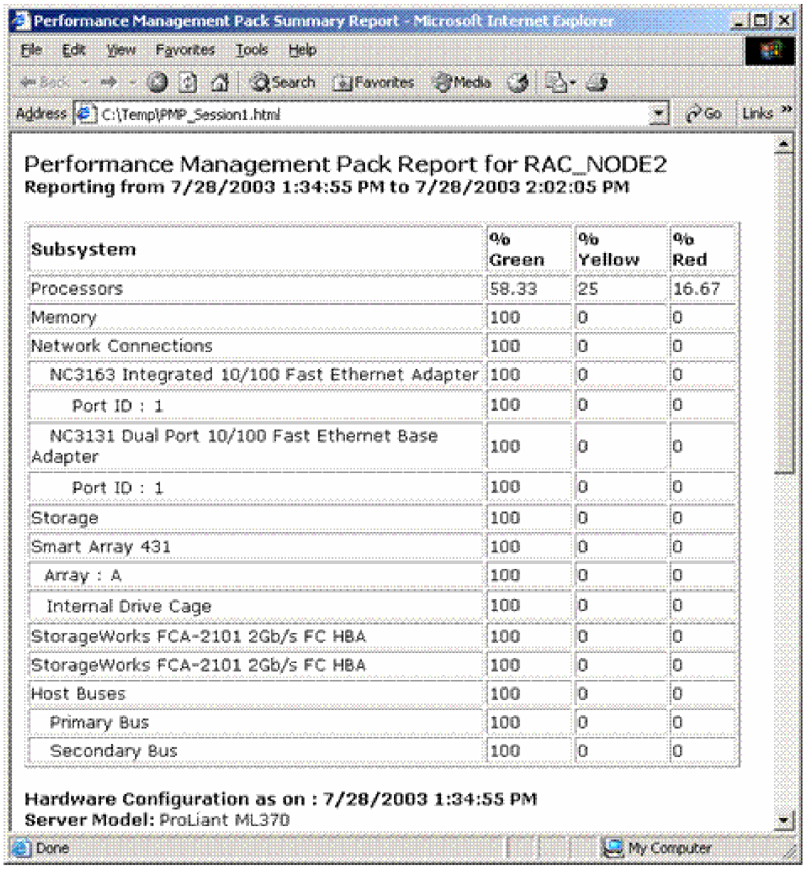
Modify date range for selected session:
Start Date: 7 /28/2003
End Date: 7 /28/2003
Start Time: 1 :34:55 PM
End Time: 2 :02:05 PM

☑ Generate a summary report in HTML format
C:\Temp\PMP_Session1.html

☑ Extract data to a .csv file
C:\Temp\PMP_Session1.csv

3. At the completion window, click *OK*. Click *Cancel* to exit the application.
4. If Microsoft Excel is installed, the .CSV file will automatically be imported into an Excel worksheet.

   The following screen shot illustrates sample HTML output.


Performance Management Pack Summary Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address C:\Temp\PMP_Session1.html
Go Links
Done
My Computer

Performance Management Pack Report for RAC_NODE2
Reporting from 7/28/2003 1:34:55 PM to 7/28/2003 2:02:05 PM

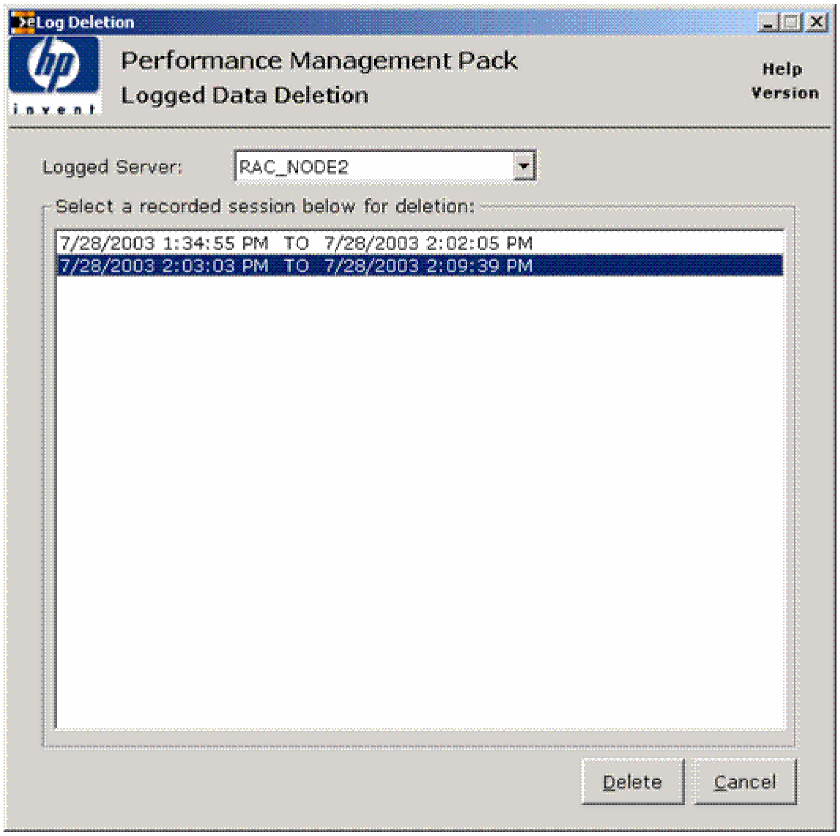
Subsystem	**% Green**	**% Yellow**	**% Red**
Processors	58.33	25	16.67
Memory	100	0	0
Network Connections	100	0	0
NC3163 Integrated 10/100 Fast Ethernet Adapter	100	0	0
Port ID : 1	100	0	0
NC3131 Dual Port 10/100 Fast Ethernet Base Adapter	100	0	0
Port ID : 1	100	0	0
Storage	100	0	0
Smart Array 431	100	0	0
Array : A	100	0	0
Internal Drive Cage	100	0	0
StorageWorks FCA-2101 2Gb/s FC HBA	100	0	0
StorageWorks FCA-2101 2Gb/s FC HBA	100	0	0
Host Buses	100	0	0
Primary Bus	100	0	0
Secondary Bus	100	0	0

Hardware Configuration as on : 7/28/2003 1:34:55 PM
Server Model: ProLiant ML370

Deleting logged data

The logged data deletion tool enables you to delete recorded sessions from the performance database. Use this tool on a regular basis to remove unwanted recorded sessions and to reduce database size.

1. Select *Start* → *Programs* → *Performance Management Pack* → *Log Deletion* to launch the logged data deletion tool.
2. At the Logged Data Deletion screen, select the desired options and click *Delete*.
   - **Logged Server** — If the performance database contains data for multiple target servers, select the appropriate server.
   - **Select a recorded session below for deletion** — If the performance database contains multiple recorded sessions for the selected server, choose the desired session from this list.



Logged Server: RAC_NODE2

Select a recorded session below for deletion:

7/28/2003 1:34:55 PM TO 7/28/2003 2:02:05 PM
7/28/2003 2:03:03 PM TO 7/28/2003 2:09:39 PM

3. Click *Cancel* to exit the application.

Configuring performance-based alerts

PMP supports proactive notification of device status change using the Insight Manager 7 notification mechanism. Using any of the supported notification methods, you can set up rules to generate these notifications when a performance issue is detected.

Using knowledge you have learned in this course, configure and test a performance-based application launch alert as follows:

> **Note**
>
> You must configure HP Insight Manager 7 to query the Performance Status Change event, which can be found in the Event(s) of type list under HTTP EVENTS.

1. Create a Windows command file called *netsend.cmd*. The contents of this file should be as follows (substitute `<server>` with the correct machine name where you would like to receive the alert):

   ```
   Net send <server> “PMP Performance Status Change”
   ```

2. Execute the *netsend.cmd* file to ensure it is functioning properly. You should receive a Messenger Service popup window with the preceding message upon execution.
3. Using the knowledge you have gained from this course, configure Insight Manager 7 to generate a performance-based alert when the monitored server performance changes. Use the PMP Alerting demo as a reference, if necessary.
4. Introduce a workload at the monitored server and validate the alerting to function as expected. For every performance change at the monitored server, PMP should generate an alert using the Insight Manager 7 alerting mechanism (a Messenger Service popup window should display stating that the performance status change has occurred).

Comparing current performance with baseline performance

If a performance baseline exists, it can help in analyzing performance trends and determining performance bottlenecks. If it does not exist, you should create one as soon as the server performance returns to acceptable levels.

Performance baseline and all subsequent performance measurements to be compared against this baseline should be created using the same tool, preferably PMP. To create the performance measurement:

1. Start PMP and set the mode of operation to any setting that includes logging – *Monitor and Log* or *Monitor, Log, and Alert*. Set the remaining parameters to desired levels.
2. The performance statistics will be automatically logged into the PMP database repository. The logging session will close when you change the mode of operation to a non-logging setting.
3. Use the Report Generator to extract statistics associated with the desired sessions and to write them to a CSV file. Use one session as the baseline; use another session to compare against the baseline.
4. Import these two CSV files into a spreadsheet application such as Excel. Compare different statistics and determine which performance attributes have changed, when, and by how much. The CSV file contains all parameters collected by PMP, organized in labeled and easy-to-read columns, with values dated according to when they were collected.

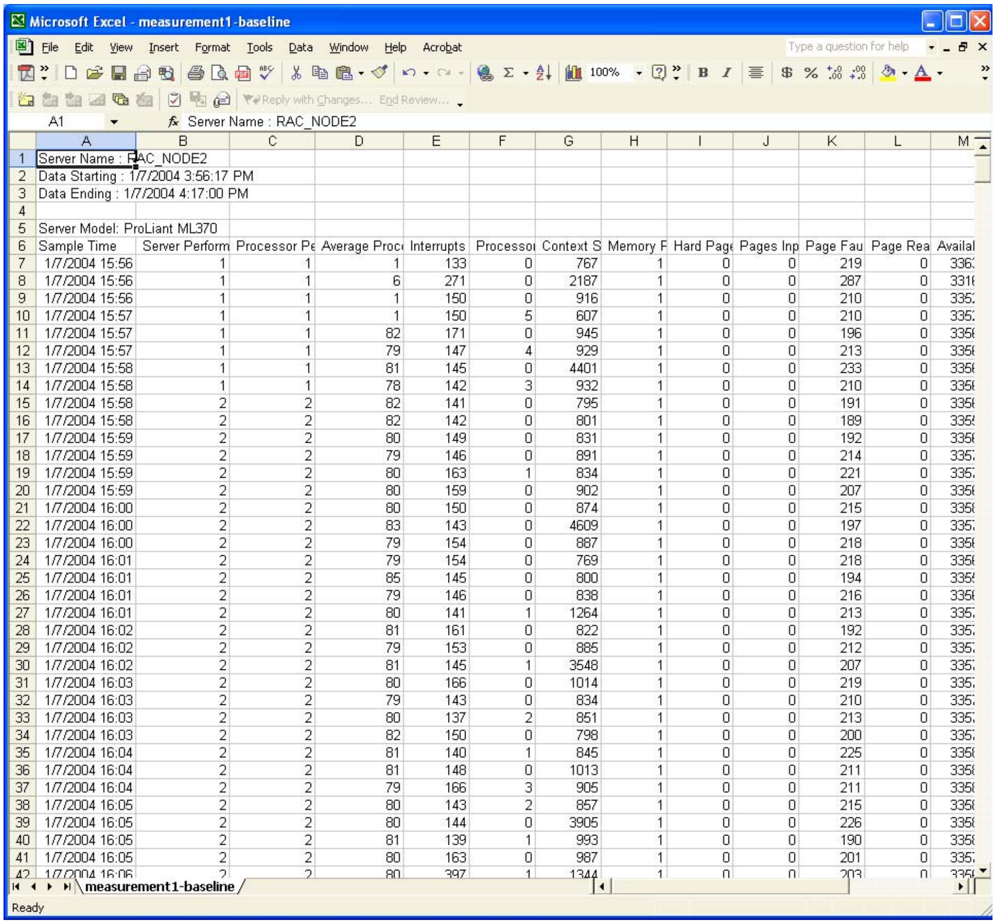
Example of working with logged performance measurements

You have taken two measurements using the PMP logging feature—one when you initially deployed the server and the performance was meeting expectations; the other after the users began reporting long server response times.

Both measurement sessions were stored in the PMP database repository. To determine what has changed and when, compare the later measurement with the baseline.

1. At the performance analysis server, start the Report Generator, select the appropriate server and session associated with the baseline measurement, and generate a CSV file named *measurement1-baseline.csv*.
2. Repeat the previous step to extract the measurement session you want to compare with the baseline. Name this CSV file *measurement2.csv*.

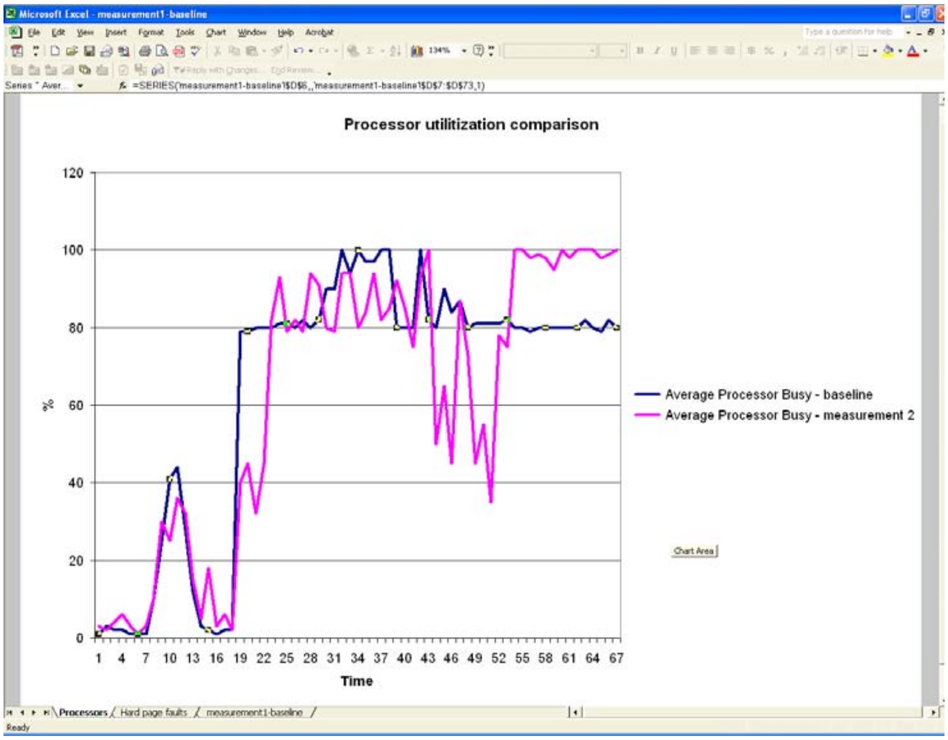
3. Open both CSV files with Excel. Each file will resemble the following example.



A1 Server Name : RAC_NODE2

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Server Name : RAC_NODE2												
2	Data Starting : 1/7/2004 3:56:17 PM												
3	Data Ending : 1/7/2004 4:17:00 PM												
4													
5	Server Model: ProLiant ML370												
6	Sample Time	Server Perform	Processor Pe	Average Proc	Interrupts	Processo	Context S	Memory F	Hard Page	Pages Inp	Page Fau	Page Rea	Availal
7	1/7/2004 15:56	1	1	1	133	0	767	1	0	0	219	0	336
8	1/7/2004 15:56	1	1	6	271	0	2187	1	0	0	287	0	331
9	1/7/2004 15:56	1	1	1	150	0	916	1	0	0	210	0	335
10	1/7/2004 15:57	1	1	1	150	5	607	1	0	0	210	0	335
11	1/7/2004 15:57	1	1	82	171	0	945	1	0	0	196	0	335
12	1/7/2004 15:57	1	1	79	147	4	929	1	0	0	213	0	335
13	1/7/2004 15:58	1	1	81	145	0	4401	1	0	0	233	0	335
14	1/7/2004 15:58	1	1	78	142	3	932	1	0	0	210	0	335
15	1/7/2004 15:58	2	2	82	141	0	795	1	0	0	191	0	335
16	1/7/2004 15:58	2	2	82	142	0	801	1	0	0	189	0	335
17	1/7/2004 15:59	2	2	80	149	0	831	1	0	0	192	0	335
18	1/7/2004 15:59	2	2	79	146	0	891	1	0	0	214	0	335
19	1/7/2004 15:59	2	2	80	163	1	834	1	0	0	221	0	335
20	1/7/2004 15:59	2	2	80	159	0	902	1	0	0	207	0	335
21	1/7/2004 16:00	2	2	80	150	0	874	1	0	0	215	0	335
22	1/7/2004 16:00	2	2	83	143	0	4609	1	0	0	197	0	335
23	1/7/2004 16:00	2	2	79	154	0	887	1	0	0	218	0	335
24	1/7/2004 16:01	2	2	79	154	0	769	1	0	0	218	0	335
25	1/7/2004 16:01	2	2	85	145	0	800	1	0	0	194	0	335
26	1/7/2004 16:01	2	2	79	146	0	838	1	0	0	216	0	335
27	1/7/2004 16:01	2	2	80	141	1	1264	1	0	0	213	0	335
28	1/7/2004 16:02	2	2	81	161	0	822	1	0	0	192	0	335
29	1/7/2004 16:02	2	2	79	153	0	885	1	0	0	212	0	335
30	1/7/2004 16:02	2	2	81	145	1	3548	1	0	0	207	0	335
31	1/7/2004 16:03	2	2	80	166	0	1014	1	0	0	219	0	335
32	1/7/2004 16:03	2	2	79	143	0	834	1	0	0	210	0	335
33	1/7/2004 16:03	2	2	80	137	2	851	1	0	0	213	0	335
34	1/7/2004 16:03	2	2	82	150	0	798	1	0	0	200	0	335
35	1/7/2004 16:04	2	2	81	140	1	845	1	0	0	225	0	335
36	1/7/2004 16:04	2	2	81	148	0	1013	1	0	0	211	0	335
37	1/7/2004 16:04	2	2	79	166	3	905	1	0	0	211	0	335
38	1/7/2004 16:05	2	2	80	143	2	857	1	0	0	215	0	335
39	1/7/2004 16:05	2	2	80	144	0	3905	1	0	0	226	0	335
40	1/7/2004 16:05	2	2	81	139	1	993	1	0	0	190	0	335
41	1/7/2004 16:05	2	2	80	163	0	987	1	0	0	201	0	335
42	1/7/2004 16:06	2	2	80	397	1	1344	1	0	0	203	0	335

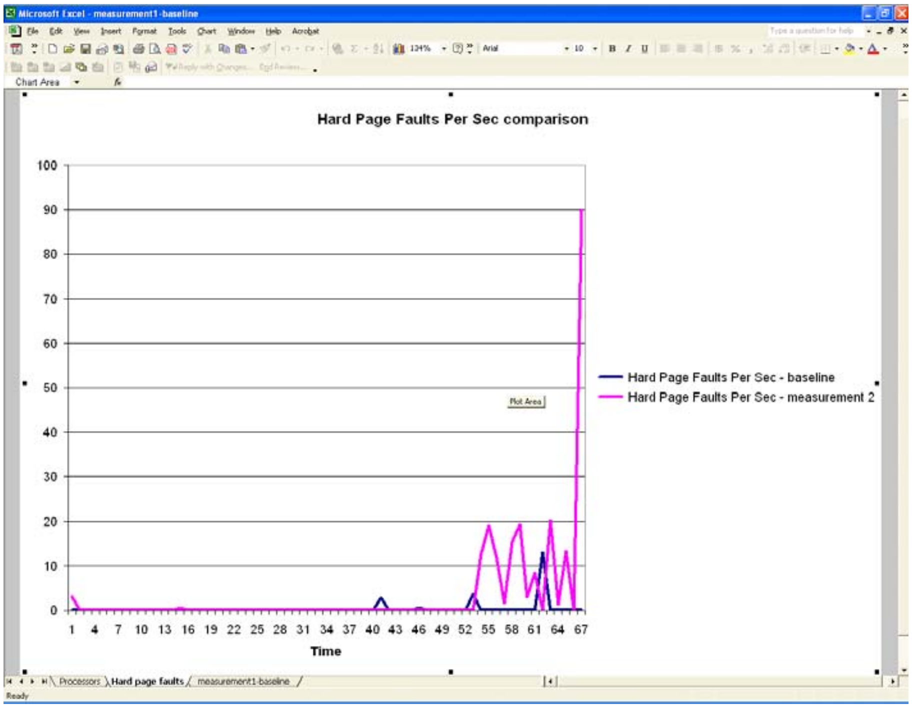
4. Graph the selected data points for visual comparison. Use any applicable Excel feature to determine the cause of the performance discrepancy. The following graphics compare processors, paging, and available memory.



=SERIES('measurement1-baseline'!$D$6,,'measurement1-baseline'!$D$7:$D$73,1)

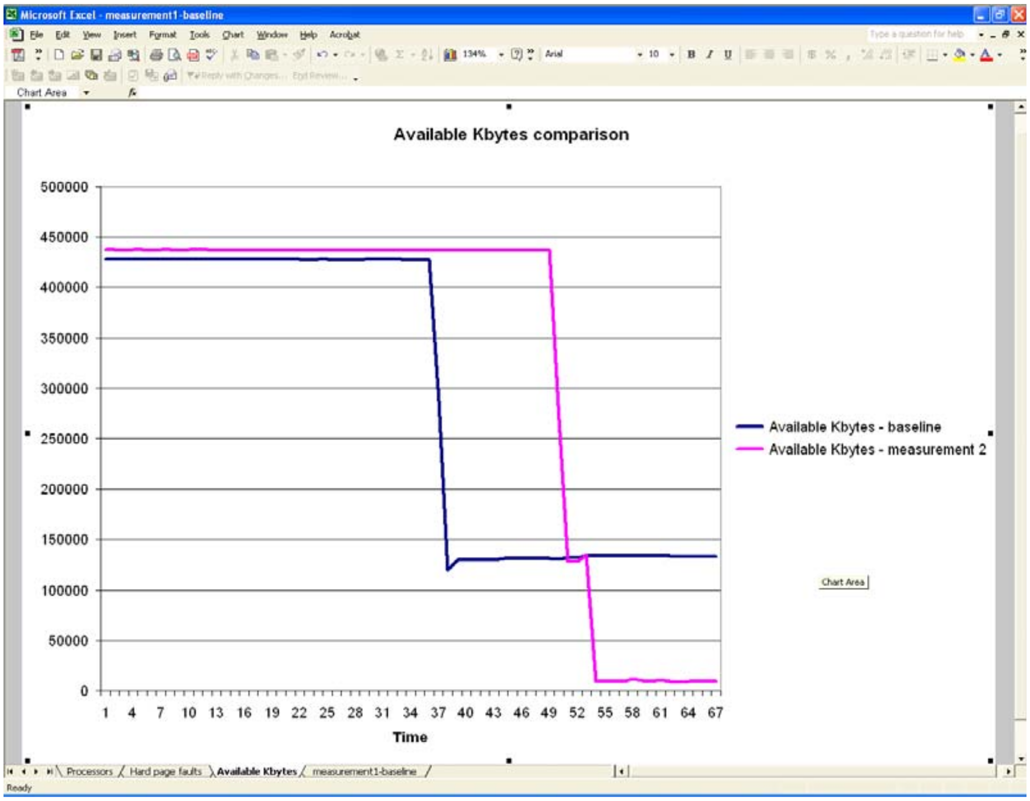
From this comparison you can conclude that the baseline processor utilization is approximately 80%. Some sporadic processor utilization occurs between data point 19 and 49, which can be contributed to an application initializing and performance reaching a steady state.

Measurement 2 indicates a similar pattern; however, the performance does not stabilize around 80%. Instead, the processor utilization peaks at 100%, and fluctuates between 95% and 100%.



Sample hard page faults per second comparison

This graph compares hard page faults of the baseline and of the second measurement. The baseline indicates low paging; the second measurement exposes erratic paging, particularly after data point 54. This trend coincides with the processor utilization graph, where the processor utilization increases significantly.



Sample available KB comparison

Here, the baseline indicates that after the applications initialize, the available memory drops to approximately 135,000KB. The second measurement exposes the same pattern for a short period of time, but then the available memory drops to a very low level. This could be attributed to the same application requesting additional memory, or to a new application starting and requesting memory that is not available. The two previous graphs indicate that during the same time the processor utilization peaks, and severe paging occurs.

Further investigation into these performance trends is warranted, but is not covered in this document. Instead, this section shows examples of how to use the performance statistics gathered by PMP to perform trend analysis and comparison.

Removing PMP (optional)

PMP and Insight Manager 7 must be uninstalled separately from the system. Uninstalling one does not uninstall the other.

Uninstalling PMP

To remove PMP from your system:

> **Note**
> Uninstalling PMP will **not** remove Insight Manager 7 from your system.

1. Close all PMP browser sessions.
2. Select *Start* → *Programs* → *Performance Management Pack* → *PMP Uninstall*.

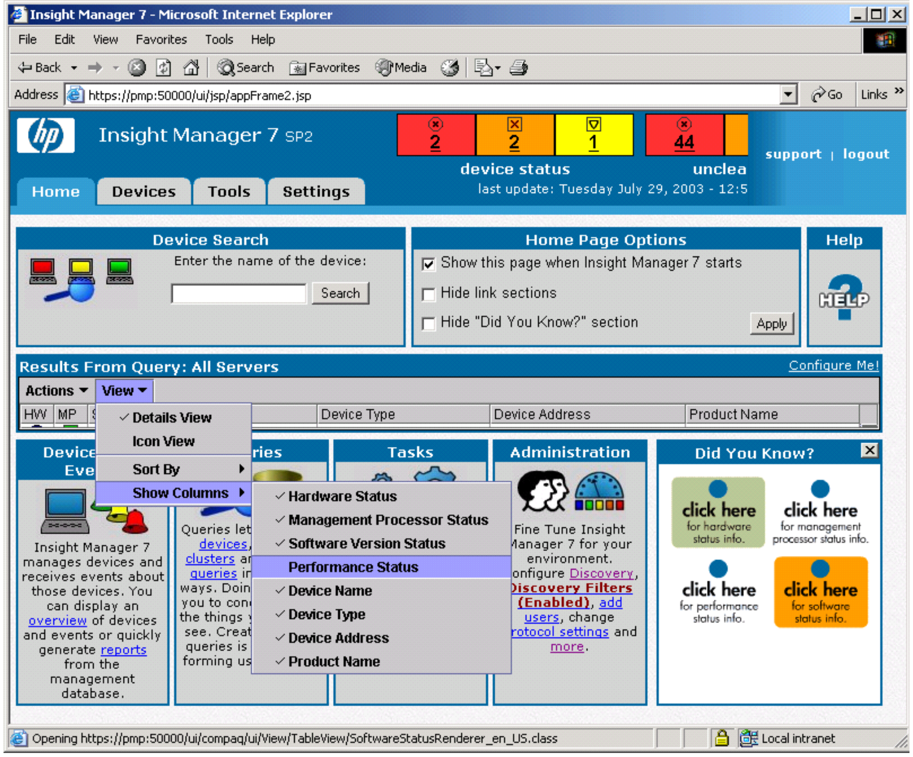
   or

   Select *Start* → *Settings* → *Control Panel* → *Add/Remove Programs* → *Performance Management Pack* → *Change/Remove*.
3. Restart the system.
4. Delete the folder where PMP was installed. The default location is *C:\Program Files\HP\ProLiant Performance Analyzer.*

Insight Manager 7 remains unaffected by uninstalling PMP. The PF column on the Insight Manager 7 Home page remains after uninstalling PMP. Clicking the PF column displays *HTTP Status 404, Page not found* in the newly opened window.

Hiding the Insight Manager 7 PF column

To prevent the PF column from displaying on the Insight Manager 7 Home page, at the Insight Manager 7 Home page, click *View*. Then unselect *Show Columns* → *Performance Status*.


Insight Manager 7 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address https://pmp:50000/ui/jsp/appFrame2.jsp
Insight Manager 7 SP2
2 2 1 44
device status
unclea
last update: Tuesday July 29, 2003 - 12:5
support | logout
Home Devices Tools Settings
Device Search
Enter the name of the device:
Search
Home Page Options
☑ Show this page when Insight Manager 7 starts
☐ Hide link sections
☐ Hide "Did You Know?" section
Apply
Help
Results From Query: All Servers
Configure Me!
Actions View
HW MP
Device Type
Device Address
Product Name
✓ Details View
Icon View
Sort By
Show Columns
✓ Hardware Status
✓ Management Processor Status
✓ Software Version Status
Performance Status
✓ Device Name
✓ Device Type
✓ Device Address
✓ Product Name
Tasks
Administration
Did You Know?
click here for hardware status info.
click here for management processor status info.
click here for performance status info.
click here for software status info.
Opening https://pmp:50000/ui/compaq/ui/View/TableView/SoftwareStatusRenderer_en_US.class
Local intranet

Uninstalling Insight Manager 7

To remove Insight Manager 7 from your system, follow these steps:

Note

Uninstalling Insight Manager 7 will **not** remove PMP from your system.

---

1. Select *Start* → *Programs* → *Insight Manager 7 SP2* → *Uninstall Insight Manager 7*.

   or

   Select *Start* → *Settings* → *Control Panel* → *Add/Remove Programs* → *Insight Manager 7* → *Change/Remove*.
2. After uninstalling Insight Manager 7, you might need to remove any configured ODBC (Open Database Connectivity) connections. In the Control Panel, click *Administrative Tools* → *Data Sources (ODBC)*. On the System DSN tab, select *INSIGHT_DB_V3* and *INSIGHT_VCDB* and click *Remove*.
3. Restart the system.

Exercise 2 — Monitoring and tuning a database server

Monitoring and tuning is a repetitive process, involving modifications to the configuration, applying a predetermined workload, and measuring the results. This section gives you an insight into such a process, using a database server environment as the reference point.

Preparing the environment

To prepare the environment, install the database software and the benchmark suite according to the following instructions. Ask your instructor for the path to the required installation files. In most cases, the software will reside on the instructor server and is accessible over the network.

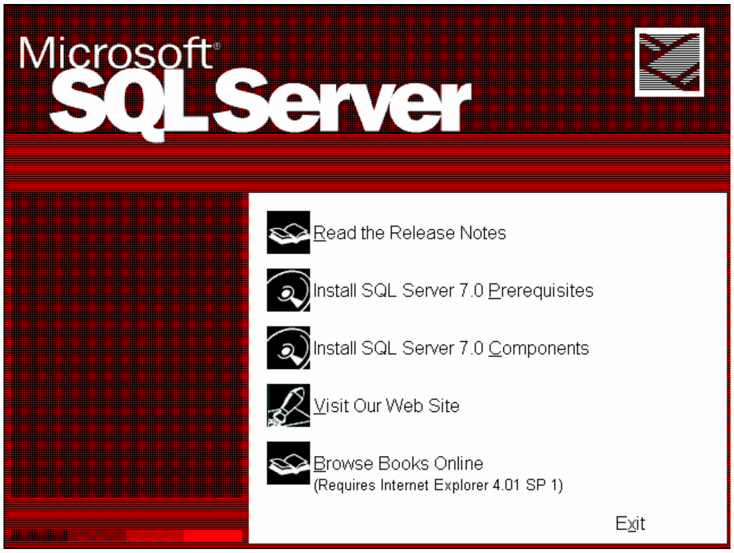
Installing and configuring Microsoft SQL Server 7.0

You must install SQL Server 7.0 on both the server and the client machines.

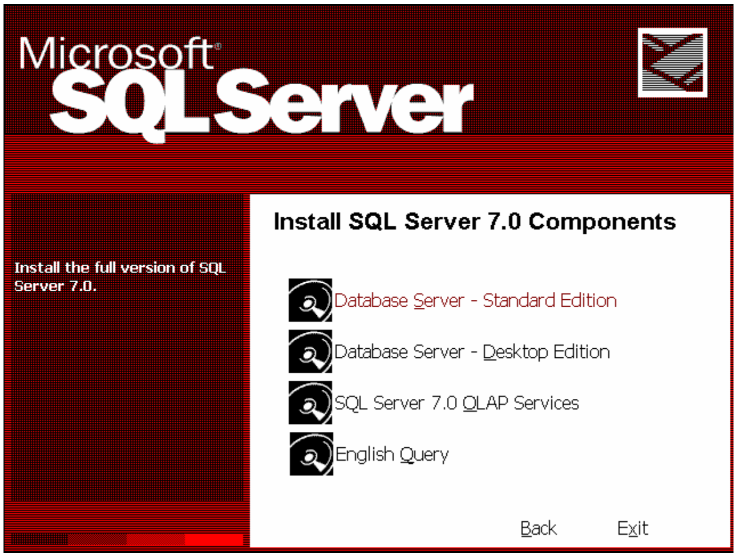
Target server installation

This section contains detailed instructions on installing Microsoft SQL Server 7.0 Standard Edition on a server. It assumes that SQL Server has never been installed on your system. The approximate time to install SQL Server 7.0 is five minutes.

1. Map a drive letter to the shared directory containing SQL Server installation files instead of using the UNC path. (With the Universal Naming Convention (UNC) path, you might experience installation problems.)
2. Connect to the shared directory where the SQL Server installation files reside and execute the *autorun.exe* file. If you are installing SQL Server directly from the CD-ROM, the autorun.exe program will be executed automatically. At the following screen, select *Install SQL Server 7.0 Components*.


Microsoft
SQL Server
Read the Release Notes
Install SQL Server 7.0 Prerequisites
Install SQL Server 7.0 Components
Visit Our Web Site
Browse Books Online
(Requires Internet Explorer 4.01 SP 1)
Exit

3. At the following screen, select *Database Server – Standard Edition*.

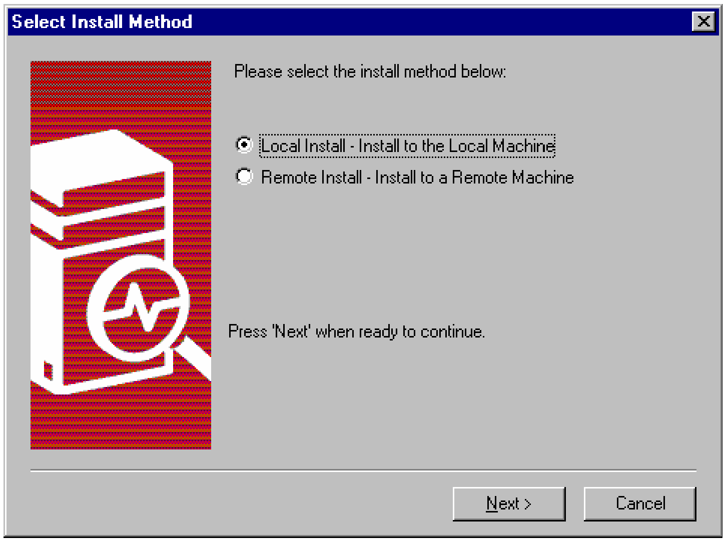


Install SQL Server 7.0 Components

Install the full version of SQL Server 7.0.

Database Server - Standard Edition
Database Server - Desktop Edition
SQL Server 7.0 OLAP Services
English Query
Back
Exit

4. At the Select Install Method screen, select *Local Install – Install to the Local Machine* and click *Next*.



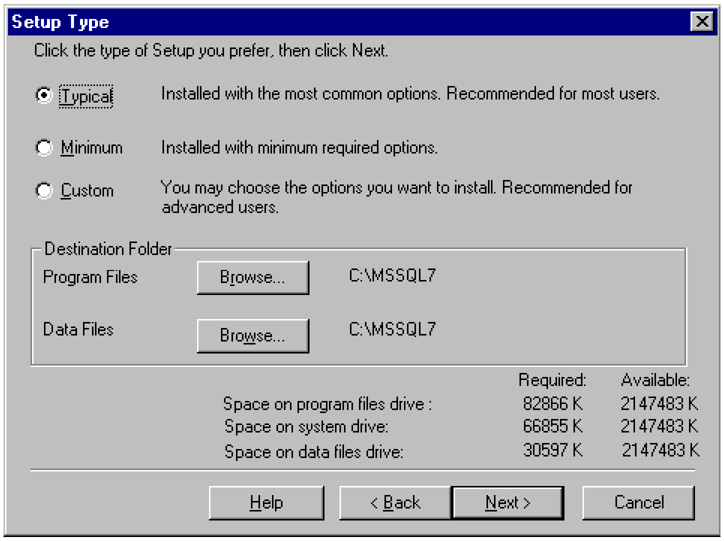
Select Install Method

Please select the install method below:

● Local Install - Install to the Local Machine
○ Remote Install - Install to a Remote Machine

Press 'Next' when ready to continue.

5. At the Welcome screen, click *Next*.
6. At the Software License Agreement screen, review the licensing information and click *Yes*.
7. At the User Information screen, enter your name and your company, and click *Next*.
8. At the Setup Type screen, accept the defaults and click *Next*.



Setup Type

Click the type of Setup you prefer, then click Next.

● Typical Installed with the most common options. Recommended for most users.

○ Minimum Installed with minimum required options.

○ Custom You may choose the options you want to install. Recommended for advanced users.

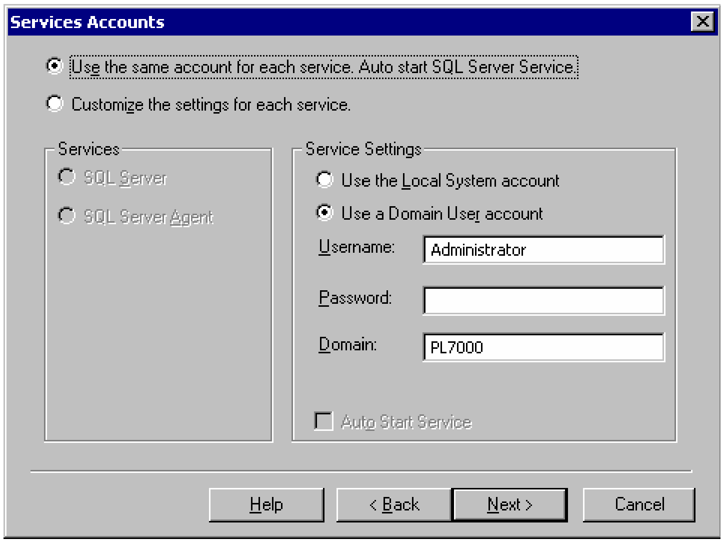
Destination Folder

Program Files: C:\MSSQL7

Data Files: C:\MSSQL7

	Required:	Available:
Space on program files drive :	82866 K	2147483 K
Space on system drive:	66855 K	2147483 K
Space on data files drive:	30597 K	2147483 K

9. At the Services Accounts screen, select *Use a Domain User account*, accept all other defaults, and click *Next*.



Services Accounts

● Use the same account for each service. Auto start SQL Server Service.

○ Customize the settings for each service.

Services

○ SQL Server

○ SQL Server Agent

Service Settings

○ Use the Local System account

● Use a Domain User account

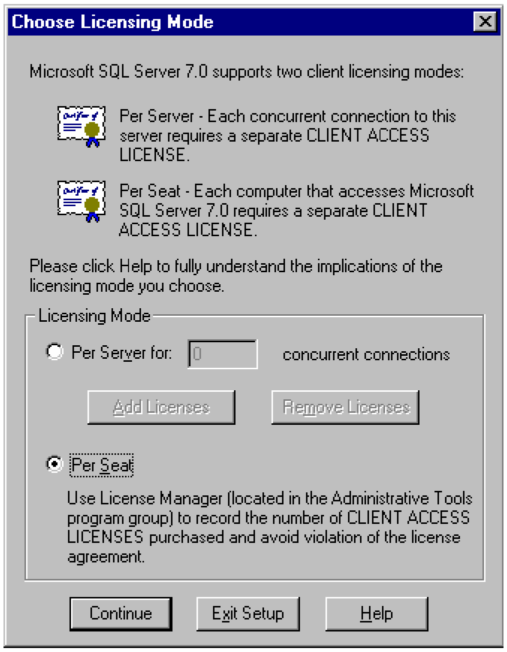
Username: Administrator

Password:

Domain: PL7000

☐ Auto Start Service

10. At the Start Copying Files screen, click *Next*.
11. At the Choose Licensing Mode screen, select *Per Seat* and click *Continue*.



Choose Licensing Mode

Microsoft SQL Server 7.0 supports two client licensing modes:

Per Server - Each concurrent connection to this server requires a separate CLIENT ACCESS LICENSE.

Per Seat - Each computer that accesses Microsoft SQL Server 7.0 requires a separate CLIENT ACCESS LICENSE.

Please click Help to fully understand the implications of the licensing mode you choose.

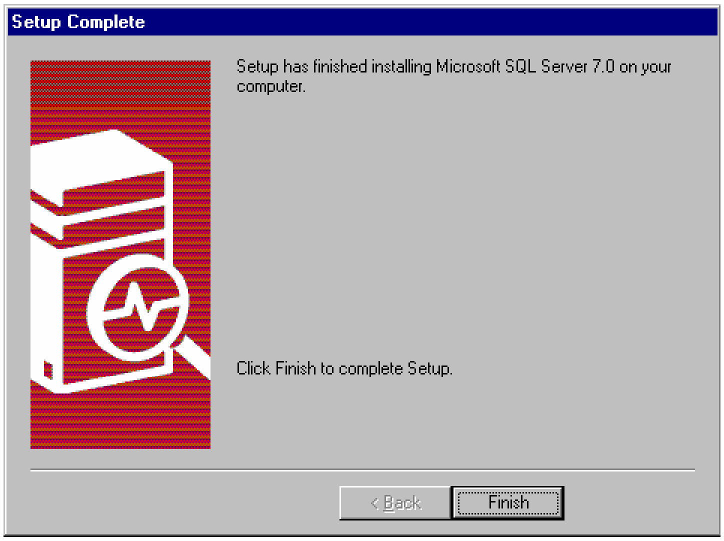
Licensing Mode

○ Per Server for: 0 concurrent connections

● Per Seat

Use License Manager (located in the Administrative Tools program group) to record the number of CLIENT ACCESS LICENSES purchased and avoid violation of the license agreement.

12. The installer program begins copying the necessary files. When finished, it presents the following screen. Click *Finish* to complete the installation and restart your system.



Setup Complete

Setup has finished installing Microsoft SQL Server 7.0 on your computer.

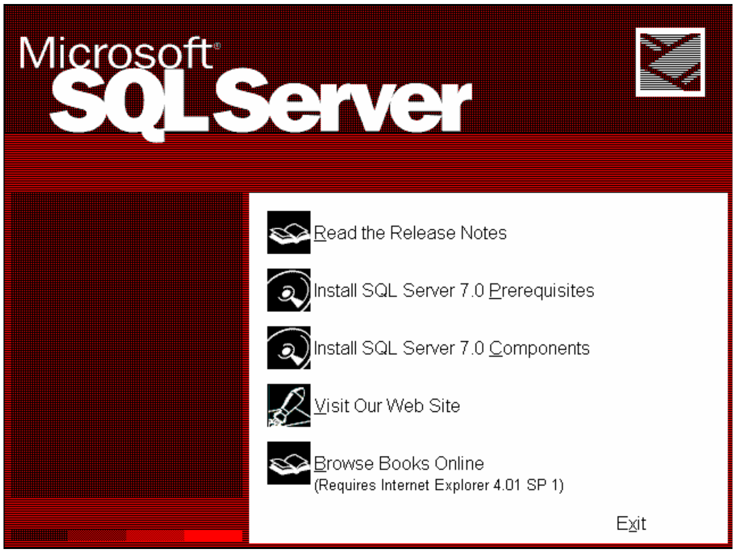
Click Finish to complete Setup.

13. After system reboot, ensure that the MSSQLServer service started successfully.

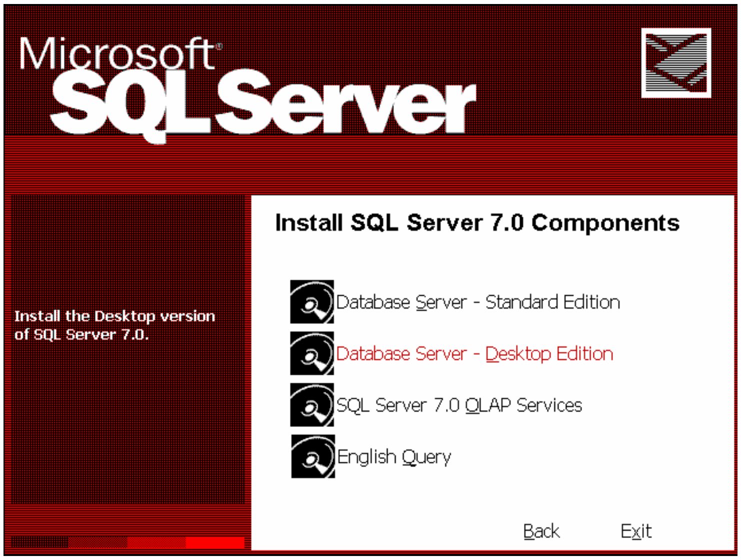
Client installation

To install SQL Server on the client machine, follow these steps. They assume that SQL Server has never been installed on this system. The approximate time to install SQL Server 7.0 client is less than five minutes.

1. Map a drive letter to the shared directory containing SQL Server installation files instead of using the UNC path. (With the Universal Naming Convention (UNC) path, you might experience installation problems.)
2. Connect to the shared directory where the SQL Server installation files reside and execute the *autorun.exe* file. If you are installing SQL Server directly from the CD-ROM, the autorun.exe program will be executed automatically. At the following screen, select *Install SQL Server 7.0 Components*.

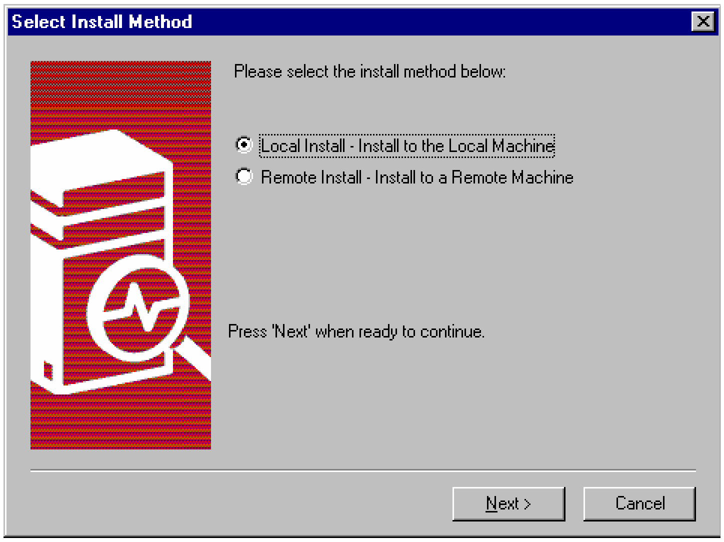

Microsoft SQL Server
Read the Release Notes
Install SQL Server 7.0 Prerequisites
Install SQL Server 7.0 Components
Visit Our Web Site
Browse Books Online
(Requires Internet Explorer 4.01 SP 1)
Exit

3. At the following screen, select *Database Server – Desktop Edition*.



Microsoft SQL Server
Install SQL Server 7.0 Components
Install the Desktop version of SQL Server 7.0.
Database Server - Standard Edition
Database Server - Desktop Edition
SQL Server 7.0 OLAP Services
English Query
Back
Exit

4. At the Select Install Method screen, select *Local Install – Install to the Local Machine* and click *Next*.



Select Install Method

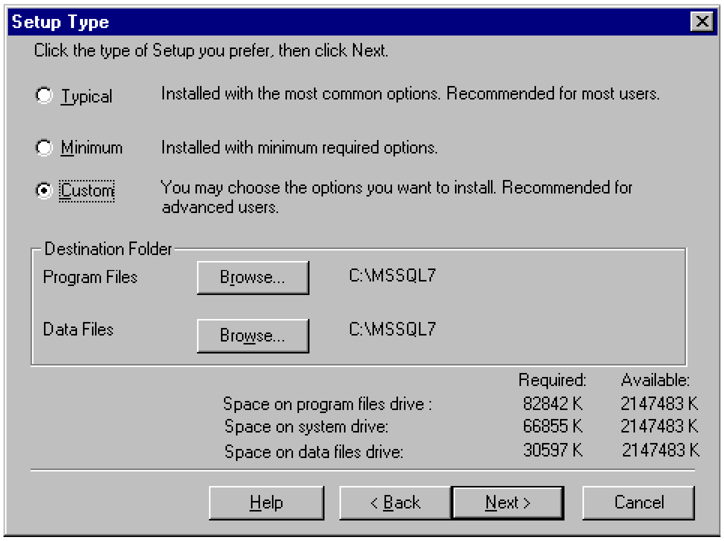
Please select the install method below:

● Local Install - Install to the Local Machine

○ Remote Install - Install to a Remote Machine

Press 'Next' when ready to continue.

5. At the Welcome screen, click *Next*.
6. At the Software License Agreement screen, review the licensing information and click *Yes*.
7. At the User Information screen, enter your name and your company and click *Next*.
8. At the Setup Type screen, select *Custom* and click *Next*.



Setup Type

Click the type of Setup you prefer, then click Next.

○ Typical — Installed with the most common options. Recommended for most users.

○ Minimum — Installed with minimum required options.

● Custom — You may choose the options you want to install. Recommended for advanced users.

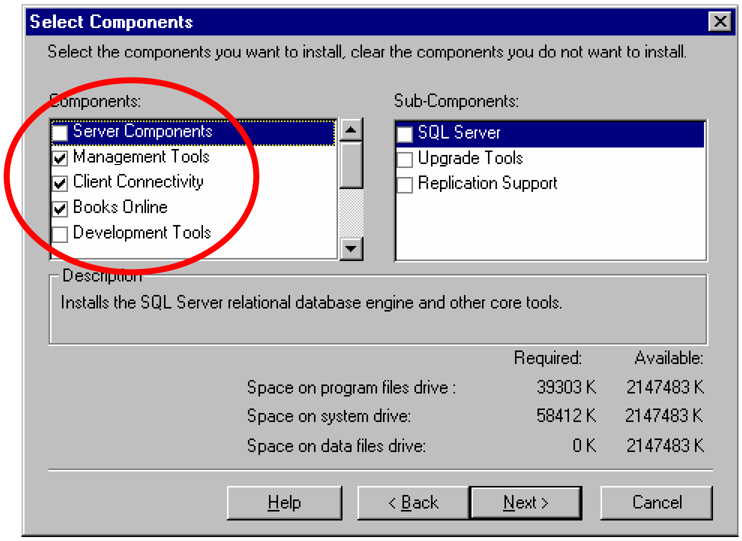
Destination Folder

Program Files: C:\MSSQL7

Data Files: C:\MSSQL7

	Required:	Available:
Space on program files drive :	82842 K	2147483 K
Space on system drive:	66855 K	2147483 K
Space on data files drive:	30597 K	2147483 K

9. At the Select Components screen, select *Management Tools*, *Client Connectivity*, and *Books Online* and click *Next*.



Select Components

Select the components you want to install, clear the components you do not want to install.

Components:

☐ Server Components
☑ Management Tools
☑ Client Connectivity
☑ Books Online
☐ Development Tools

Sub-Components:

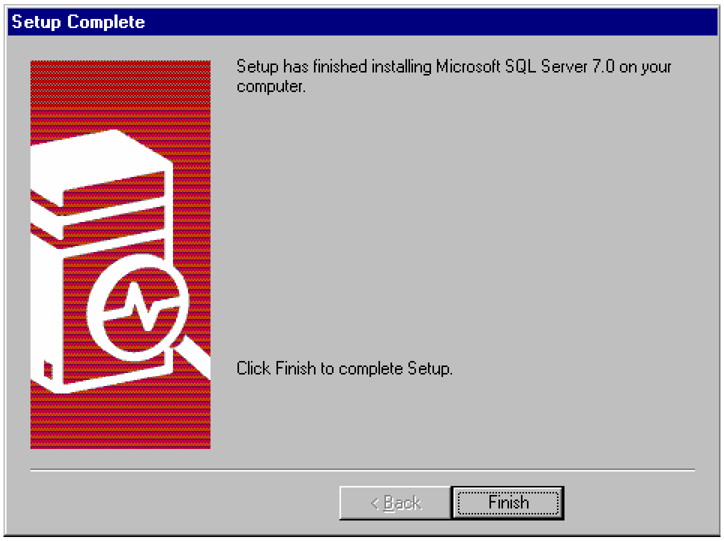
☐ SQL Server
☐ Upgrade Tools
☐ Replication Support

Description

Installs the SQL Server relational database engine and other core tools.

	Required:	Available:
Space on program files drive :	39303 K	2147483 K
Space on system drive:	58412 K	2147483 K
Space on data files drive:	0 K	2147483 K

10. At the Start Copying Files screen, click *Next*.
11. The installer program begins copying the necessary files. When finished, it presents the following screen. Click *Finish* to complete the installation and restart your system.



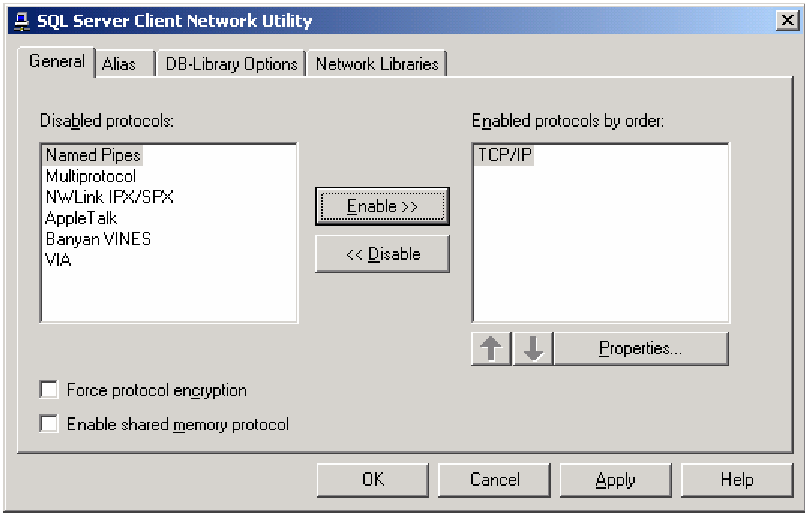
Setup has finished installing Microsoft SQL Server 7.0 on your computer.

Click Finish to complete Setup.

Client configuration

At the client machine, follow these steps to configure the client component of SQL Server for proper TCP/IP network connectivity.

1. From the SQL Server 7.0 program group (click *Start* → *Programs* → *Microsoft SQL Server 7.0*), click *Client Network Utility*.
2. At the *SQL Server Client Network Utility* screen, select the *General* tab and choose *TCP/IP* as the default network library. Then click *Add*.



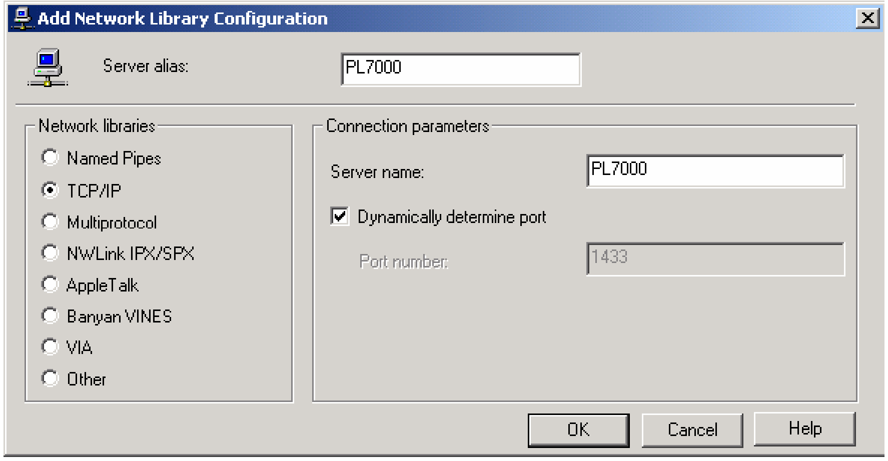
Disabled protocols:
- Named Pipes
- Multiprotocol
- NWLink IPX/SPX
- AppleTalk
- Banyan VINES
- VIA

Enabled protocols by order:
- TCP/IP

☐ Force protocol encryption

☐ Enable shared memory protocol

3. Click the *Alias* tab, click *Add*, enter the following parameters, and click *OK*.
   - Server alias — Enter the target server NetBIOS name.
   - Network libraries — Select *TCP/IP*.
   - Server name — Enter the target server NetBIOS name.
   - Port number — Select *Dynamically determine port*.



Server alias: PL7000

Network libraries
- ○ Named Pipes
- ● TCP/IP
- ○ Multiprotocol
- ○ NWLink IPX/SPX
- ○ AppleTalk
- ○ Banyan VINES
- ○ VIA
- ○ Other

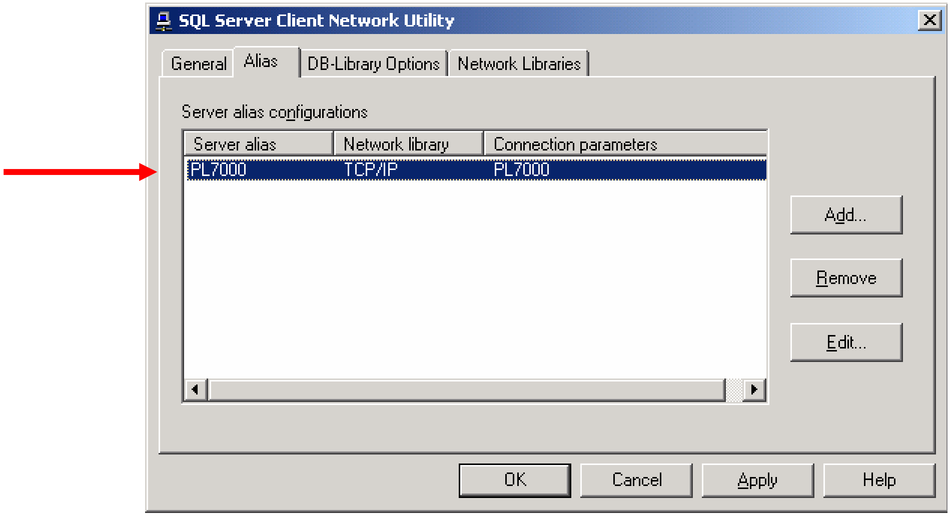
Connection parameters

Server name: PL7000

☑ Dynamically determine port

Port number: 1433

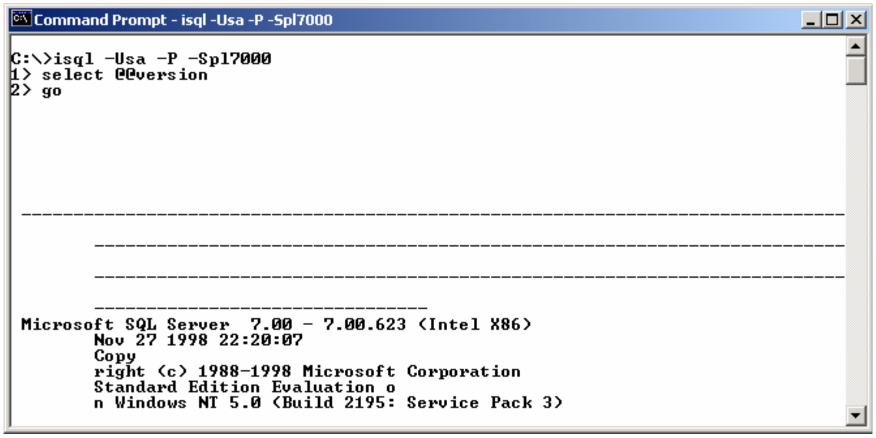
4. At the *SQL Server Client Network Utility* screen, verify that the new Server alias configuration entry is correct. Then click *OK* to exit the utility.



Server alias	Network library	Connection parameters
PL7000	TCP/IP	PL7000

5. To test the connectivity to the database server, open a command prompt window and enter the following command:

```
C:\> isql –Usa –P –Spl7000
1> select @@version
2> go
```



```
C:\>isql -Usa -P -Spl7000
1> select @@version
2> go




 -------------------------------------------------------------------------------

        -----------------------------------------------------------------------

        -----------------------------------------------------------------------

        --------------------------------
 Microsoft SQL Server  7.00 - 7.00.623 (Intel X86)
        Nov 27 1998 22:20:07
        Copy
        right (c) 1988-1998 Microsoft Corporation
        Standard Edition Evaluation o
        n Windows NT 5.0 (Build 2195: Service Pack 3)
```

The isql.exe utility parameters are:

- –U — Specifies the username. Enter *sa* for system administrator.
- –P — Specifies the password. Leave the password blank for the *sa* account.
- –S — Specifies the server name.

Configuring the TPC-B benchmark environment

The TPC-B benchmark environment simulates an online transaction processing database environment. The TPC-B benchmark kit is easy to use, quick to install and set up, and free to distribute. Its requirements are:

- One workstation with Windows 2000 and SQL Server 7.0 client utilities.
- One server with Windows 2000 Advanced Server and SQL Server 7.0 database engine.

Use the tpcbmdb2 version of the TPC-B benchmarking kit. This kit builds two identical databases, bench1 and bench2, with the following disk layout:

- Bench1 consists of both the transaction log and the data files residing on C.
- Bench2 consists of the transaction log residing on C and the data files residing on E.

Target server

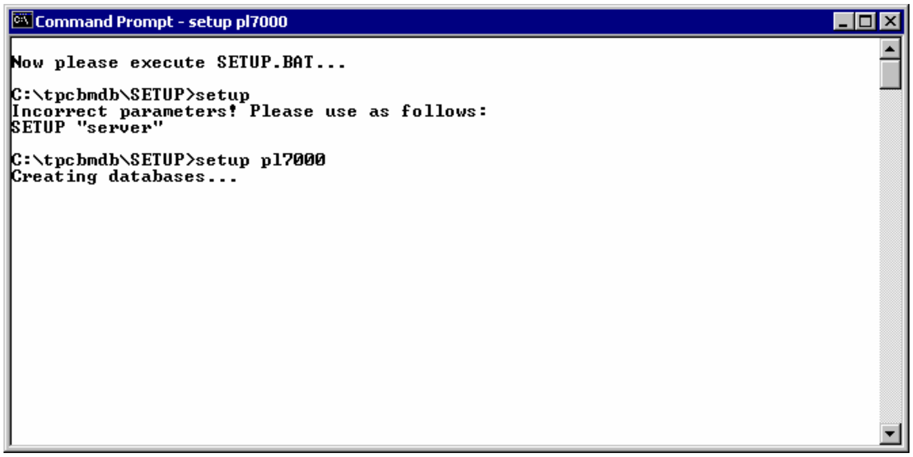
At the database server, perform these steps to install and execute the benchmark kit:

1. From the TPC-B benchmark kit distribution medium, execute *install.bat* from the appropriate folder. The installer copies the files to your local C: drive into the C:\tpcbmdb folder.

   ```
   C:\>SQL Server 7 TPC-B kit\tpcbmdb2\install
   ```

2. Execute *setup.bat* with the name of the database server as the parameter.

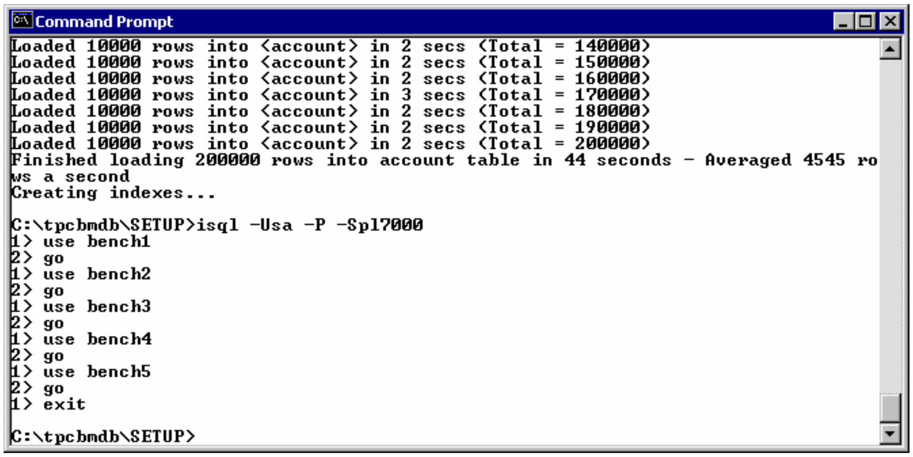
   ```
   C:\tpcbmdb\setup\> setup yourservername
   ```



```
Now please execute SETUP.BAT...

C:\tpcbmdb\SETUP>setup
Incorrect parameters! Please use as follows:
SETUP "server"

C:\tpcbmdb\SETUP>setup pl7000
Creating databases...
```

3. Verify that all databases have been created. The number of created databases should match the selected benchmark kit version. For example, tpcbmdb2 kit will create two databases, named *bench1* and *bench2*. Use the following script.

```
C:\>isql –Usa –P –Syourservername

1> use bench1

2> go

1> use bench2

2> go

1> exit
```



```
Loaded 10000 rows into <account> in 2 secs (Total = 140000)
Loaded 10000 rows into <account> in 2 secs (Total = 150000)
Loaded 10000 rows into <account> in 2 secs (Total = 160000)
Loaded 10000 rows into <account> in 3 secs (Total = 170000)
Loaded 10000 rows into <account> in 2 secs (Total = 180000)
Loaded 10000 rows into <account> in 2 secs (Total = 190000)
Loaded 10000 rows into <account> in 2 secs (Total = 200000)
Finished loading 200000 rows into account table in 44 seconds - Averaged 4545 ro
ws a second
Creating indexes...

C:\tpcbmdb\SETUP>isql -Usa -P -Spl7000
1> use bench1
2> go
1> use bench2
2> go
1> use bench3
2> go
1> use bench4
2> go
1> use bench5
2> go
1> exit

C:\tpcbmdb\SETUP>
```

Notify your instructor if any of these commands return an error code.

Client

If your client is not the machine that is running the SQL database, perform these steps to install the benchmark kit on the client machine:

1. From the TPC-B benchmark kit distribution medium, execute *install.bat* from the appropriate folder. The installer copies the files to your local C: drive into the C:\tpcbmdb folder.

   ```
   C:\>SQL Server 7 TPC-B kit\tpcbmdb2\install
   ```

   > **Note**
   >
   > Upon its completion, the install script prompts you to execute SETUP. Do not run SETUP at the client.

2. Change your current folder to C:\tpcbmdb\run\ntintel. Two batch files are located in this folder:

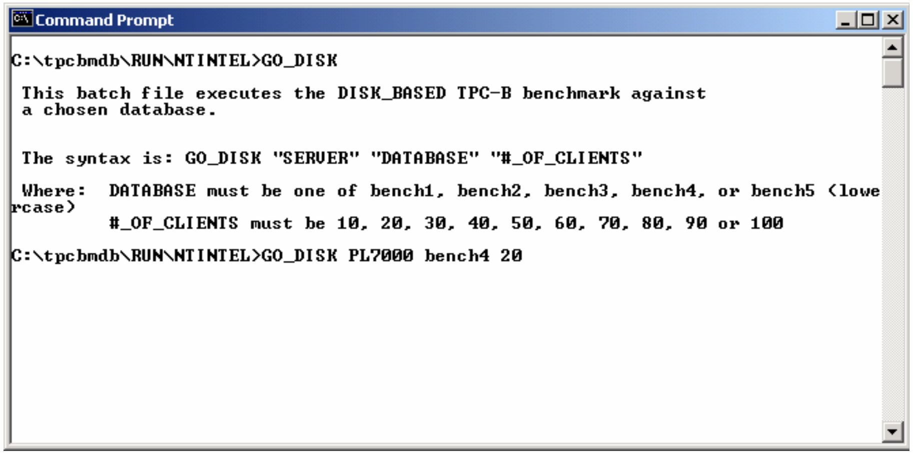
   - Go_mem.bat executes the memory-based TPC-B benchmark. It causes the client drivers to access only a small portion of the entire database, so that the accessed pages can fit comfortably in the data cache.
   - Go_disk.bat executes the disk-based TPC-B benchmark. It causes the client drivers to access the entire range of the database, allowing SQL Server to cache only a portion of the data.

Validation run

At the client machine, perform these steps:

1. Execute *run_disk.bat* or *run_mem.bat* with these parameters:

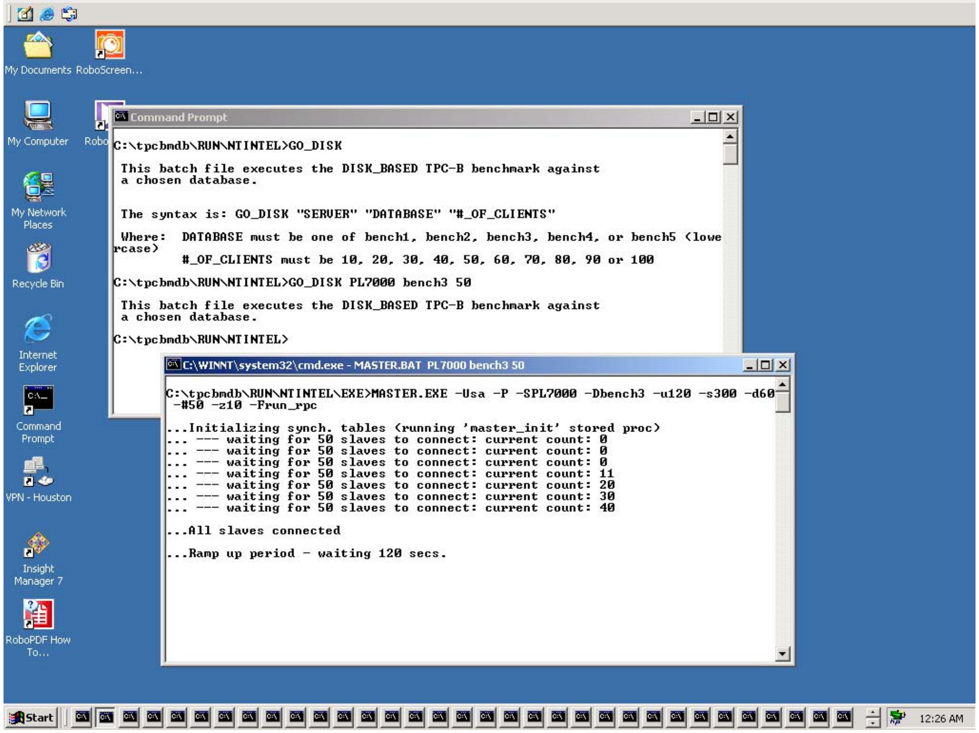
   - <server> — The NetBIOS name of the database server
   - <database> — The name of the target database (for example, bench3)
   - <# of clients> — The number of clients to be simulated (must be between 10 and 100, with increments of 10)



```
C:\tpcbmdb\RUN\NTINTEL>GO_DISK

 This batch file executes the DISK_BASED TPC-B benchmark against
 a chosen database.


 The syntax is: GO_DISK "SERVER" "DATABASE" "#_OF_CLIENTS"

 Where:  DATABASE must be one of bench1, bench2, bench3, bench4, or bench5 (lowe
rcase)
         #_OF_CLIENTS must be 10, 20, 30, 40, 50, 60, 70, 80, 90 or 100

C:\tpcbmdb\RUN\NTINTEL>GO_DISK PL7000 bench4 20
```

2. Each eight-minute run consists of three stages:
    - Ramp-up of two minutes
    - Steady state of five minutes
    - Ramp-down of one minute

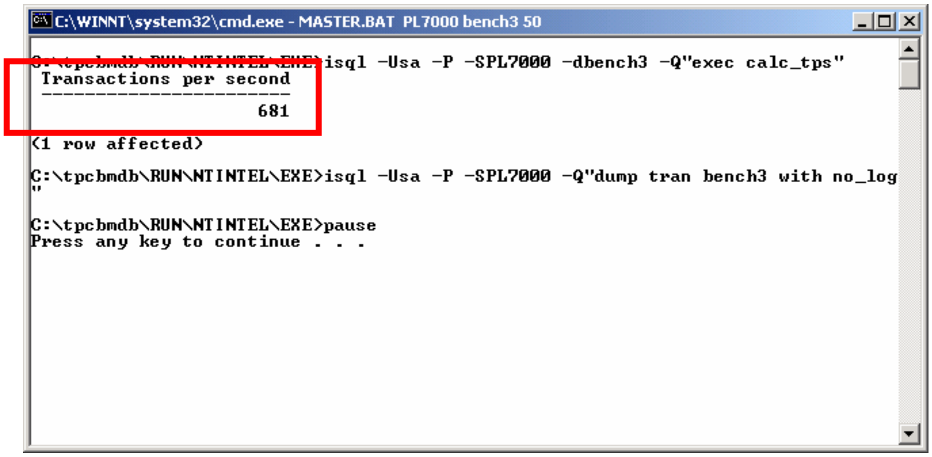
    The kit starts a Command Prompt window for each simulated client. Each simulated client window is automatically minimized, and shows in the Windows task bar at the bottom of the screen. The master window displays the number of clients connected and the execution stage.



```
C:\tpcbmdb\RUN\NTINTEL>GO_DISK

 This batch file executes the DISK_BASED TPC-B benchmark against
 a chosen database.


 The syntax is: GO_DISK "SERVER" "DATABASE" "#_OF_CLIENTS"

 Where:  DATABASE must be one of bench1, bench2, bench3, bench4, or bench5 (lowe
rcase)
         #_OF_CLIENTS must be 10, 20, 30, 40, 50, 60, 70, 80, 90 or 100

C:\tpcbmdb\RUN\NTINTEL>GO_DISK PL7000 bench3 50

 This batch file executes the DISK_BASED TPC-B benchmark against
 a chosen database.

C:\tpcbmdb\RUN\NTINTEL>
```

```
C:\tpcbmdb\RUN\NTINTEL\EXE>MASTER.EXE -Usa -P -SPL7000 -Dbench3 -u120 -s300 -d60
 -#50 -z10 -Frun_rpc

...Initializing synch. tables (running 'master_init' stored proc)
... --- waiting for 50 slaves to connect: current count: 0
... --- waiting for 50 slaves to connect: current count: 0
... --- waiting for 50 slaves to connect: current count: 0
... --- waiting for 50 slaves to connect: current count: 11
... --- waiting for 50 slaves to connect: current count: 20
... --- waiting for 50 slaves to connect: current count: 30
... --- waiting for 50 slaves to connect: current count: 40

...All slaves connected

...Ramp up period - waiting 120 secs.
```

3. When the run completes, the master window displays the measured transactions per second (TPS). The TPS rate is the rate at which the target database responds to client requests and processes transactions. Only the steady state is included in the measurement. Different runs against the same configuration should produce similar results. Runs against different configurations (different memory configuration, different number of processors, different database, etc.) produce results reflecting that configuration performance.



```
C:\tpcbmdb\RUN\NTINTEL\EXE>isql -Usa -P -SPL7000 -dbench3 -Q"exec calc_tps"
 Transactions per second
 -----------------------
                     681

(1 row affected)

C:\tpcbmdb\RUN\NTINTEL\EXE>isql -Usa -P -SPL7000 -Q"dump tran bench3 with no_log
"

C:\tpcbmdb\RUN\NTINTEL\EXE>pause
Press any key to continue . . .
```

Monitoring and tuning

Using the TPC-B benchmarking environment, tune the server for highest performance at the lowest configuration cost. First, show the importance of data placement and its effect on performance by completing the Disk section. Then, using the fastest database layout, complete the Processor, Memory, and Network sections. Finally, experiment with array controller caching.

Note

Consult with your instructor to determine which monitoring and tuning exercises you should complete. The selection will depend on the hardware configuration you have available, the time constrains, and the instructor objectives.

Disk

Bench1

Execute the TPC-B benchmark against the bench1 database while monitoring performance and component utilization. Discuss your findings with your instructor and fellow students, and answer the following questions.

Bench1 transaction file location:...

Number of spindles servicing the transaction log:..

RAID level for the transaction log:..

Bench1 data file location: ....

Number of spindles servicing the data files:...

RAID level for the data files:..

Bench1 performance (tps):..

Characterize the I/O profile (sequential/random, reads/writes, and so forth) for each logical drive. Explain what is causing this type of I/O.

Logical drive E:..

Logical drive G: ....

To increase the performance of this database, what would you recommend?

....

....

Bench2

Execute the TPC-B benchmark against the bench2 database while monitoring performance and component utilization. The bench2 database differs from the bench1 database only in disk layout. Discuss your findings with your instructor and fellow students, and answer the following questions.

Bench2 transaction file location:..

Number of spindles servicing the transaction log:...

RAID level for the transaction log:..

Bench2 data file location: ....

Number of spindles servicing the data files:...

RAID level for the data files:..

Bench2 performance (tps):..

Characterize the I/O profile (sequential/random, reads/writes, and so forth) for each logical drive. Explain what is causing this type of I/O.

Logical drive E:..

Logical drive G: ....

To increase the performance of this database, what would you recommend?

....

....

Conclusion

Which database layout is the fastest and why?

....

....

Which database layout is the slowest and why?

....

....

What is the most significant performance-limiting factor with the bench1 database layout? Explain.

....

....

Which subsystem is the performance bottleneck under each database?

....

....

....

....

To increase the performance of your fastest database, what would you recommend?

....

....

To maximize server performance and data protection, what disk configuration would you recommend?

....

....

Processors

Use the fastest database layout and focus on monitoring and tuning the processors. Using the /numproc option in the boot.ini file, artificially reduce the number of processors to *one* and rerun the benchmark.

```
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows 2000
    Advanced Server" /fastdetect /NUMPROC=1
```

! **Important**

Each change to the boot.ini file requires a system reboot.

Determine the database performance with different processor configurations. Increase the number of processors up to the number of processors present in the system. Record your findings in the spaces provided.

Number of processors = 1 (/numproc=1), TPS rate =.......................................

Number of processors = 2 (/numproc=2), TPS rate =.......................................

Number of processors = 3 (/numproc=3), TPS rate =.......................................

Number of processors = 4 (/numproc=4), TPS rate =.......................................

Discuss with the instructor and fellow students how the processor configuration affects performance. Record your results in the following spaces.

....

....

....

Based on your processor scalability results, what is the optimal number of processors, given the cost of additional processors and the associated performance gains? Record your findings in the following spaces.

....

In this particular environment, would a fewer number of faster processors yield better performance than a higher number of slower processors? For example, eight 400MHz processors compared with four 800MHz processors. Consider the processing environment – an online transaction processing database. Explain.

....

....

....

Lastly, set the /numproc option to the number of processors you have determined to be optimal for this environment.

Memory

Use the fastest database layout and your choice of the processor configuration, and focus on monitoring and tuning the memory. Using the /maxmem option in the boot.ini file, artificially reduce the amount of memory available to the operating system to 32MB and rerun the benchmark.

```
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft Windows
2000 Advanced Server" /fastdetect /NUMPROC=4 /MAXMEM=32
```

> **!** **Important**
>
> Each change to the boot.ini file requires a system reboot.

Determine the database performance with different memory configurations. Increase the amount of memory up to the memory installed in the system. Record your findings in the following spaces.

Amount of memory = 32 (/maxmem=32), TPS rate =......................................

Amount of memory = 64 (/maxmem=64), TPS rate =......................................

Amount of memory = 128 (/maxmem=128), TPS rate =..................................

Amount of memory = 256 (/maxmem=256), TPS rate =..................................

Amount of memory = 512 (/maxmem=512), TPS rate =..................................

Discuss with the instructor and fellow students how the memory configuration affects performance. Record your results in the following spaces.

....

....

....

Based on your memory scalability results, what is the optimal amount of memory, given the cost of additional memory and the associated performance gains? Record your findings in the following spaces.

....

....

Set the /maxmem option to the amount of memory you have determined to be optimal for this environment.

Network

Use the fastest server configuration you determined to this point. Monitor the server network interface controller and conclude whether you would make any adjustments or recommendations. Record your findings in the following spaces.

....

....

....

....

....

Controller caching

Use the fastest server configuration to this point. With the Array Configuration Utility, change the configuration of the array controller cache (the Array Accelerator) and rerun the benchmark. Determine the best Array Accelerator setting for the transaction log and for the database. Discuss your findings with the instructor and fellow students.

Record your findings in the spaces provided.

Array Accelerator setting for the transaction log	Array Accelerator setting for the data files	Transactions per second (TPS)

....

....

....

....

....

....

....

....

Exercise 3 — Installing and using HP Resource Partitioning Manager 2.0

RPM is an easy-to-use application that extends the Windows 2000 operating system to enable IT administrators to optimize their ProLiant servers dynamically.

In this exercise, you will learn how to create, modify, and configure resource partitions.

Installing RPM

To install RPM, follow these steps:

1. Insert the HP ProLiant Essentials Workload Management Pack CD into the CD-ROM drive.
2. If autorun is enabled, the Resource Partitioning Manager Setup window will display. If autorun is not enabled, select *Start* → *Run* and enter:

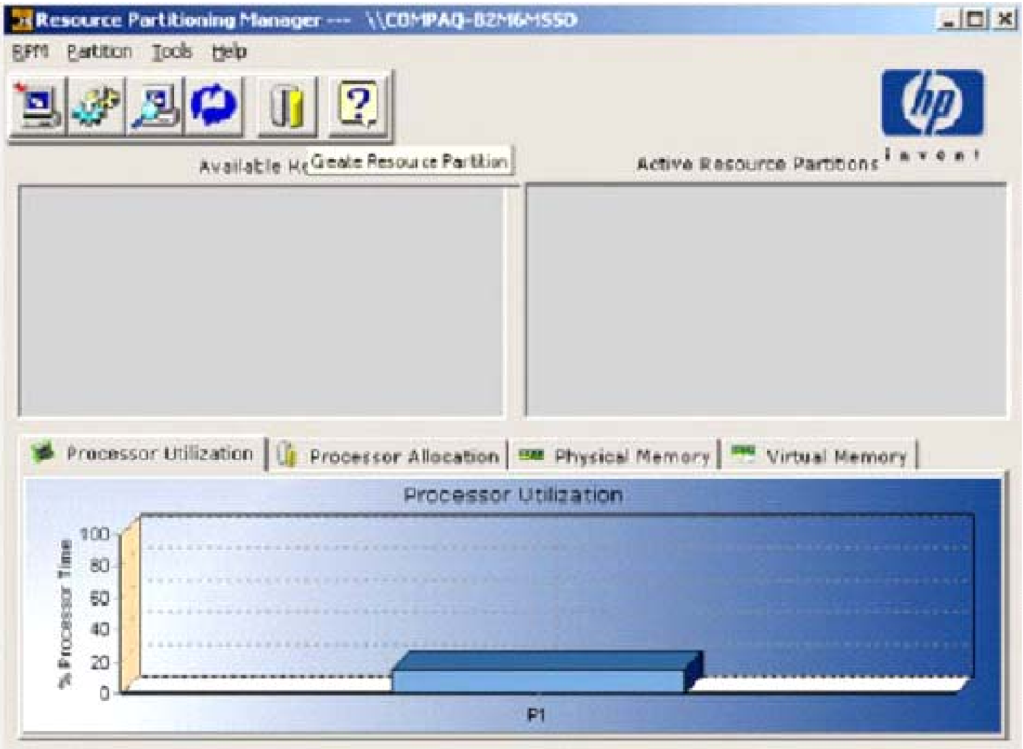
   ```
   [CD drive]:\Setup.exe
   ```
3. Follow the instructions to install RPM.
4. Enter the product key into the blank spaces when the product key window displays.
5. When the Completing the Resource Partitioning Manager Setup wizard displays in the Setup window, click *Finish*. RPM is now installed on your server.

> **Note**
> When upgrading from a previous version of RPM, close any active resource partitions before installing RPM 2.0.

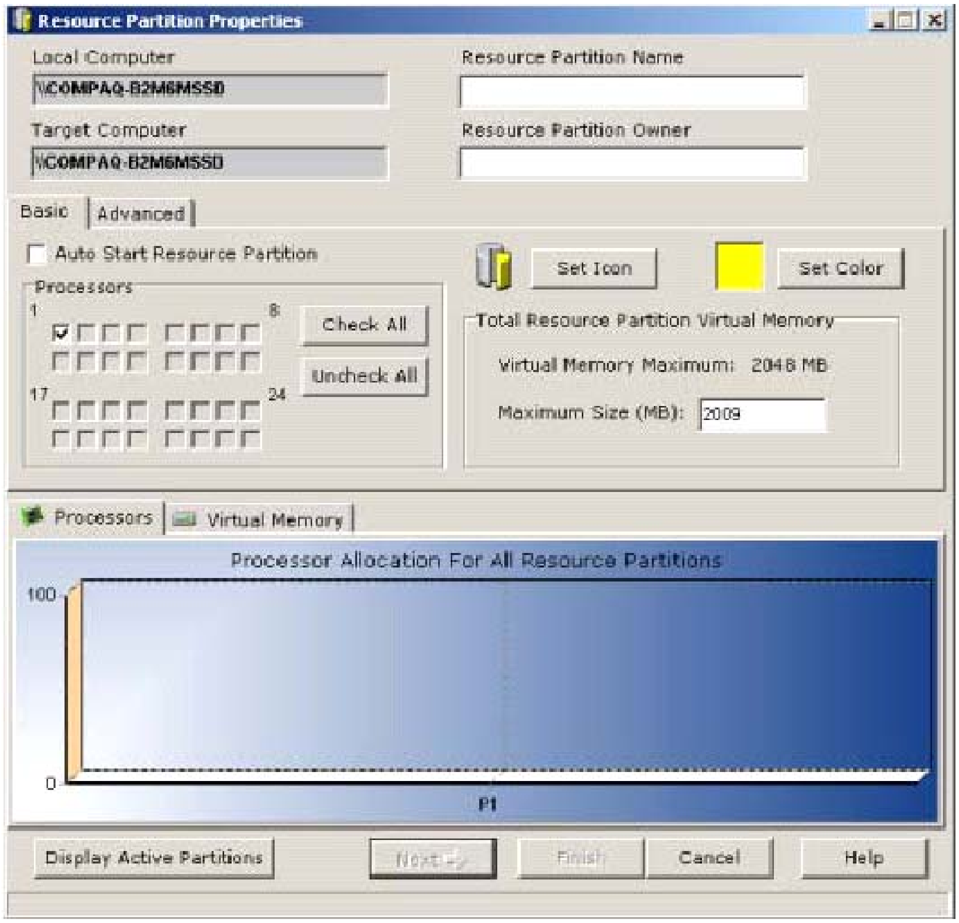
Creating resource partitions

To create a resource partition, follow these steps:

1. Select *Start* → *Programs* → *HP Resource Partitioning Manager*. The following screen displays.



2. Click the *Create Resource Partition* icon. The Resource Partition Properties window displays.



Local Computer: \\COMPAQ-B2M6MSSD

Target Computer: \\COMPAQ-B2M6MSSD

Resource Partition Name:

Resource Partition Owner:

☐ Auto Start Resource Partition

Virtual Memory Maximum: 2048 MB

Maximum Size (MB): 2009

Resource Partition Properties
Basic
Advanced
Processors
1
8
17
24
Check All
Uncheck All
Set Icon
Set Color
Total Resource Partition Virtual Memory
Processors
Virtual Memory
Processor Allocation For All Resource Partitions
100
0
P1
Display Active Partitions
Next
Finish
Cancel
Help

3. The Resource Partition Properties window allows you to define a name, assign a user, and modify the properties for your new resource partition. In the Resource Partition Name field, enter *Compaq1*.

4. You can use the Resource Partition Owner field to associate the partition with a specific organizational entity or to provide additional information about the partition. In the Resource Partition Owner field, enter *User1*.
5. Select the *Basic* tab and locate the Processors section. This section consists of several boxes, each one representing a single processor. By default, RPM selects all available processors.

Note

In the processor section:

- Checked boxes represent processors to be used by the current resource partition.
- White boxes represent other available processors.
- Gray boxes represent processors that are not physically present.

---

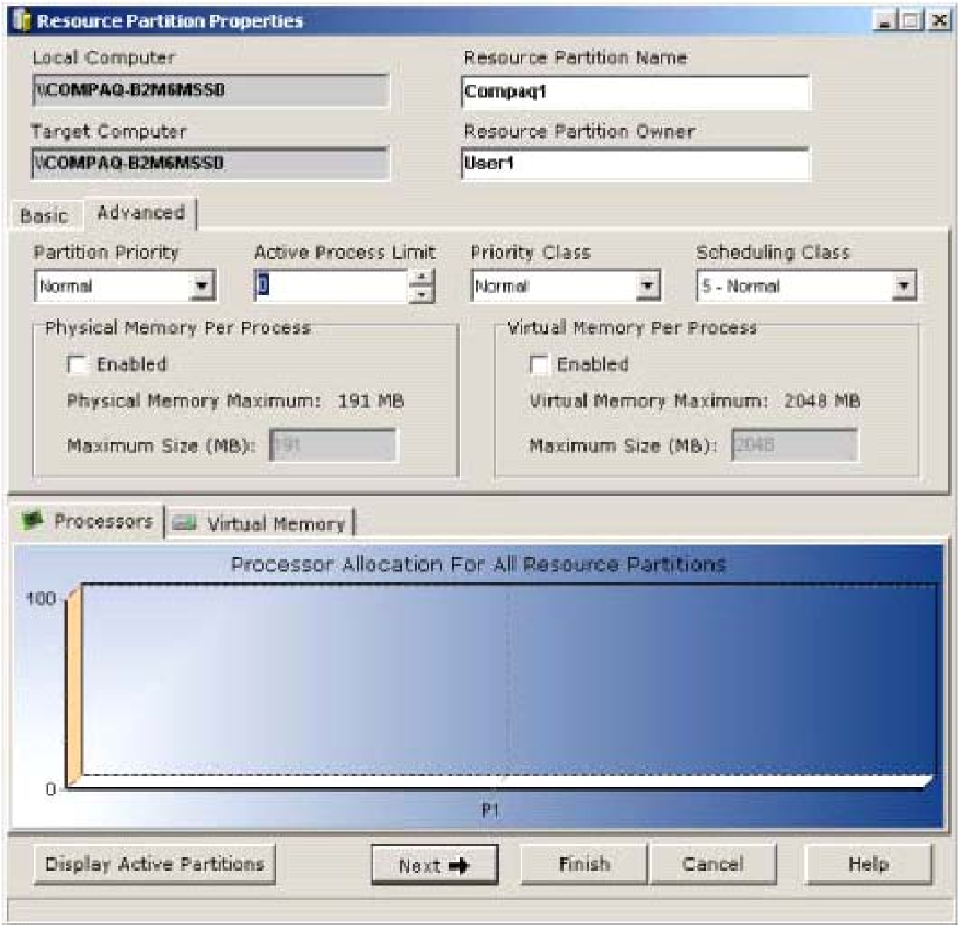
6. Locate the Total Resource Partition Virtual Memory section. This section lists the maximum amount of virtual memory available for the resource partition. What is the maximum amount of virtual memory available?

   ....

   How much memory is listed in the Maximum Size (MB) field?

   ....
7. Enter *2000* in the Maximum Size (MB) field.
8. Check the *Auto Start Resource Partition* check box. This enables the resource partition and all associated processes to activate automatically when the server starts.

9. Select the *Advanced* tab. The following screen displays.



Resource Partition Properties

Local Computer: \\COMPAQ-B2M6MSSD

Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSSD

Resource Partition Owner: User1

Partition Priority: Normal

Active Process Limit: 0

Priority Class: Normal

Scheduling Class: 5 - Normal

Physical Memory Per Process

☐ Enabled

Physical Memory Maximum: 191 MB

Maximum Size (MB): 191

Virtual Memory Per Process

☐ Enabled

Virtual Memory Maximum: 2048 MB

Maximum Size (MB): 2048

Basic
Advanced
Processors
Virtual Memory
Processor Allocation For All Resource Partitions
100
0
P1
Display Active Partitions
Next
Finish
Cancel
Help

10. Click the *Partition Priority* drop-down arrow to assign a level of prioritization to a partition. This feature ensures that a lower partition does not use all system resources when higher priority partitions are initiated. You can select from the following:

- High
- Normal (default)
- Below Normal

Verify that *Normal* is selected.

11. By default, the active process limit is zero. Using the default setting allows unlimited processes to be activated within a given resource partition.
12. Click the *Priority Class* drop-down arrow to set the Windows 2000 priority class for all threads within each process in the resource partition. You can select from the following:
    - High
    - Above Normal
    - Normal (default)
    - Below Normal

    Select *Above Normal*.
13. Click the *Scheduling Class* drop-down arrow to set the length of time allocated for all threads within each process in the resource partition. You can select from the following:
    - 7 – High
    - 6 – Above Normal
    - 5 – Normal
    - 4 – Below Normal
    - 3 – Low

    Select *6 – Above Normal*.
14. Locate the *Physical Memory Per Process* section. The maximum amount of physical memory available to any individual process contained within the resource partition is determined automatically and displayed in this section. What is the maximum amount of physical memory available per process?

    ....

15. You can modify the amount of **physical** memory available. Click the *Enabled* check box. In the Maximum Size field, enter a new amount for the physical memory.

Note

You cannot enter an amount greater than the maximum amount of physical memory allowed per process.

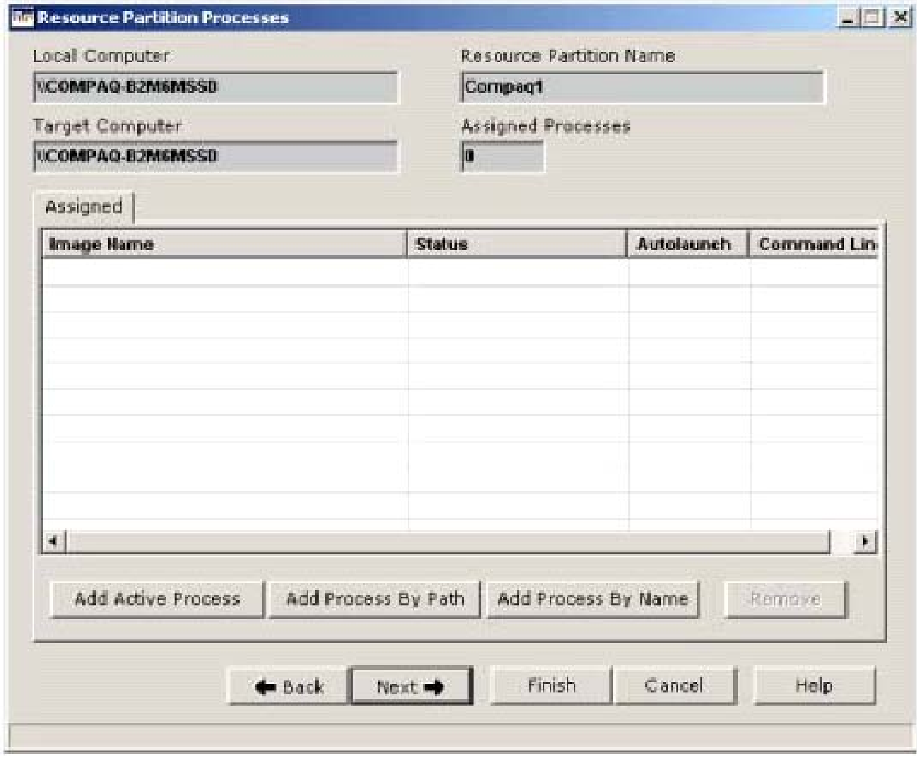
---

16. Locate the Virtual Memory Per Process section. This section displays the amount of memory available to any individual process within the resource partition. What is the maximum amount of virtual memory available per process?

   ....

17. You also can modify the amount of **virtual** memory available. Click the *Enabled* check box. In the Maximum Size field, enter a new amount for the virtual memory.

18. You have created a resource partition. Click *Next* to display the Resource Partition Processes window.



Local Computer: \\COMPAQ-B2M6MSSD

Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSSD

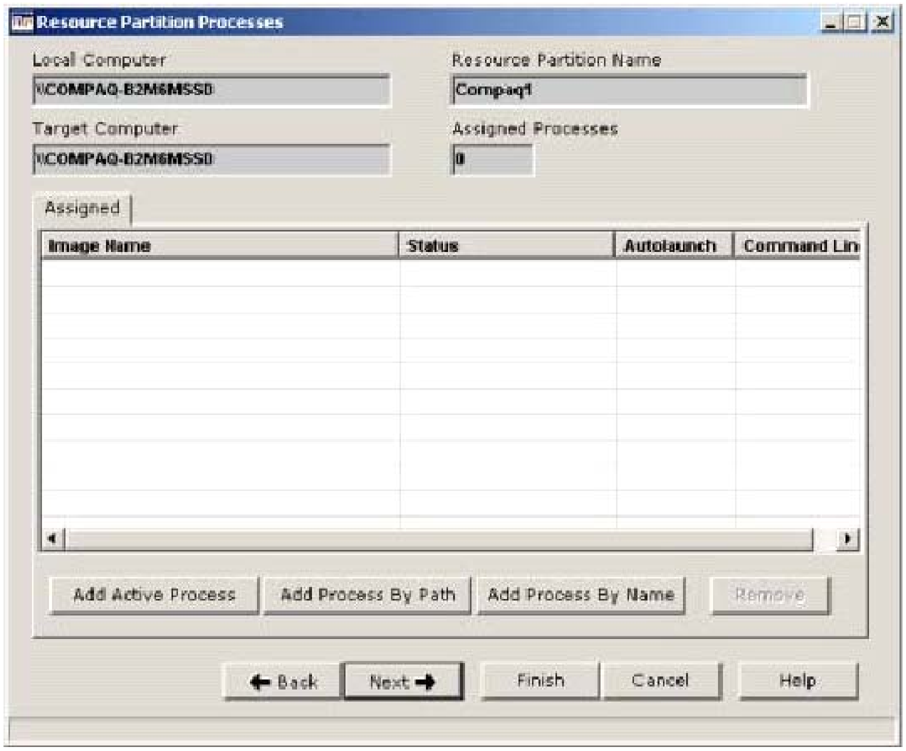
Assigned Processes: 0

Adding a new process to a resource partition

The Resource Partition Processes window allows you to assign processes to the resource partition. Examples of processes include executables, Dynamic Link Libraries (DLLs), and services that an administrator selects to run within a resource partition.

To assign a process to a resource partition, follow these instructions:

1. In the Resource Partition Processes window, click on any one of the following buttons to add a process:
   - **Add Active Process** — Add a currently running process
   - **Add Process By Path** — Add a process by entering the full directory of the process
   - **Add Process By Name** — Add a process by entering its image name



Local Computer: \\COMPAQ-B2M6MSSD

Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSSD

Assigned Processes: 0

2. To add an active process, click the *Add Active Process* button. The Add Active Process window displays.

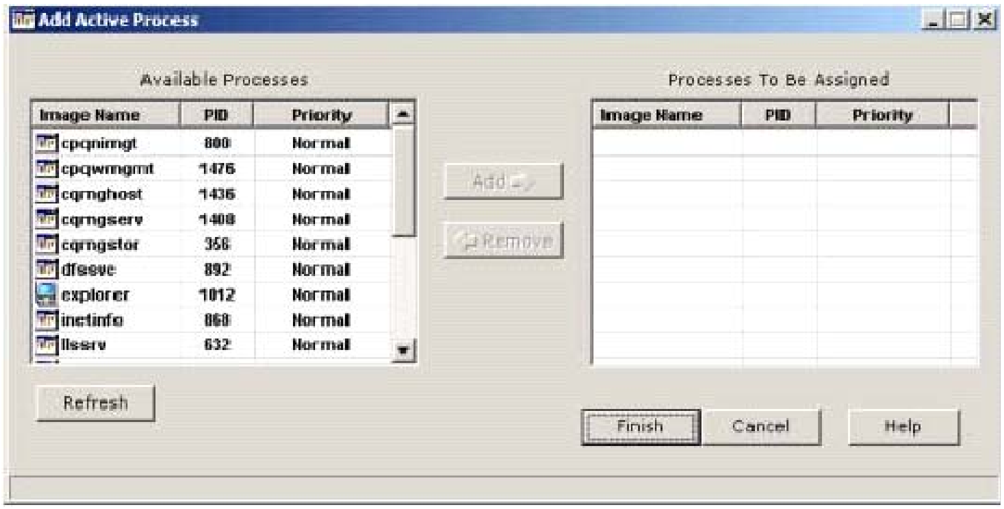


Image Name	PID	Priority
cpqnimgt	800	Normal
cpqwmgmt	1476	Normal
cqmghost	1436	Normal
cqmgserv	1408	Normal
cqmgstor	356	Normal
dfssvc	892	Normal
explorer	1012	Normal
inetinfo	868	Normal
llssrv	632	Normal

Image Name	PID	Priority

3. In the Available Processes section, select *cpqwmgmt*. Click *Add*. *Cpqnimgt* now displays in the Processes To Be Assigned section on the right side of the screen.
4. Click *Yes* if a caution box displays the following message:

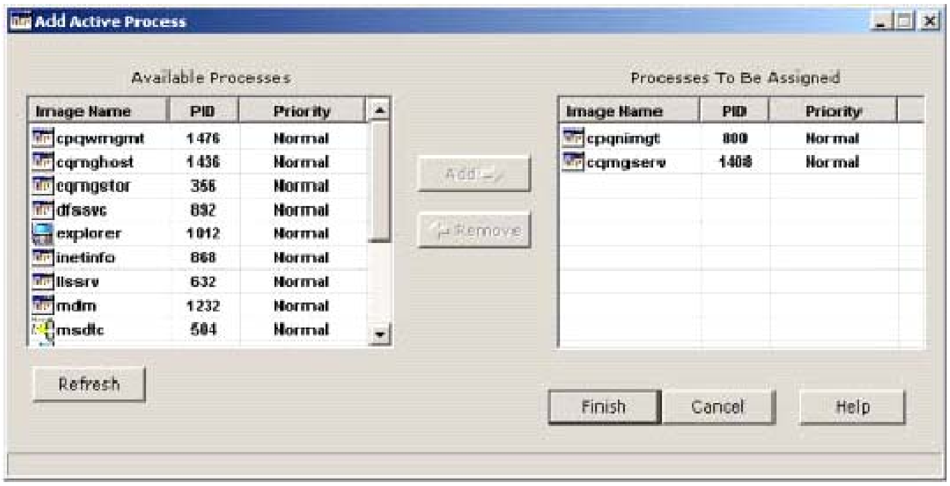
   Adding a running process to a resource partition will result in that process being terminated if the partition is later deactivated.

! **Important**

If the Resource Partitioning Manager window displays after you click *Add*, your available process is currently activated. Click *Yes* to continue. When the resource partition is deactivated, the running process will be terminated.

---

5. In the Available Processes section, select *cqmgserv*. Click *Add*. Cqmgserv is also displayed in the Processes To Be Assigned section.



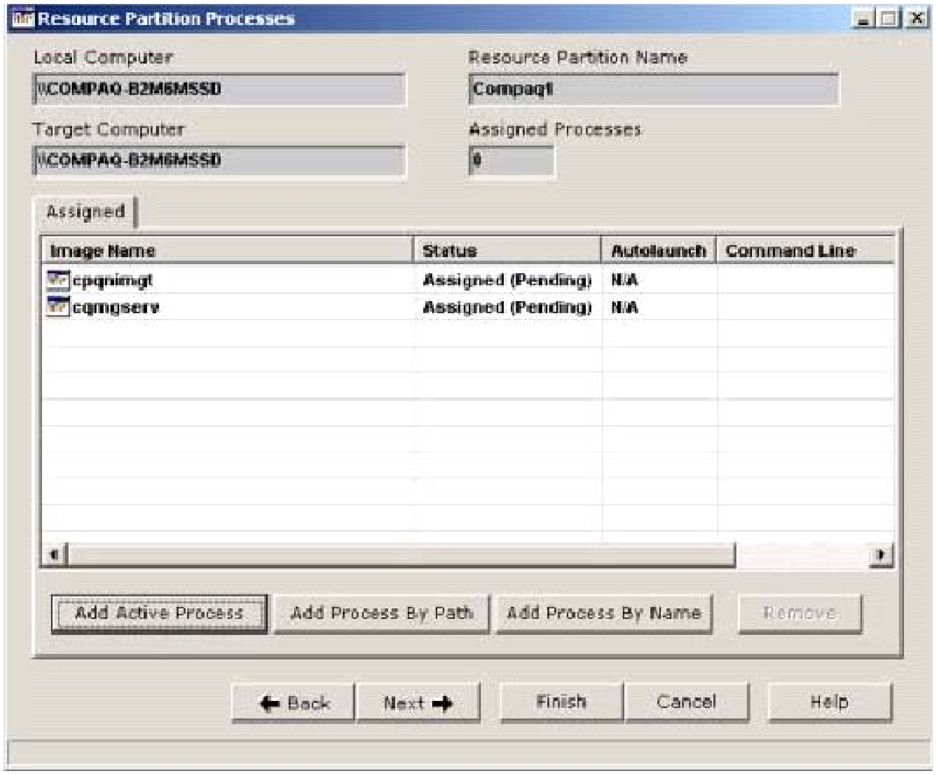
Available Processes

Image Name	PID	Priority
cpqwmgmt	1476	Normal
cqmghost	1436	Normal
cqmgstor	356	Normal
dfssvc	892	Normal
explorer	1012	Normal
inetinfo	868	Normal
llssrv	632	Normal
mdm	1232	Normal
msdtc	504	Normal

Processes To Be Assigned

Image Name	PID	Priority
cpqnimgt	800	Normal
cqmgserv	1408	Normal

6. Click *Finish*. The Resource Partition Processes window displays the assigned processes.



Local Computer: \\COMPAQ-B2M6MSSD

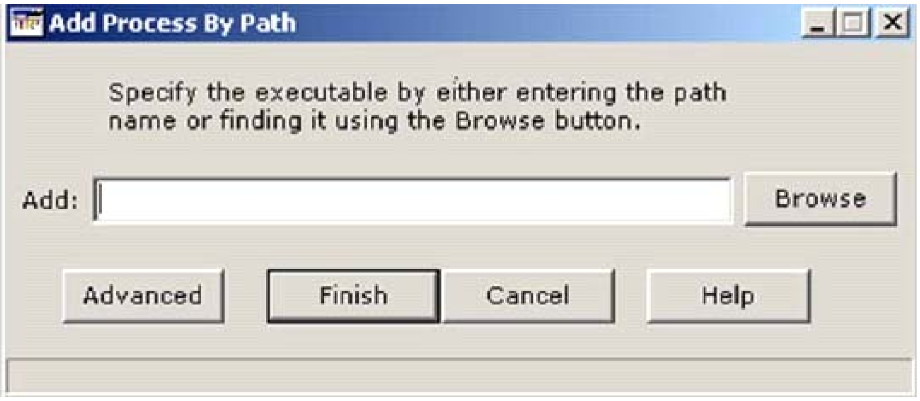
Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSSD

Assigned Processes: 0

Image Name	Status	Autolaunch	Command Line
cpqnimgt	Assigned (Pending)	N/A	
cqmgserv	Assigned (Pending)	N/A	

7. To add a process by entering its location, click the *Add Process By Path* button. The Add Process By Path window displays.

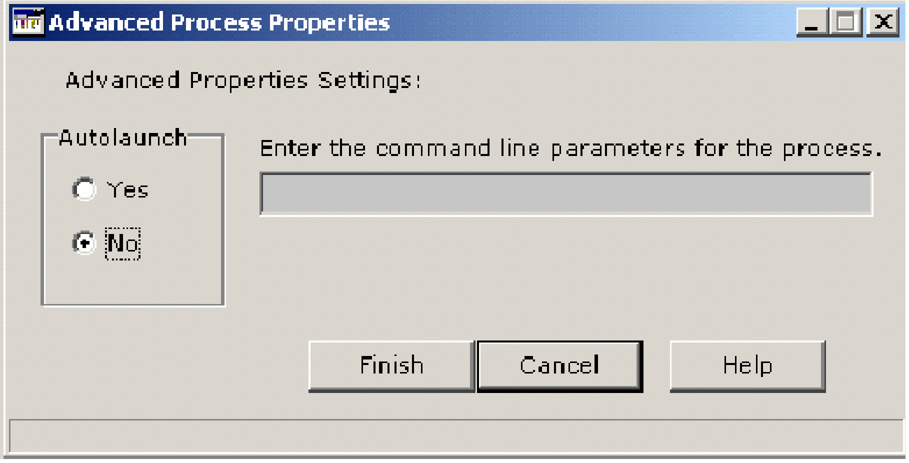


Add Process By Path

Specify the executable by either entering the path name or finding it using the Browse button.

8. Click the *Browse* button. Locate the Survey Utility file (c:\Compaq\Survey\Survey.exe) and click *Open*. The file directory displays in the Add field.

9. Click the *Advanced* button. The Advanced Process Properties window displays.



Advanced Process Properties

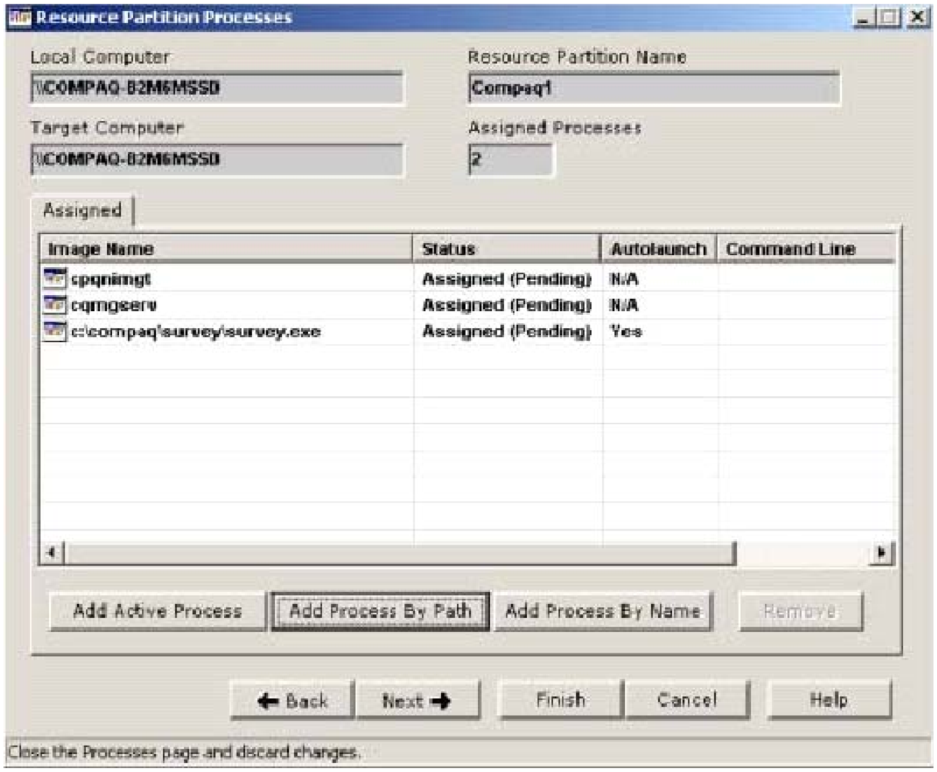
Advanced Properties Settings:

Autolaunch
○ Yes
● No

Enter the command line parameters for the process.

10. In the Autolaunch section, click *Yes*. RPM will attempt to launch the Survey Utility when the associated resource partition (Compaq1) is activated.
11. Click *Finish* → *Finish* to return to the Resource Partition Processes window.

    Notice that the Compaq Survey Utility file directory displays in the Image Name column.



Local Computer: \\COMPAQ-B2M6MSSD

Resource Partition Name: Compaq1

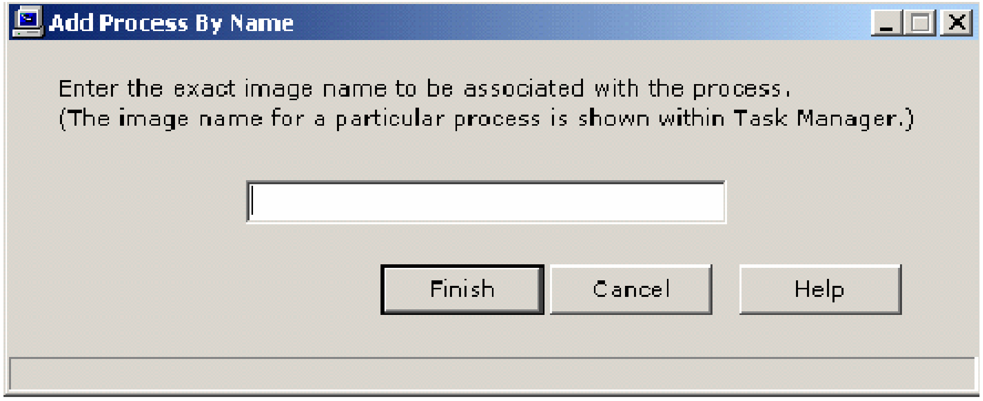
Target Computer: \\COMPAQ-B2M6MSSD

Assigned Processes: 2

Image Name	Status	Autolaunch	Command Line
cpqnimgt	Assigned (Pending)	N/A	
cqmgserv	Assigned (Pending)	N/A	
c:\compaq\survey\survey.exe	Assigned (Pending)	Yes	

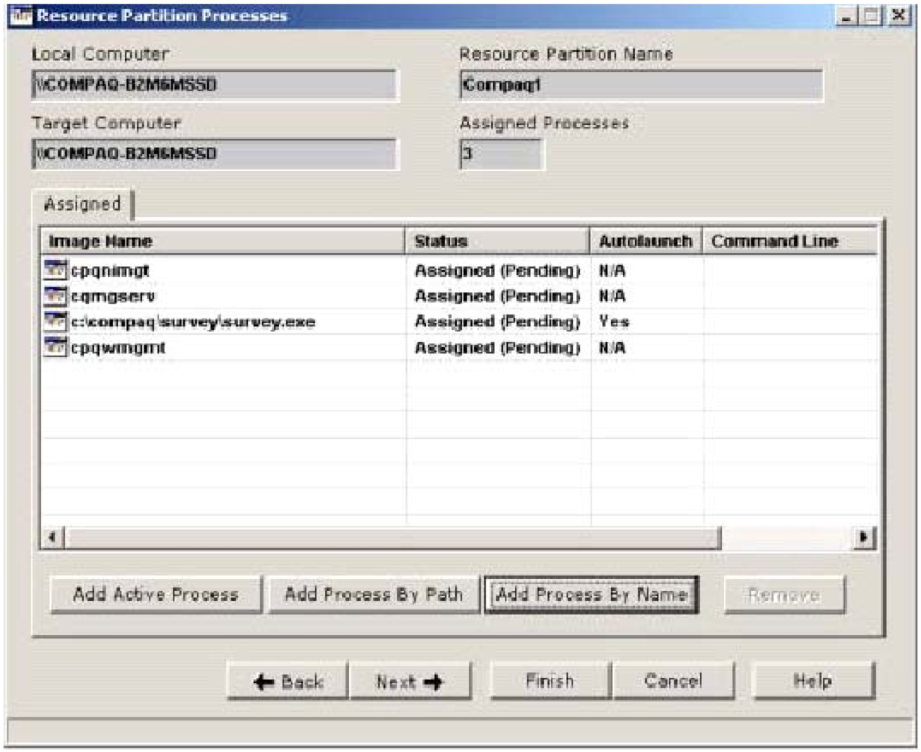
Close the Processes page and discard changes.

12. To add a process by entering its image name, click *Add Process By Name*. The Add Process By Name window displays.



Enter the exact image name to be associated with the process.
(The image name for a particular process is shown within Task Manager.)

13. Enter *cpqwmgmt* in the open field. Click *Finish*. The new process displays in the Image Name column of the Resource Partition Processes window. You can delete a process at any time by highlighting its image name and clicking the *Remove* button.



Local Computer: \\COMPAQ-B2M6MSSD

Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSSD

Assigned Processes: 3

Image Name	Status	Autolaunch	Command Line
cpqnimgt	Assigned (Pending)	N/A	
cqmgserv	Assigned (Pending)	N/A	
c:\compaq\survey\survey.exe	Assigned (Pending)	Yes	
cpqwmgmt	Assigned (Pending)	N/A	

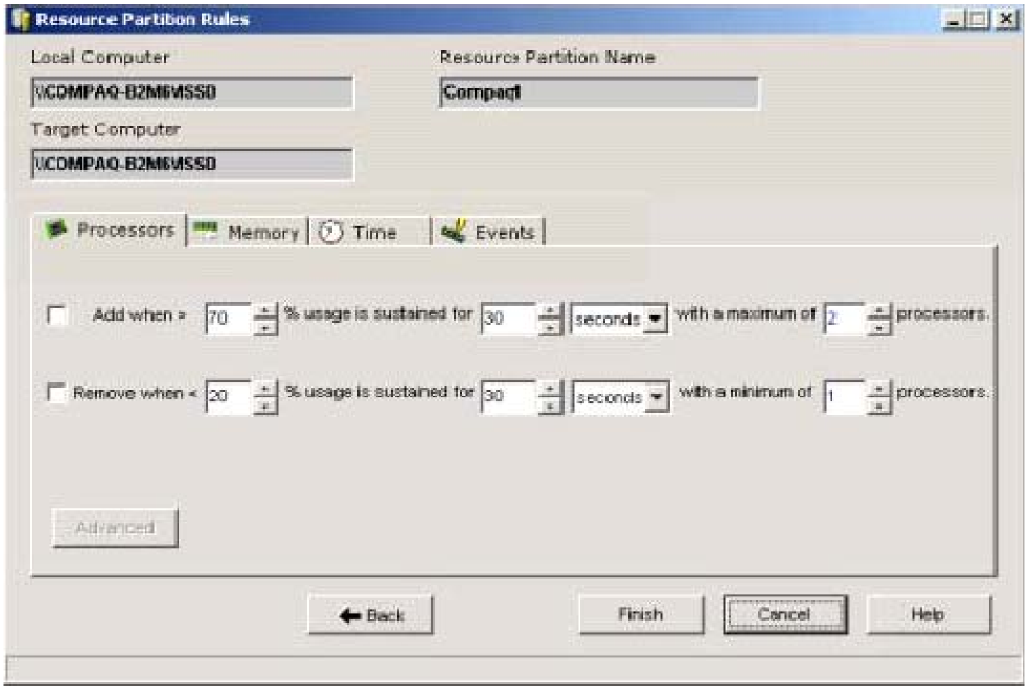
14. Click *Next* to proceed to the next exercise, Assigning Rules for a Resource Partition.

Assigning rules for a resource partition

After a process has been assigned to a resource partition, rules can be associated with that resource partition. The Resource Partition Rules window lists the local computer name, target computer, resource partition name, and the processors, memory, time, and events tabs.

To assign rules to a resource partition, follow these steps:

1. In the Resource Partition Rules window, click the *Processors* tab. This tab displays two processor rules:
    - Add when > (greater than)
    - Remove when < (less than)



Local Computer: \\COMPAQ-B2M6MSS0

Resource Partition Name: Compaq

Target Computer: \\COMPAQ-B2M6MSS0

☐ Add when > 70 % usage is sustained for 30 seconds with a maximum of 2 processors.

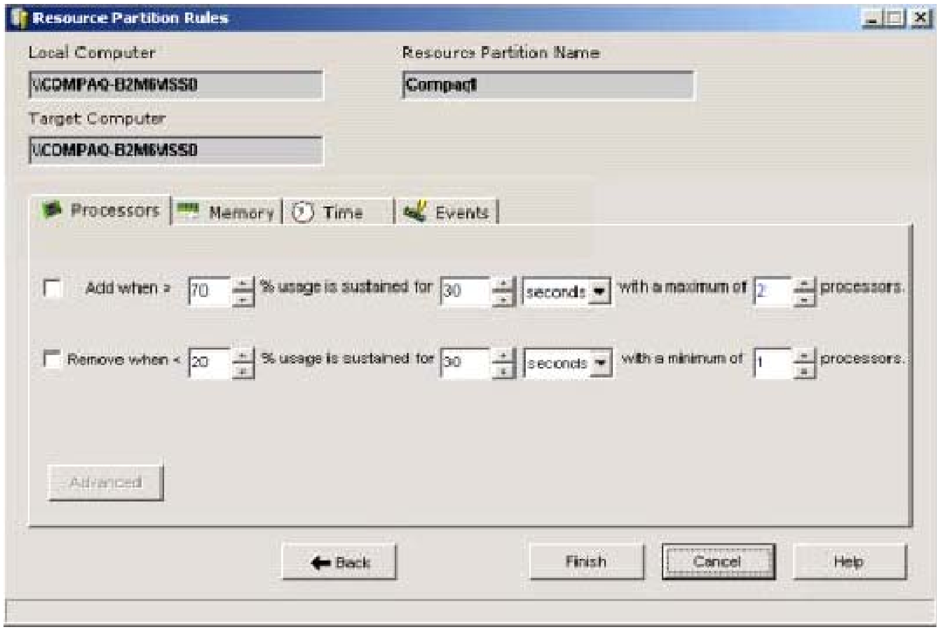
☐ Remove when < 20 % usage is sustained for 30 seconds with a minimum of 1 processors.

! **Important**

The Rules options on the Processor tab will be disabled and shaded gray if only one processor is installed on your server. If the rules on the Processor tab are disabled, bypass steps 2 through 4 and continue to step 5.

---

2. Click the *Add when* box to enable the first processor rule. If enabled, available processors are allocated to the resource partition dynamically when the preset rule conditions arise.
3. Enter the following information:
    - Add when > *85*
    - % usage is sustained for *45 seconds*
    - With a maximum of *2*



Local Computer: \\COMPAQ-B2M6MSS0

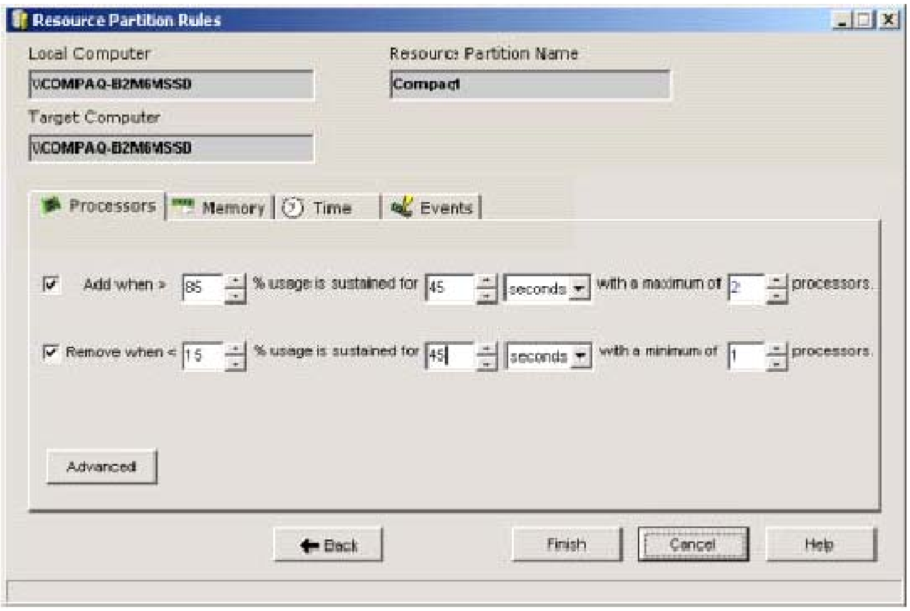
Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSS0

☐ Add when > 70 % usage is sustained for 30 seconds with a maximum of 2 processors.

☐ Remove when < 20 % usage is sustained for 30 seconds with a minimum of 1 processors.

4. Click the *Remove when* box to enable the second processor rule. Enter the following information:
   - Remove when > *15*
   - % usage is sustained for *45 seconds*
   - With a minimum of *1*



Local Computer: \\COMPAQ-B2M6MSSD

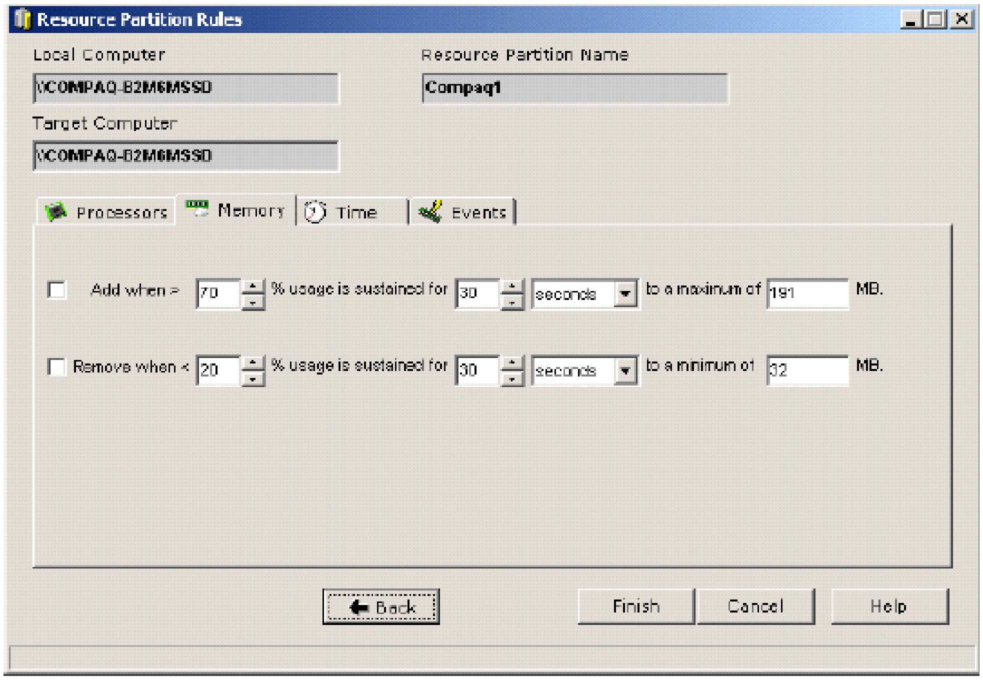
Resource Partition Name: Compaq

Target Computer: \\COMPAQ-B2M6MSSD

☑ Add when > 85 % usage is sustained for 45 seconds with a maximum of 2 processors.

☑ Remove when < 15 % usage is sustained for 45 seconds with a minimum of 1 processors.

5. Select the *Memory* tab. This tab displays two memory rules:
    - Add when >
    - Remove when <



Local Computer: \\COMPAQ-B2M6MSSD

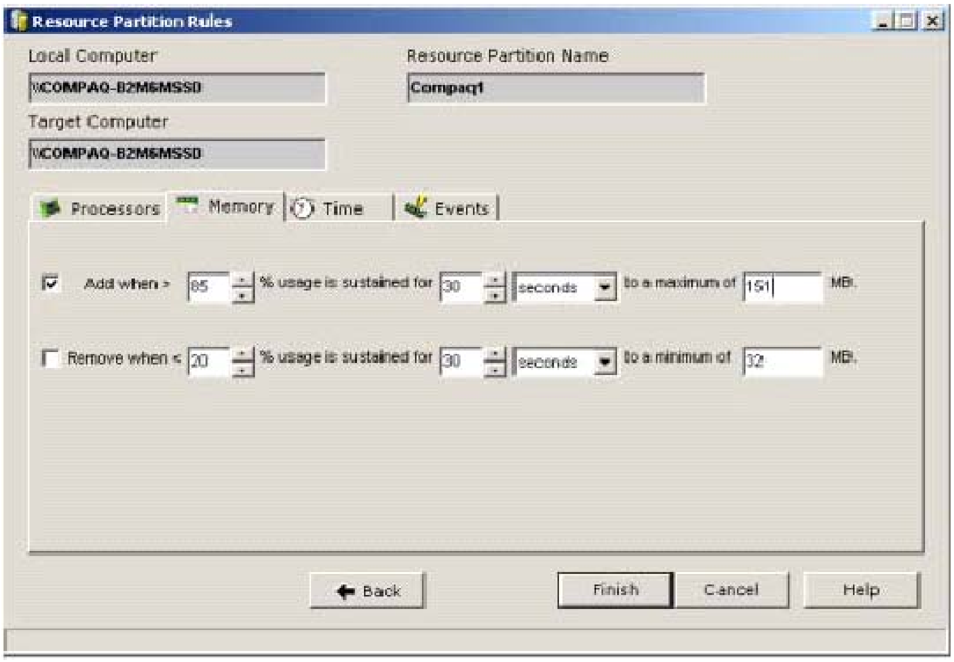
Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSSD

☐ Add when > 70 % usage is sustained for 30 seconds to a maximum of 191 MB.

☐ Remove when < 20 % usage is sustained for 30 seconds to a minimum of 32 MB.

6. Click the *Add when* box to enable the first memory rule. Enter the following information:
   - Add when > *85*
   - % usage is sustained for *30 seconds*
   - To a maximum of *151* MB



Local Computer: \\COMPAQ-B2M6MSSD

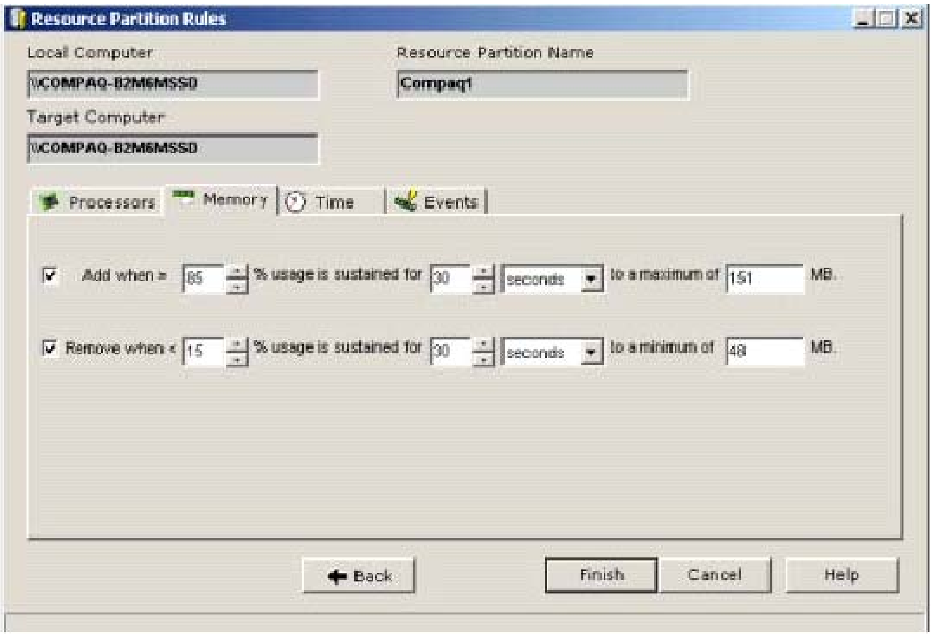
Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSSD

☑ Add when > 85 % usage is sustained for 30 seconds to a maximum of 151 MB.

☐ Remove when < 20 % usage is sustained for 30 seconds to a minimum of 32 MB.

7. Click the *Remove when* box to enable the second memory rule. Enter the following information:
   - Remove when < *15*
   - % usage is sustained for *30 seconds*
   - To a minimum of *48* MB



Resource Partition Rules

Local Computer: \\COMPAQ-B2M6MSSD

Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSSD

☑ Add when > 85 % usage is sustained for 30 seconds to a maximum of 151 MB.

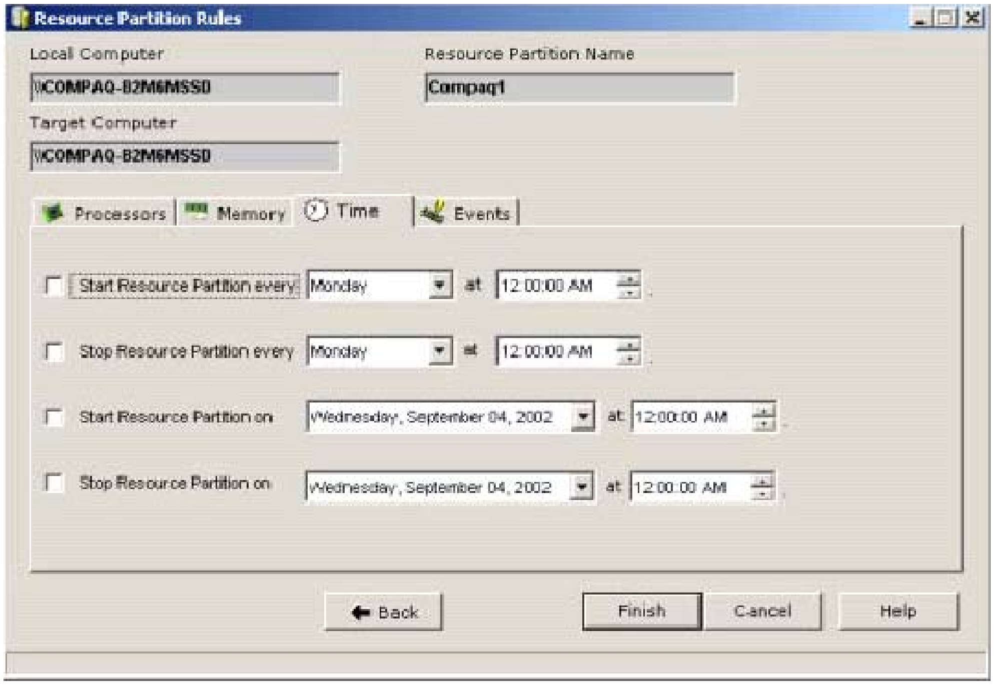
☑ Remove when < 15 % usage is sustained for 30 seconds to a minimum of 48 MB.

Note

Memory is added and removed in 16MB increments.

---

8. Select the *Time* tab. This tab displays the following four rules:
   - Start Resource Partition every (day and time)
   - Stop Resource Partition every (day and time)
   - Start Resource Partition on (date and time)
   - Stop Resource Partition on (date and time)



Local Computer: \\COMPAQ-B2M6MSSD

Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSSD

☐ Start Resource Partition every Monday at 12:00:00 AM

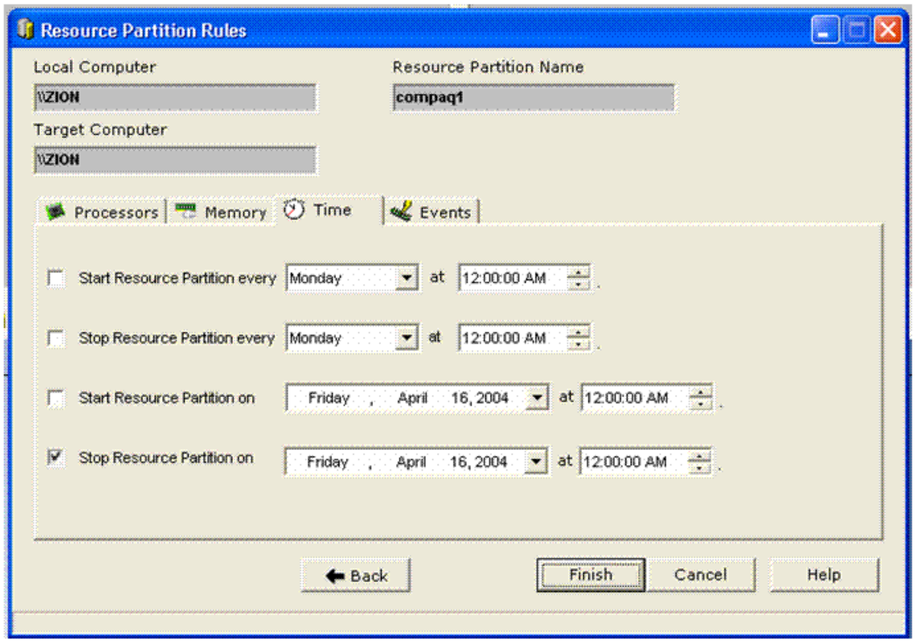
☐ Stop Resource Partition every Monday at 12:00:00 AM

☐ Start Resource Partition on Wednesday, September 04, 2002 at 12:00:00 AM

☐ Stop Resource Partition on Wednesday, September 04, 2002 at 12:00:00 AM

9. Click the *Start Resource Partition on* check box to schedule the resource partition to start at a particular time. On the drop-down menu, select the current date. On the list box, select 30 minutes from the current time.

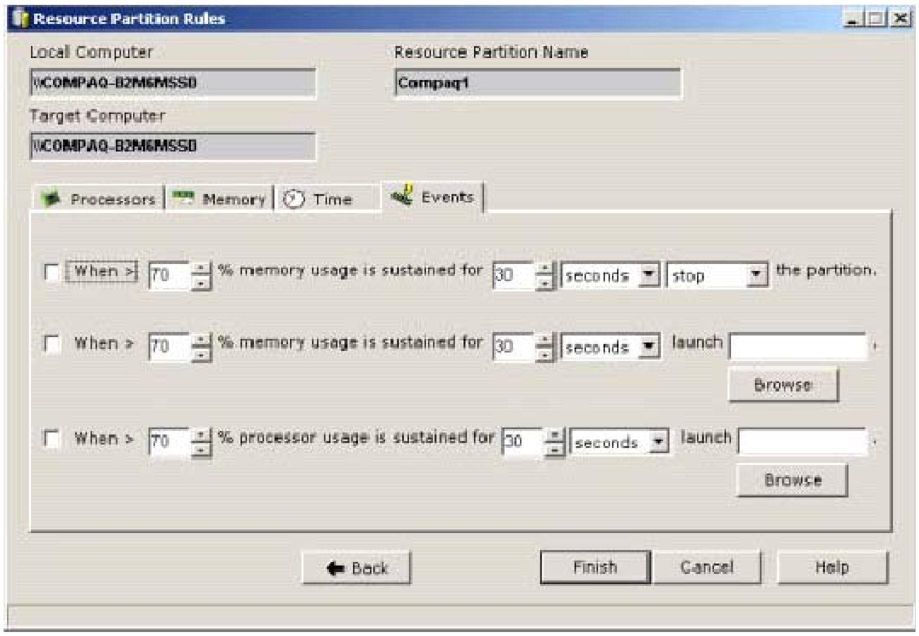
10. Click the *Stop Resource Partition on* check box to schedule the resource partition to stop at a particular time. On the first drop-down menu, select tomorrow's date. On the list box, select *12:00 AM*.



Local Computer: \\ZION
Resource Partition Name: compaq1
Target Computer: \\ZION

☐ Start Resource Partition every Monday at 12:00:00 AM
☐ Stop Resource Partition every Monday at 12:00:00 AM
☐ Start Resource Partition on Friday , April 16, 2004 at 12:00:00 AM
☑ Stop Resource Partition on Friday , April 16, 2004 at 12:00:00 AM

11. Click the *Events* tab. This tab displays three event rules:
    - Partition stop/restart
    - Launch on memory utilization level
    - Launch on processor utilization level



Local Computer: \\COMPAQ-B2M6MSSD

Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSSD

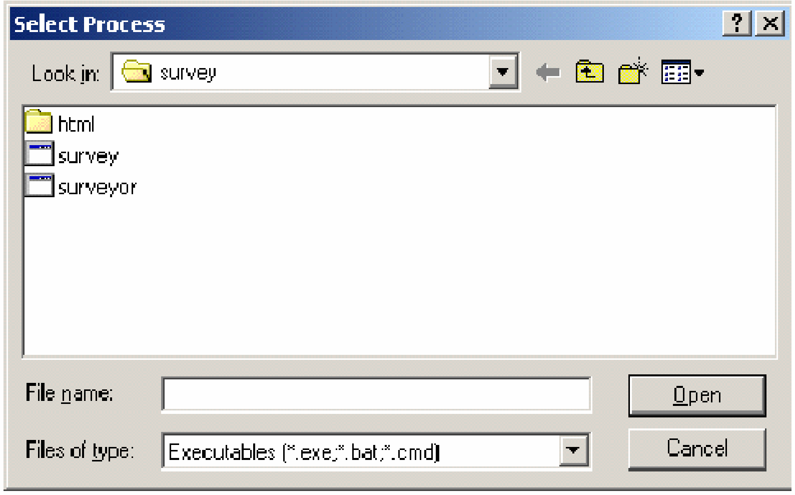
☐ When > 70 % memory usage is sustained for 30 seconds stop the partition.

☐ When > 70 % memory usage is sustained for 30 seconds launch

☐ When > 70 % processor usage is sustained for 30 seconds launch

12. Click the first check box to enable the partition stop/restart rule. This rule allows you to start or stop a partition if its memory usage exceeds a specified percentage for a fixed period of time.
13. Enter the following information:
    - 85% memory usage
    - 20 seconds
    - Stop the partition

14. Click the second check box to enable the Launch on memory utilization level rule. This rule enables RPM to launch a user-specified process or command file if memory usage exceeds a specified percentage for a fixed period of time. Click the *Browse* button. The Select Process window displays.



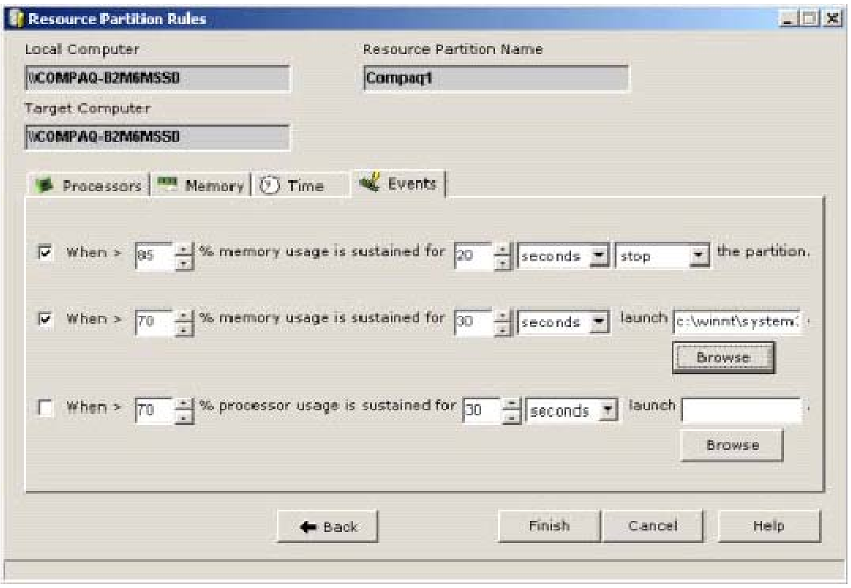
Select Process

Look in: survey

html
survey
surveyor

File name:
Files of type: Executables (*.exe;*.bat;*.cmd)

15. Select any executable file. Click *Open*. The directory of the executable file you selected displays in the launch field.



Resource Partition Rules

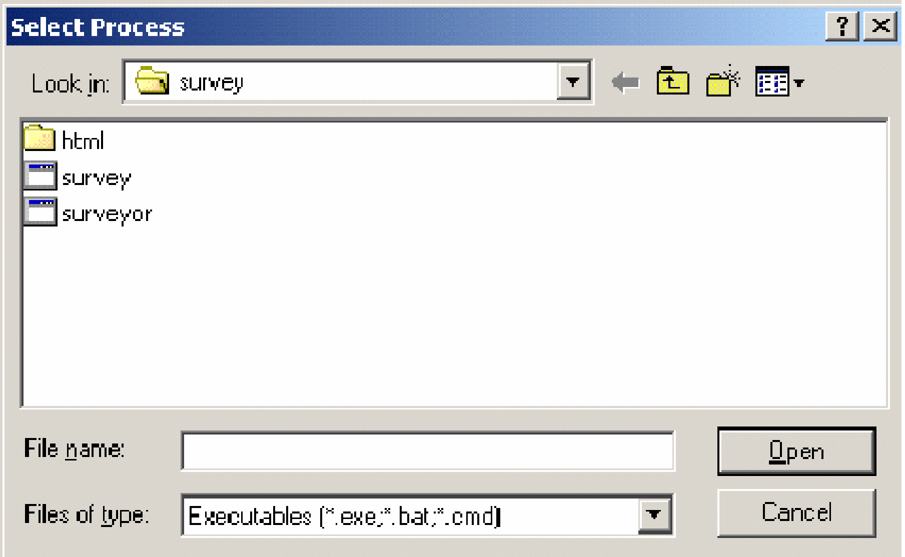
Local Computer: \\COMPAQ-B2M6MSSD
Resource Partition Name: Compaq1
Target Computer: \\COMPAQ-B2M6MSSD

☑ When > 85 % memory usage is sustained for 20 seconds stop the partition.

☑ When > 70 % memory usage is sustained for 30 seconds launch c:\winnt\system

☐ When > 70 % processor usage is sustained for 30 seconds launch

16. Click the third check box to enable the launch on processor utilization level rule. This rule enables you to launch a user-specified process or command file if processor usage exceeds a specified percentage for a fixed period of time. Click the *Browse* button. The Select Process window displays.

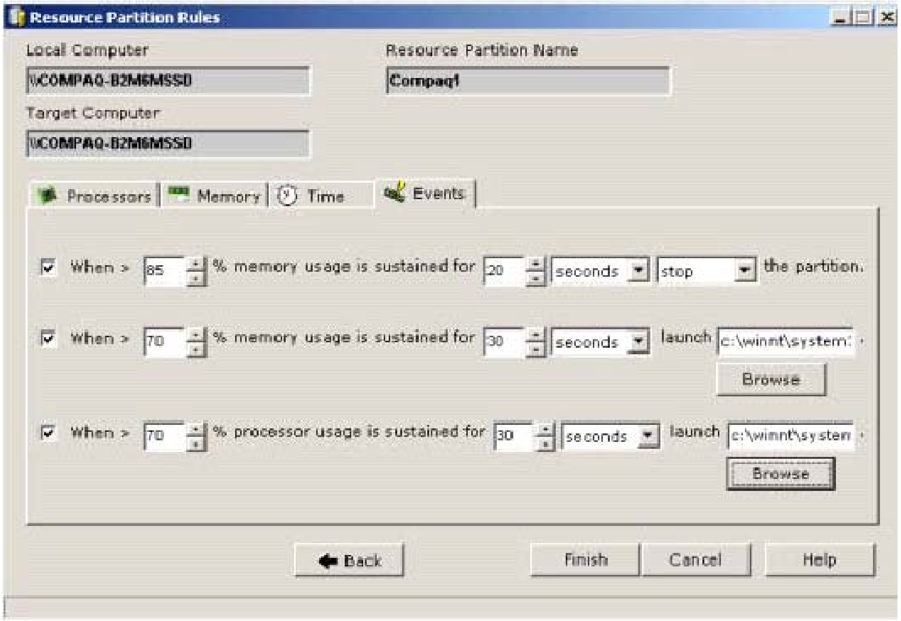


Look in: survey

File name:

Files of type: Executables (*.exe;*.bat;*.cmd)

17. Select a different executable file. Click *Open*. The directory of the executable file displays in the launch field.



Local Computer: \\COMPAQ-B2M6MSSD

Resource Partition Name: Compaq1

Target Computer: \\COMPAQ-B2M6MSSD

☑ When > 85 % memory usage is sustained for 20 seconds stop the partition.

☑ When > 70 % memory usage is sustained for 30 seconds launch c:\winnt\system:

☑ When > 70 % processor usage is sustained for 30 seconds launch c:\winnt\systen

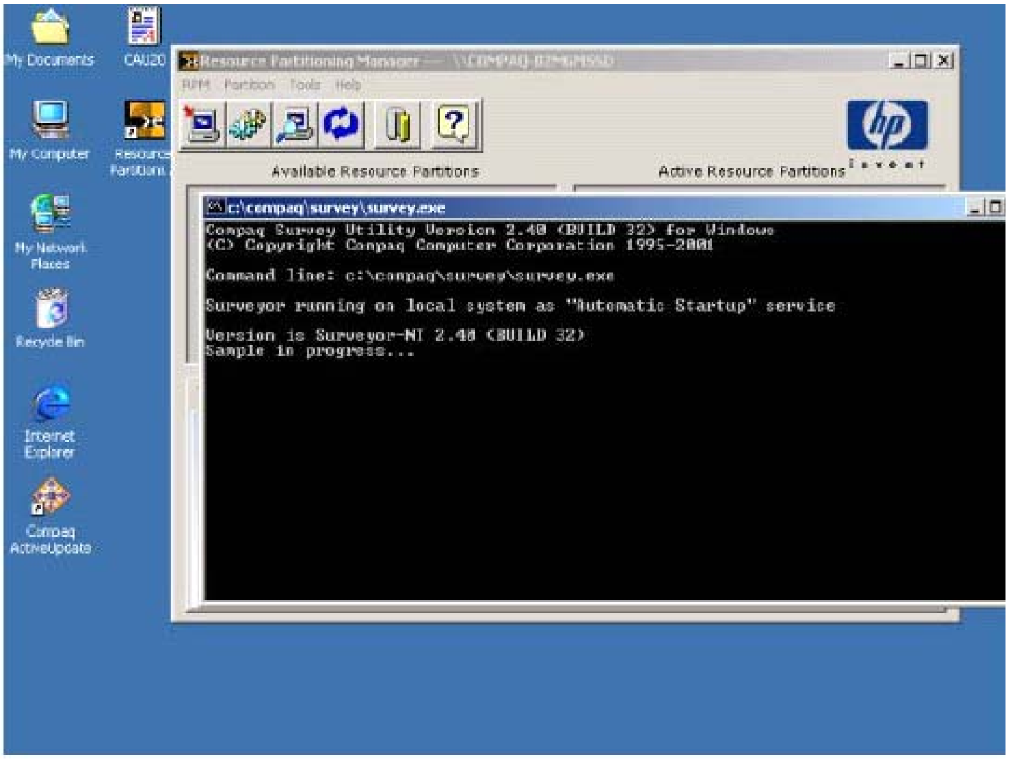
18. Click *Finish* to apply the rules.

Activating resource partitions

To activate an available resource partition:

1. Launch RPM if you have not already done so.
2. Locate the Available Resource Partitions panel and right-click *Compaq1*.
3. From the drop-down menu, select *Start*. What happens next?

   ....



```
Compaq Survey Utility Version 2.40 (BUILD 32) for Windows
(C) Copyright Compaq Computer Corporation 1995-2001

Command line: c:\compaq\survey\survey.exe

Surveyor running on local system as "Automatic Startup" service

Version is Surveyor-NT 2.40 (BUILD 32)
Sample in progress...
```

Deactivating resource partitions

To deactivate an active resource partition:

1. Launch RPM.
2. Locate the Active Resources Partitions panel. Right-click *Compaq1*.
3. From the drop-down menu, select *Stop*. Click *Yes* to clear the partition and terminate all associated open processes. Compaq1 is now deactivated.

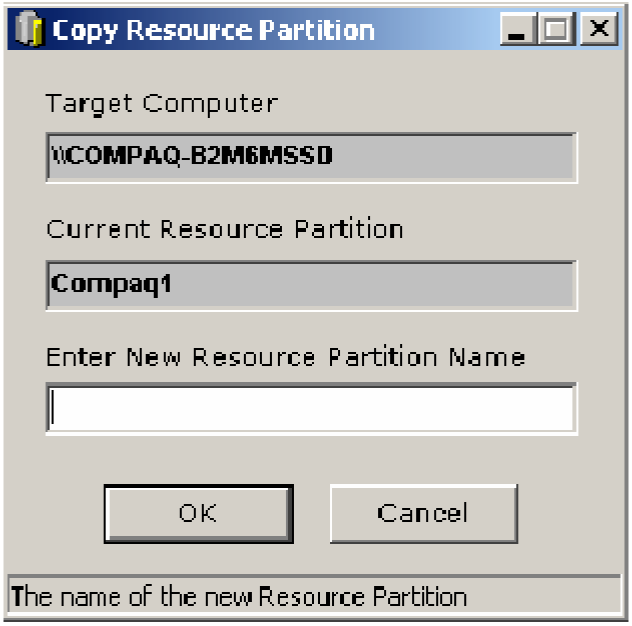
Note
Processes associated with a captured non-RPM partition are not terminated during this procedure.

Copying a resource partition

Instead of regenerating a new resource partition with the same attributes as an existing resource partition, RPM allows you to copy all the attributes of an existing resource partition.

To copy a resource partition:

1. Locate the Available Resource Partitions panel and right-click *Compaq1*.
2. From the drop-down menu, select *Copy*. The Copy Resource Partition window displays.



Copy Resource Partition

Target Computer: \\COMPAQ-B2M6MSSD

Current Resource Partition: Compaq1

Enter New Resource Partition Name

The name of the new Resource Partition

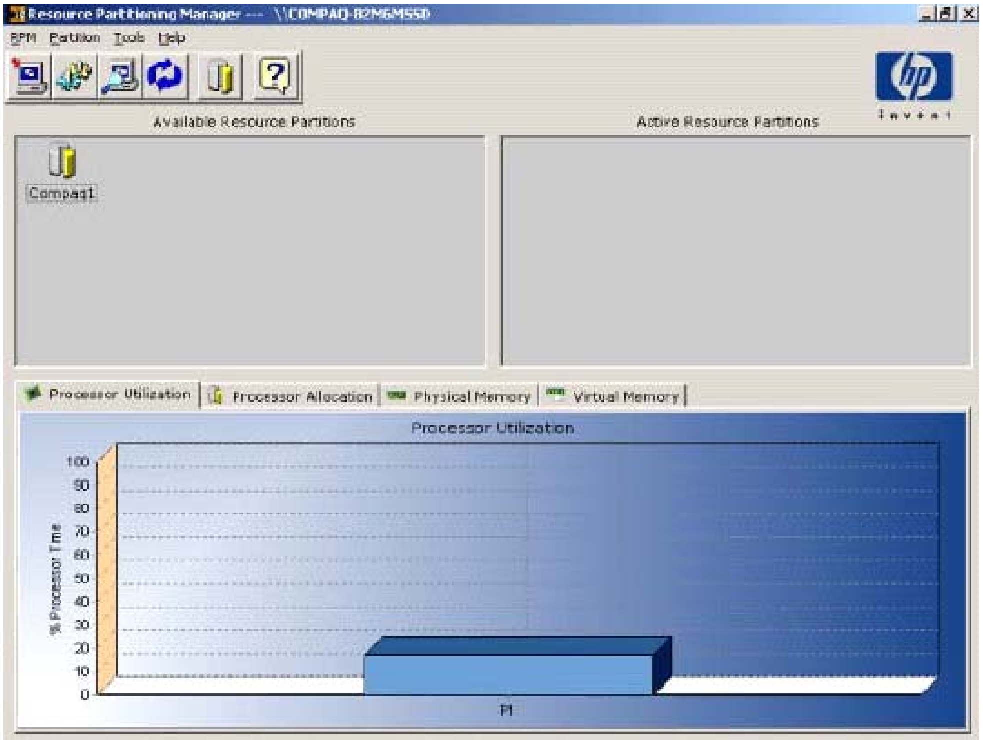
3. In the Enter New Resource Partition Name field, enter *Compaq2* and click *OK*. The newly created partition now displays in the Available Resource Partitions panel.

4. Deleting a resource partition

RPM allows you to delete an inactive resource partition. After you delete a resource partition, you can no longer modify or configure that resource partition.

To delete a resource partition:

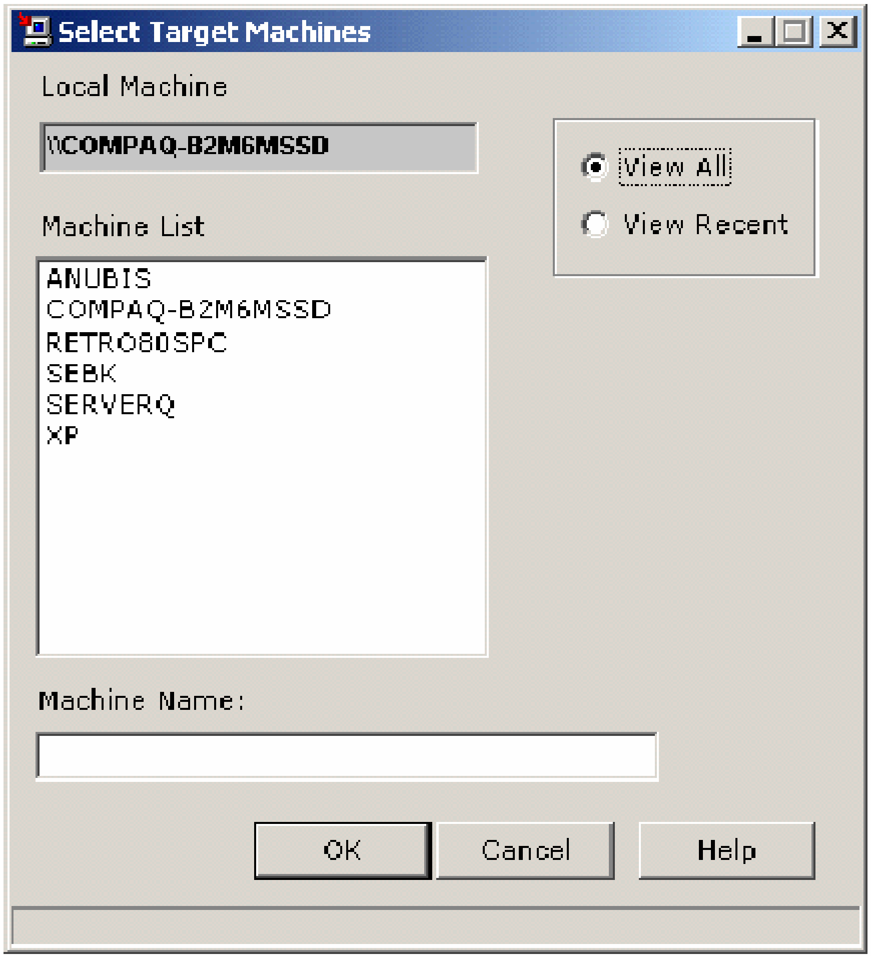
1. Locate the Available Resource Partitions panel and right-click *Compaq2*.
2. From the drop-down menu, select *Delete*. Click *Yes* to confirm the deletion. *Compaq2* no longer displays in the Available Resource Partitions panel.



Remotely Connecting to a Target Computer

To select a target computer:

1. Launch RPM.
2. Click the *Select target computer* button. The Select Target Machines window displays.



Local Machine: \\COMPAQ-B2M6MSSD

● View All
○ View Recent

Machine List:

ANUBIS
COMPAQ-B2M6MSSD
RETRO80SPC
SEBK
SERVERQ
XP

3. Click the *View All* radio button. From the Machine List, select a remote computer.

4. Click *OK* to connect to the target machine. The name of the target machine will display in the title bar of the RPM window.

Note

You must have at least two machines with RPM available displayed in the target machines window before selecting a target machine.

Connecting to remote computers enables administrators to control RPM activity with exiting management tools and processes. Working with other performance monitoring tools, RPM enables you to monitor and optimize performance locally and remotely.

High availability and clusters

Lab 5

Objectives

After completing this lab, you should be able to:

- Configure network properties
- Join the classroom domain
- Create a quorum disk
- Configure the Microsoft Cluster service
- Add disk storage to an existing HP ProLiant cluster
- Create and test a highly available file share
- Perform a direct attached storage (DAS) to storage area network (SAN) conversion
- Configure Modular SAN Array (MSA) 1000 support in Red Hat Enterprise Linux
- Boot from a SAN

Requirements

To complete this lab, you will need:

- The ProLiant servers you were working with in the previous lab, with:
    - Microsoft Windows Server 2003 installed
    - Windows Server 2003, Enterprise Edition installation files
- One HP StorageWorks Modular Smart Array (MSA) 500
- Two Fibre Channel FCA2214 host bus adapters (HBAs)
- Fiber cables
- MSA1000 Support Software CD
- HP ProLiant Essentials Rapid Deployment Pack (RDP) 1.40 or later
- An instructor server configured as a Windows 2003 domain controller, with:
    - Domain Name Service (DNS)
    - Domain administrator account with a username of *student* and a password of *password*

Introduction

As a result of the merger with the Greater Environment for the Expansion of Knowledge (GEEK), RC Engineering must migrate its equipment from SCSI to Fibre Channel. GEEK uses clusters attached to a SAN for data warehousing; RC Engineering has been using a DAS solution.

After helping Jackie and the rest of the IT staff at RC Engineering become familiar with Fibre Channel technology, you will need to perform a DAS to SAN (DtS) conversion. To complete this migration, you will need additional equipment.

GEEK and RC Engineering also need to be more highly available, and so Bob, the CEO of RC Engineering, and Carla, the managing director of GEEK, decide to cluster the ProLiant BL p-Class server blades at GEEK with the RC Engineering equipment.

Your job is to perform the DtS conversion. Then, using RDP, you will help RC Engineering deploy a two-node cluster attached to an MSA1000 running the Microsoft Cluster service.

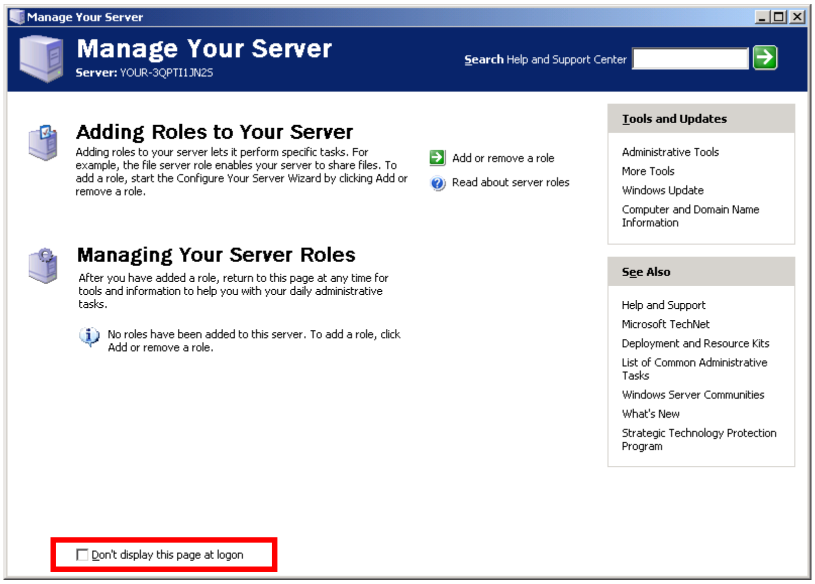
Exercise 1 — Configuring network properties

In this exercise, you will configure the network properties of the two Ethernet ports used in each server. Before you begin, ensure that both network cables are connected to LAN ports and that the SCSI cables are properly attached to the server and to the MSA500. Then power on both nodes.

> **Note**
> The shared storage device will not be used in this exercise.

Node A

1. Log on to node A as *Administrator* with a password of *password*.
2. If the Windows Server 2003 Manage Your Server wizard displays, select the *Don't display this page at logon* check box and close the window.



Manage Your Server
Manage Your Server
Server: YOUR-3QPTI1JN2S
Search Help and Support Center
Tools and Updates
Administrative Tools
More Tools
Windows Update
Computer and Domain Name Information
See Also
Help and Support
Microsoft TechNet
Deployment and Resource Kits
List of Common Administrative Tasks
Windows Server Communities
What's New
Strategic Technology Protection Program
Add or remove a role
Read about server roles
☐ Don't display this page at logon

Adding Roles to Your Server

Adding roles to your server lets it perform specific tasks. For example, the file server role enables your server to share files. To add a role, start the Configure Your Server Wizard by clicking Add or remove a role.

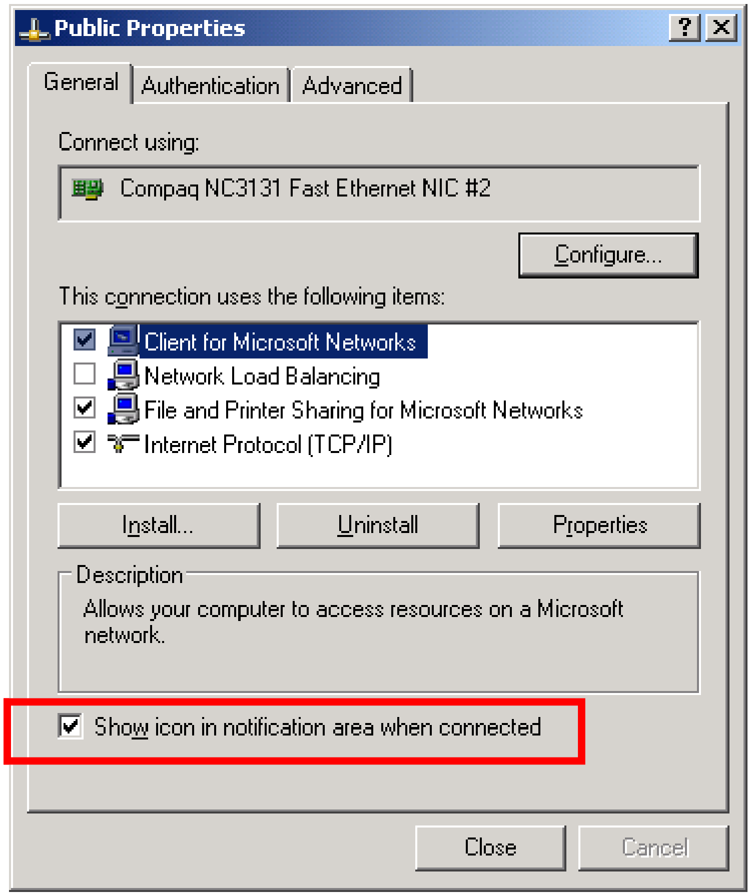
Managing Your Server Roles

After you have added a role, return to this page at any time for tools and information to help you with your daily administrative tasks.

No roles have been added to this server. To add a role, click Add or remove a role.

3. Click *Start*, right-click *Control Panel*, and choose *Open*.
4. Double-click *Network Connections*.
5. In the Network Connections window, rename the heartbeat connection *Private*.
6. Rename the LAN connection *Public*.
7. Right-click the Public connection and select *Properties*.

8. Select the *Show icon in notification area when connected* check box.



Connect using:

Compaq NC3131 Fast Ethernet NIC #2

This connection uses the following items:

☑ Client for Microsoft Networks
☐ Network Load Balancing
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected

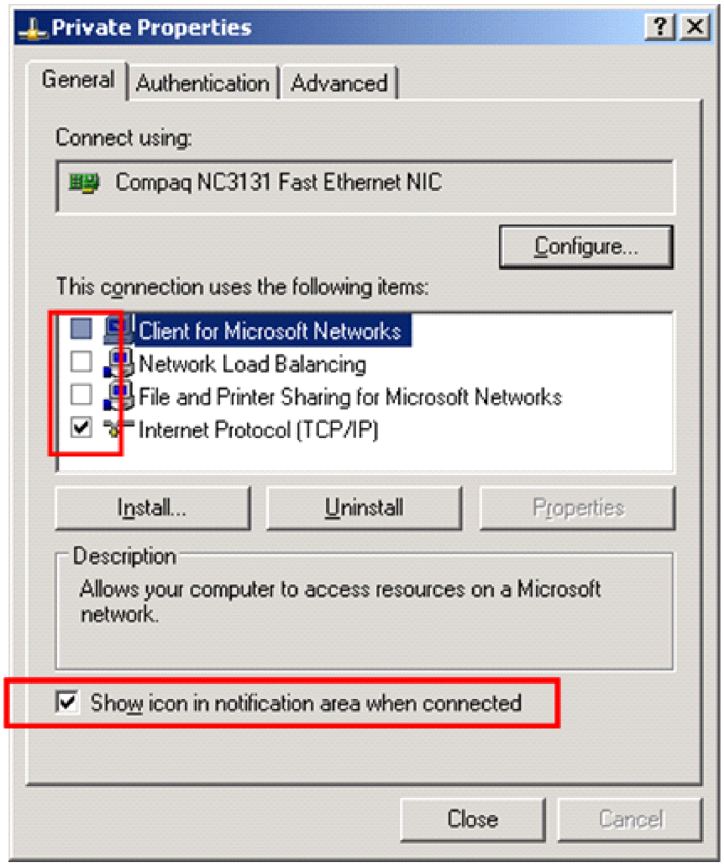
9. Select *Internet Protocol (TCP/IP)* and click *Properties*.

10. Select the *Use the following IP address:* radio button. Enter the following information:
    a. Static IP address: *192.168.0.x*, where *x* is your assigned group number
    b. Subnet mask: *255.255.255.0*
    c. Preferred DNS server: *IP address of instructor's server*
    d. Alternate DNS server: *leave blank*
11. Click *OK* to close the Internet Protocol (TCP/IP) Properties window. To close the Public Properties window and implement the setting changes, click *Close*.
12. Right-click the *Private* connection and select *Properties*.
13. Click *Configure*.
14. On the Advanced tab, change the *Speed & Duplex* property setting from *Auto detect* to *10 Mb Half* and click *OK*.

> **Note**
> You can select the *100 Mb Half* option if it is supported by the networking equipment that you are using.

15. Right-click *Private*; then select *Properties*.
16. From the General tab in the Private Properties window, deselect all protocols and services except TCP/IP and HP Network Teaming and Configuration.

17. Select the *Show icon in notification area when connected* check box. Ensure that your settings match those in the following screen shot.



Connect using: Compaq NC3131 Fast Ethernet NIC

This connection uses the following items:

- ☐ Client for Microsoft Networks
- ☐ Network Load Balancing
- ☐ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

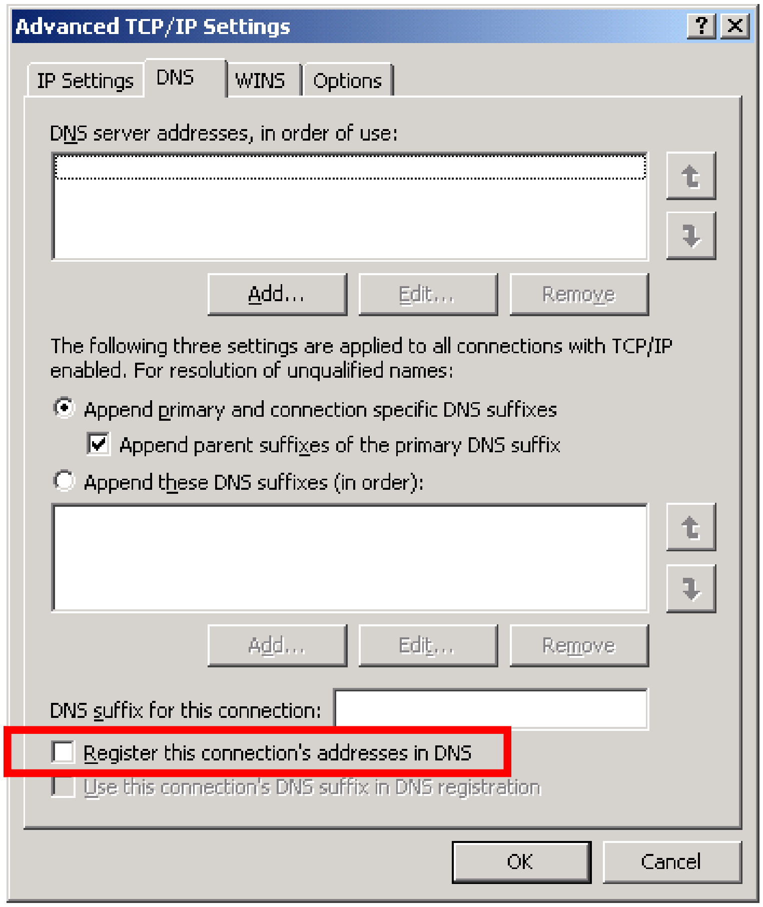
Description

Allows your computer to access resources on a Microsoft network.

☑ Show icon in notification area when connected

18. Select *Internet Protocol (TCP/IP)* and click *Properties*.
19. Select the *Use the following IP address:* radio button. Enter the following information:
    a. Static IP address: *10.1.1.1*
    b. Subnet mask: *255.0.0.0*
20. Click *Advanced*. The Advanced TCP/IP Settings window displays.

21. On the DNS tab, deselect the *Register this connection's address in DNS* check box.



The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

● Append primary and connection specific DNS suffixes

☑ Append parent suffixes of the primary DNS suffix

○ Append these DNS suffixes (in order):

☐ Register this connection's addresses in DNS

☐ Use this connection's DNS suffix in DNS registration

22. On the WINS tab, select *Disable NetBIOS over TCP/IP*. To close the Advanced TCP/IP Settings window, click *OK*. To close the Internet Protocol (TCP/IP) Properties window, click *OK*. To close the Private Properties window and implement the setting changes, click *Close*.

Node B

1. Log on to node B as *Administrator* with a password of *password*.
2. If the Windows Server 2003 Manage Your Server wizard displays, select the *Don't display this page at logon* check box and close the window.
3. Click *Start*, right-click *Control Panel*, and choose *Open*.
4. Double-click *Network Connections*.
5. In the Network Connections window, rename the heartbeat connection to *Private*. Rename the LAN connection to *Public*. Right-click the *Public* connection and select *Properties*.
6. Select the *Show icon in notification area when connected* check box.
7. Select *Internet Protocol (TCP/IP)*; then click *Properties*.
8. Select the *Use the following IP address:* radio button. Enter the following information:
    a. Static IP address: *192.168.0.x2*, where *x* is your assigned group number.
    b. Subnet mask: *255.255.255.0*
    c. Enter the IP address of the primary domain controller (PDC) for the Preferred DNS server address and leave the Alternate DNS server address blank.
9. Click *OK* to close Internet Protocol (TCP/IP) Properties window.
10. Click *Close* to exit the Public Properties window and implement the settings.
11. Right-click the *Private* connection and select *Properties*. Click *Configure*.
12. On the Advanced tab, ensure that the NIC Link Speed & Duplex property settings for the node B private connection Ethernet port are the same as previously selected for the node A private connection Ethernet port (*10Mbps/Half Duplex* or *100Mbps/Half Duplex*). Then click *OK*.
13. Right-click *Private*; then select *Properties*.

14. On the General tab of the NIC properties, deselect all protocols and services except TCP/IP. Select the *Show icon in notification area when connected* check box. Then select *Internet Protocol (TCP/IP)* and click *Properties*.
15. Select the *Use the following IP address:* radio button. Enter the following information:
    a. Static IP address: *10.1.1.2*
    b. Subnet mask: *255.0.0.0*

    Then click *Advanced*.
16. On the DNS tab, deselect the *Register this connection's address in DNS* check box. On the WINS tab, select *Disable NetBIOS over TCP/IP*.
17. Click *OK* to close the Advanced TCP/IP Settings window. Click *OK* to close the Internet Protocol (TCP/IP) Properties window. To close the Private Properties window and implement the settings, click *Close*.
18. At the command prompt, use the ipconfig and ping commands to verify that all network interfaces are configured correctly and that both nodes can communicate with each other. Then close the command prompt window.
19. Close the Network Connections windows on each node.

Exercise 2 — Joining the classroom domain

All nodes in a Cluster service cluster must be members of the same domain and must be able to access a domain controller and a DNS server. Nodes can be configured as domain controllers or member servers, but a combination of member servers and domain controllers cannot be mixed in the same cluster. If you configure one node as a domain controller, you must also configure the remaining nodes as domain controllers.

Caution
Configuring the nodes of a cluster as domain controllers is not recommended and can cause problems with your cluster or clustered applications.

In the classroom configuration, the instructor has a domain controller and DNS configured. In this exercise, you will register in the instructor's DNS and join the instructor's domain.

Renaming node A and joining the domain

1. On node A, click *Start*, right-click *My Computer*, then click *Properties*.
2. On the Computer Name tab, click *Change*.
3. Enter *NODExA* for the computer name, where *x* is your assigned student group number. Select the *Domain* radio button. Enter *CLASSROOM* for the domain name; then click *OK*. The Computer Name Change dialog box displays.
4. Enter *CLASSROOM\student* and *password*. Click *OK* → *OK* → *Yes*, to restart.

Renaming node B and joining the domain

5. On node B, click *Start*, right-click *My Computer*, click *Properties*.
6. On the Computer Name tab, click *Change*.
7. Enter *NODExB* for the computer name, where *x* is your assigned student group number. Select the *Domain* radio button. Enter *CLASSROOM* for the domain name; then click *OK.* The Computer Name Change dialog box displays.
8. Enter *CLASSROOM\student* and *password*. Click *OK* → *OK* → *Yes*, to restart.

! **Important**
The student account is a domain account that is a member of Domain Admins in the CLASSROOM domain. You will use this account for all future logins.

Exercise 3 — Creating the quorum disk

1. Shut down node B and power on the shared storage system.
2. On node A, detect the newly available storage by clicking *Start* → *Administrative Tools* → *Computer Management*. In the left pane, click *Device Manager.* In the right pane, right-click *nodeA* and click *Scan for Hardware Changes*.

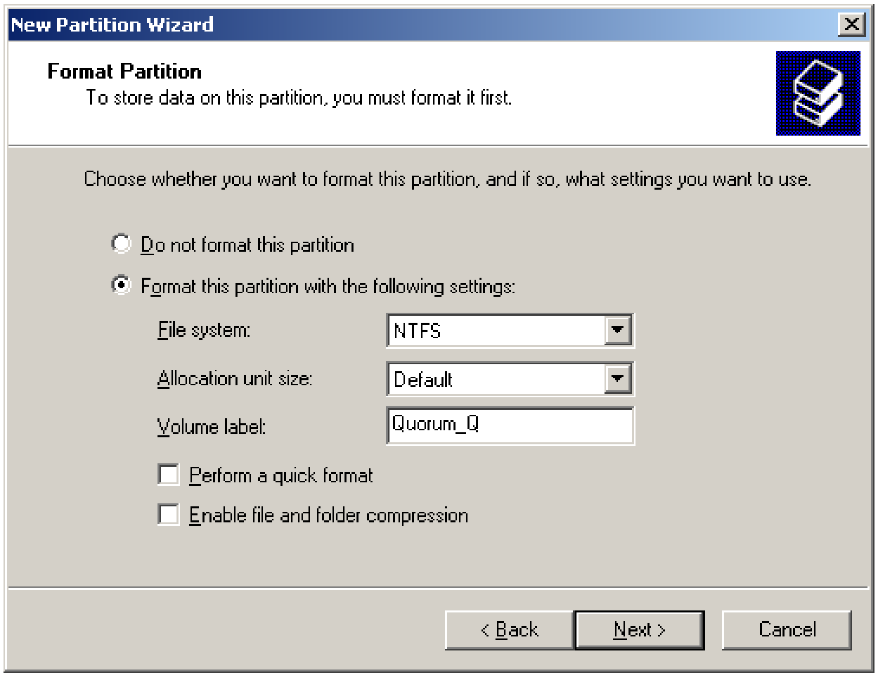
> **Note**
> You can also detect the newly available storage by restarting the node.

3. Using the appropriate utilities for the shared storage system, create a single array using all of the disks in the shared storage.
4. Create a 1024MB fault-tolerant logical drive.
5. Save your changes and exit the utility.
6. Click *Start* → *Administrative Tools* → *Computer Management*.
7. From the left pane of the Computer Management screen, select *Disk Management*.
8. Using the New Partition Wizard, initialize the new disk but do not convert it to a dynamic disk.

> **!** **Important**
> Only **basic** disks are supported for shared storage in a cluster. If you accidentally upgraded them to **dynamic**, you must revert them back to basic. You must format the new partitions with the Windows NT file system (NTFS). The Cluster service does not recognize the file allocation table (FAT) file system. Configure the drive sizes and drive letters exactly as specified in this exercise because later exercises depend on this configuration.

9. Create a primary partition on the drive and accept the default size.
10. Select *Q* as the drive letter.

11. Format the partition with NTFS, using *Quorum_Q* as the volume name.



New Partition Wizard

Format Partition

To store data on this partition, you must format it first.

Choose whether you want to format this partition, and if so, what settings you want to use.

○ Do not format this partition

● Format this partition with the following settings:

File system: NTFS

Allocation unit size: Default

Volume label: Quorum_Q

☐ Perform a quick format

☐ Enable file and folder compression

Note

These exercises include an underscore followed by the drive letter in the volume label. This will make it easier to notice when drive letter assignments have changed. It will also make recovering from drive letter changes easier.

---

12. Click *Next* → *Finish*. Close the utility.
13. Power on node B and log on.
14. Click *Start* → *Administrative Tools* → *Computer Management*.
15. Click *Disk Management*. Change the quorum drive letter to *Q*; then close the utility.

Exercise 4 — Configuring the Cluster service

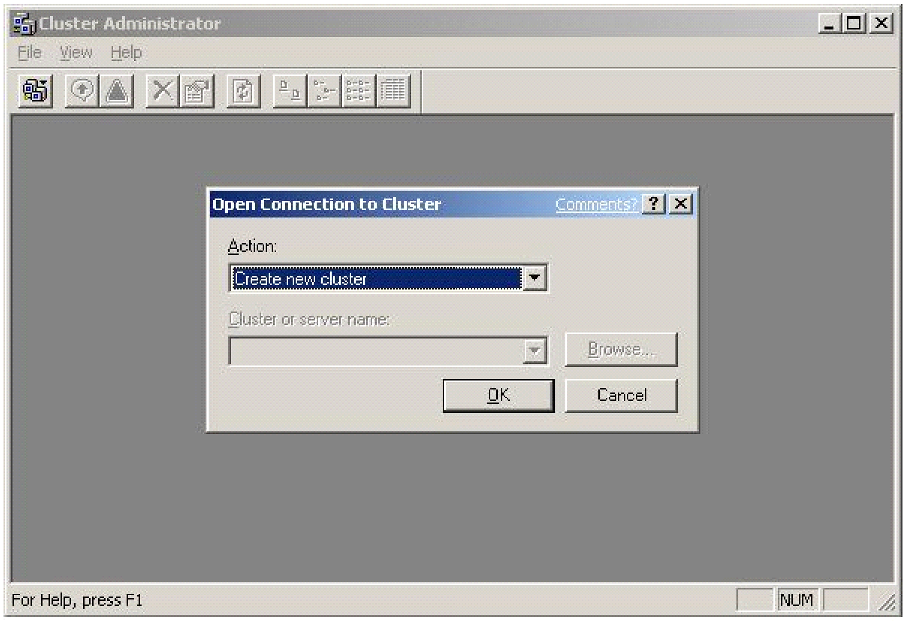
Note

During installation of the Cluster service on the first node, all other nodes must either be powered down or stopped before the Windows Server 2003 operating system startup. Ensure that all shared storage devices are powered up and ready before starting the first node.

In the first phase of installation, you must supply all initial cluster configuration information so that the cluster can be created. Use the Cluster Service Configuration Wizard to accomplish this task.

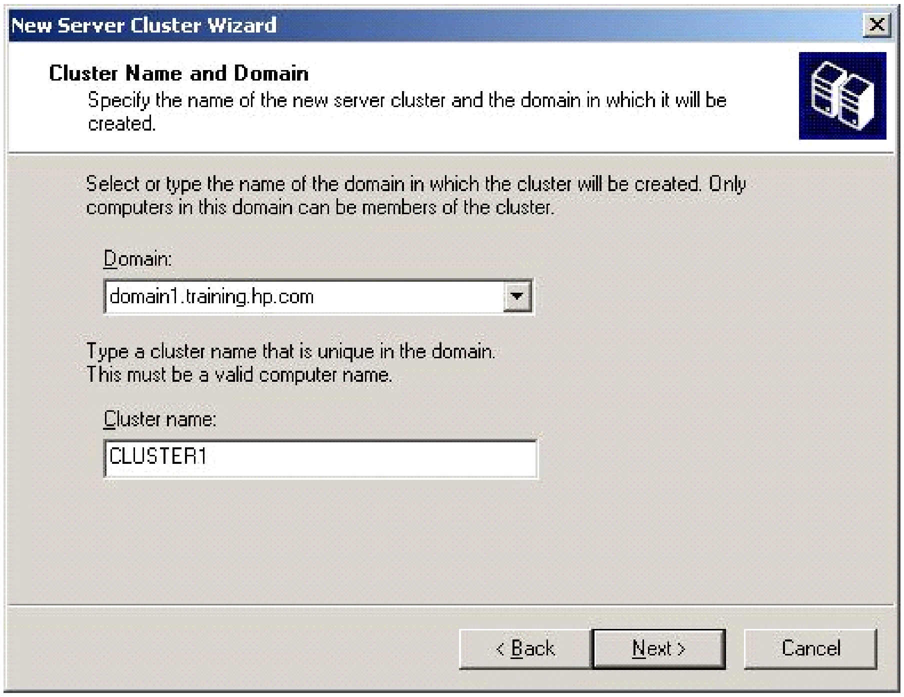
Configuring node A

1. On node A, click *Start* → *Administrative Tools* → *Cluster Administrator*.
2. In the Open Connection to Cluster dialog box, from the Action drop-down list, select *Create new cluster*. Click *OK*.



Action: Create new cluster

3. When the New Server Cluster Wizard Welcome screen displays, click *Next*.
4. For the Cluster name, enter *CLUSTERx*, where *x* is your assigned student group number; then click *Next*.



Cluster Name and Domain

Specify the name of the new server cluster and the domain in which it will be created.

Select or type the name of the domain in which the cluster will be created. Only computers in this domain can be members of the cluster.

Domain: domain1.training.hp.com

Type a cluster name that is unique in the domain. This must be a valid computer name.

Cluster name: CLUSTER1

! **Important**

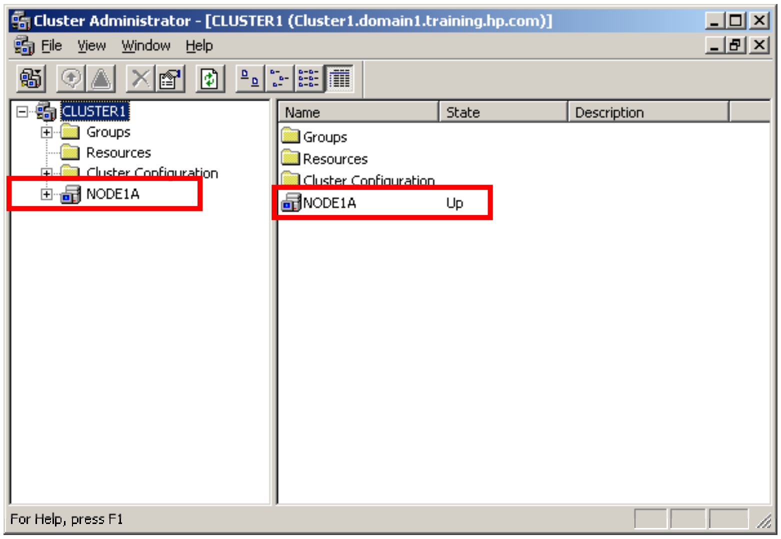
The cluster name is a NetBIOS name and therefore must be different from the domain name, all computer names in the domain, and other cluster names in the domain. These exercises use the domain name *CLASSROOM*, the node names *NODExA* and *NODExB*, and the cluster name *CLUSTERx,* where *x* is your assigned student group number.

5. If the cluster uses a crossover cable for the private heartbeat connection, power on node B to enable the New Server Cluster Wizard to detect the private connection Ethernet port as an operational port
6. Verify that *NODExA* is the computer name for the first node in the new cluster, where *x* is your assigned student group number. Then click *Next*.
7. The Analyzing Configuration window displays. When the analysis completes there should be no errors. Click *Next*.
8. Enter the IP address *192.168.0.x3*, where *x* is your assigned student group number. Then click *Next*.
9. Enter *svcCLUSTER*. This is the user name of the Cluster service account that was created on the Domain Controller (instructor's server). In the password field, enter *password*. Enter the domain name if it is not supplied by default and click *Next*.
10. Click *Next* to accept the proposed cluster configuration.
11. After the cluster is created, click *Next*.
12. Click *Finish*.

Validating the cluster installation on node A

Use the Cluster Administrator snap-in to validate the Cluster service installation on the first node.

1. If you closed Cluster Administrator, click *Start → Administrative Tools → Cluster Administrator*.
2. Verify that node A is listed.



Name	State	Description
Groups		
Resources		
Cluster Configuration		
NODE1A	Up	

Note

You can also launch Cluster Administrator using *cluadmin.exe*.

The Cluster service was successfully configured on the first node. You are now ready to configure the Cluster service on additional nodes.

Configuring node B

Note

For this section, leave node A and all shared disks powered up. Power up node B.

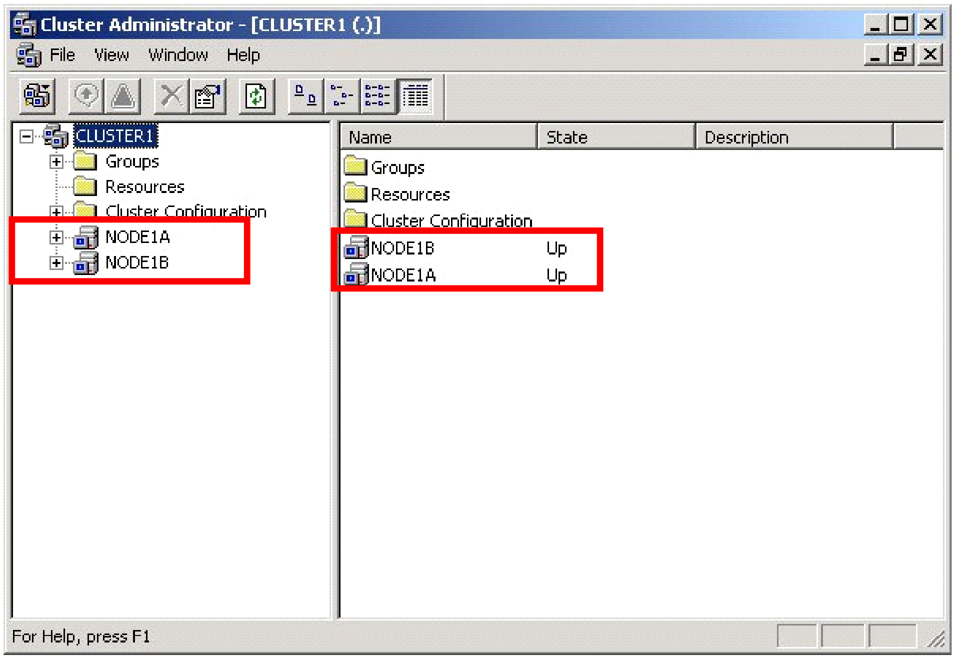
Configuring the Cluster service on additional nodes requires less time than on the first node. Setup configures the Cluster service network settings on the second node based on the configuration of the first node.

1. Power on node B. The multinode addition feature of Windows Server 2003 allows the addition of other nodes from a single console. Multiple nodes can be added at one time. In this exercise, you will only be adding a second node.
2. In Cluster Administrator on node A, right-click *CLUSTERx*, where *x* is your assigned student group number. Then select *New* → *Node*.
3. When the Add Nodes Wizard displays, click *Next*.
4. Enter *NODExB* and click *Add* → *Next*.
5. When the configuration analysis is complete, click *Next*.
6. The Cluster Service Configuration Wizard automatically supplies the name of the user account selected during the installation of the first node. Always use the same account that you used when setting up the first cluster node. Enter *password* as the password and click *Next*.
7. The proposed Cluster Configuration window displays. To add nodes to a cluster with this configuration, click *Next*.
8. The Adding Nodes to the Cluster window displays. After the cluster is configured, click *Next*.
9. Click *Finish*.

Validating the cluster installation on node B

Use the Cluster Administrator snap-in to validate the Cluster service installation on the second node.

1. If you closed Cluster Administrator, click *Start* → *Administrative Tools* → *Cluster Administrator*.
2. Verify that node A and node B are listed in the Cluster Administrator window. This confirms that the Cluster service was installed successfully on the second node.

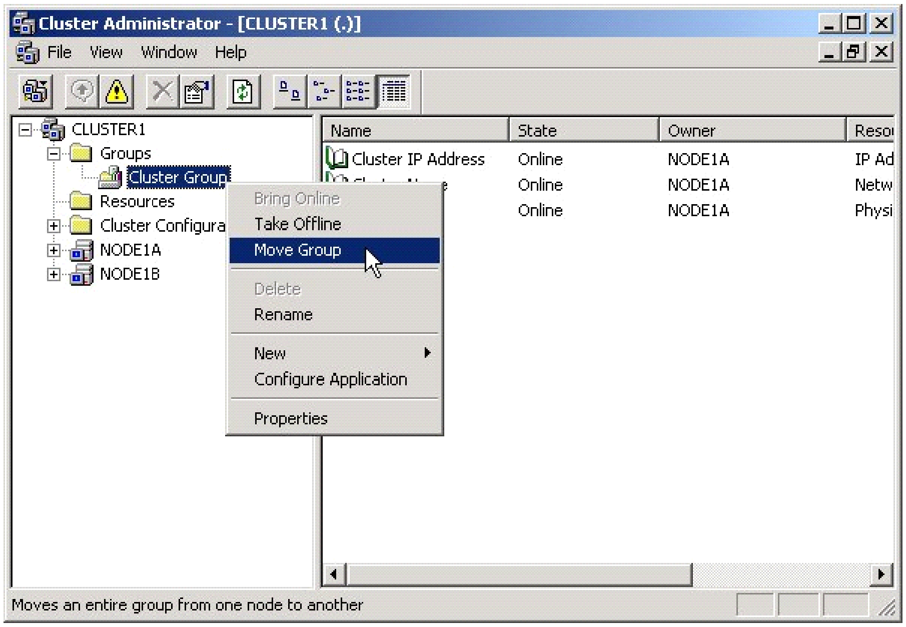


Name	State	Description
Groups		
Resources		
Cluster Configuration		
NODE1B	Up	
NODE1A	Up	

Verify that the quorum can fail over and fail back

Verify that the cluster group can fail over and fail back by completing the following steps.

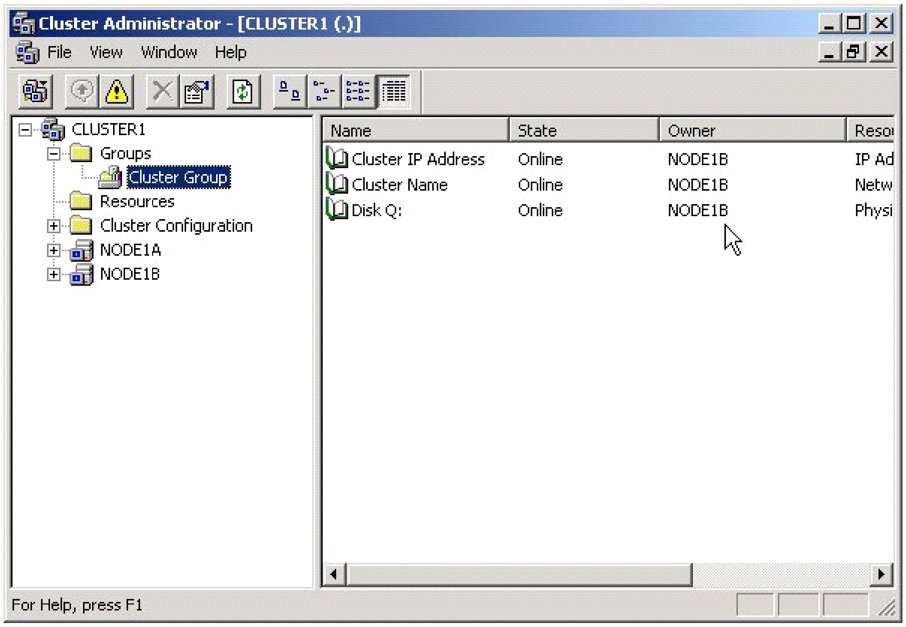
1. In Cluster Administrator, click the plus sign (+) to the left of *Groups*.
2. Right-click *Cluster Group*. From the pop-up menu, click *Move Group*.



Name	State	Owner	Reso
Cluster IP Address	Online	NODE1A	IP Ad
	Online	NODE1A	Netw
	Online	NODE1A	Physi

Moves an entire group from one node to another

3. Observe the State and Owner columns. The objects in the group should go offline on node A and come online on node B.



Name	State	Owner	Reso
Cluster IP Address	Online	NODE1B	IP Ad
Cluster Name	Online	NODE1B	Netw
Disk Q:	Online	NODE1B	Physi

4. Right-click *Cluster Group*. From the pop-up menu, click *Move Group*.

5. Observe the State and Owner columns. The objects in that group should go offline on node B and come online on node A. If this is successful, the cluster is working properly.

Exercise 5 — Adding disk storage to a Windows Server 2003 cluster

In this exercise, you will create a new logical drive on your shared storage, partition it, and assign a drive letter to it on both nodes of your cluster.

1. On node A, use the appropriate utility for your shared storage system to create a fault-tolerant 1000MB logical drive. Save the settings and close the utility.
2. Click *Start* → *Administrative Tools* → *Computer Management* → *Storage* → *Disk Management*.
3. Click *Next* at the Initialize and Convert Disk Wizard.
4. Verify that the check box next to the new disk is selected and click *Next*.
5. Do not convert the disk. Click *Next*.
6. At the Summary screen, click *Finish*.

Note

If the new drive does not display, wait a few seconds; then click *Action* → *Rescan disks*.

---

7. Right-click the unallocated disk space on the 1000MB logical drive. From the drop-down menu, click *New Partition*.
8. Click *Next* at the Welcome Screen.
9. Select *Primary Partition* → *Next*. Create a primary partition on the 1000MB logical drive, using all available space on the volume. Click *Next*.
10. Assign the drive letter *R* to the 1000MB logical drive. Click *Next*.

11. At the Format Partition window, format the new partition with NTFS and assign *Fileshare_R* as the volume label. Click *Next*.

> ! **Important**
> You must format the new partition with NTFS. The Microsoft Cluster service does not recognize the FAT file system.

12. Click *Finish* and restart node A.

> **Note**
> Restarting the nodes ensures that the Cluster service reinitializes so that it can detect the new drive.

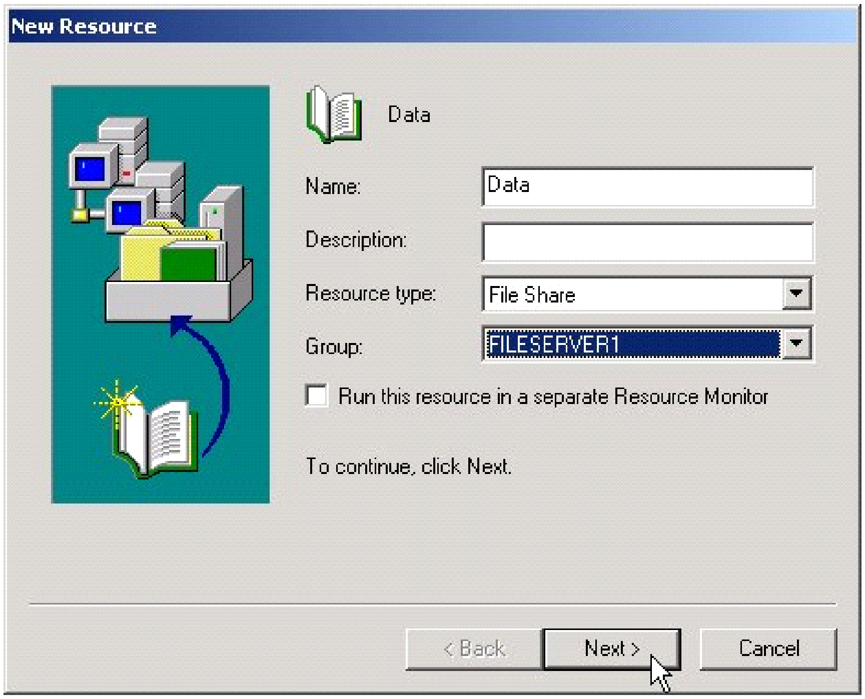
13. When node A has restarted and rejoined the cluster, restart node B.
14. Using the Microsoft Management Console (MMC) Disk Management snap-in on each node, verify that both nodes see the new storage and have the drive letter *R* assigned to them. Change the drive letter if needed. Also ensure that:
    - It is a basic disk
    - The volume label is correct
    - The disk is formatted with NTFS
15. Verify that drive letter *Q* is assigned to the 1000MB logical drive that serves as the quorum disk. You might need to move the cluster group from one node to the other. If both nodes have owned the quorum drive, the drive letter *Q* should be assigned to the 1000MB logical drive on both nodes. Otherwise, the quorum could possibly display as an unknown disk within Disk Management on one node.
16. Close Disk Management on both nodes.

Exercise 6 — Creating highly available file shares

During this exercise, you will configure the newly created storage as a highly available file share.

1. On node A, open Cluster Administrator and select your cluster. Click *File* → *Configure Application*.
2. The Cluster Application Wizard starts. At the Welcome screen, click *Next*.
3. At the Select or Create a Virtual Server screen, ensure that *Create a new virtual server* is selected and click *Next*.
4. At the Resource Group for the Virtual Server screen, select *Create a new resource group*; then click *Next*.
5. At the Resource Group Name screen, enter *FILESERVERx* as the name, where *x* is your assigned student group number; then click *Next*.
6. At the Virtual Server Access Information screen, enter the following information; then click *Next*.
    - Network name = *FILESERVERx*
    - IP address = *192.168.0.x4*
7. At the Advanced Properties for the New Virtual Server screen, click *Next*.
8. When prompted to create a cluster resource, select *Yes, create a cluster resource for my application now*; then click *Next*.
9. When prompted for the Application Resource Type, select *Physical Disk* from the drop-down list; then click *Next*.
10. At the Application Resource Name and Description screen, enter *Disk R:* as the name; then click *Next*.
11. At the Disk Parameters for Disk R: screen, ensure that *R: (Fileshare_R)* is selected; then click *Next*.
12. At the Completing the Cluster Application Wizard screen, verify that the information is correct; then click *Finish*.
13. Right-click the *FILESERVERx* group and click *Bring Online*. Confirm that the group was brought online.
14. Right-click the *FILESERVERx* group and click *New* → *Resource*.

15. The New Resource screen displays. Assign the following parameters to the new resource and click *Next*.
    - Name = *Data*
    - Resource type = *File Share*
    - Group = FILESERVERx



Name: Data

Description:

Resource type: File Share

Group: FILESERVER1

☐ Run this resource in a separate Resource Monitor

To continue, click Next.

16. Ensure that both servers are possible owners; then click *Next*.
17. At the Dependencies screen, select the *FILESERVERx* name resource and add it to the Resource Dependencies column; then click *Next*.
18. At the File Share Parameters screen, enter the following:
    - Share Name = *DATA*
    - Path = *R:\*
    - Comment = *File Share*
19. Leave the other parameters at their default values. Click *Finish* → *OK* to complete the process.
20. Right-click the *FILESERVERx* group and select *Bring Online*. Confirm that the group was brought online.

Testing the highly available file share

To test the highly available file share that you just created, connect to the share and start viewing a movie stored there. While the movie is playing, move the group from one node to the other to simulate a failover. Then observe the client behavior during a failover event on a file share.

1. Copy the video from the instructor machine to drive R on your cluster. To copy the file to the drive, in the address bar of Windows Explorer, you must specify the R:\ drive. Otherwise, it is a hidden drive.
2. From a client machine, connect to the file share. Be sure to use the virtual server name that you configured for the group, *\\FILESERVERx\DATA*.
3. Start the movie.
4. When the movie is playing, use Cluster Administrator to move the group from one node to the other.
5. Observe what happens to the movie on the client.
6. Close the Windows Media Player.

Exercise 7 — DAS to SAN conversion

SAN architecture is widely accepted as the definitive solution for networked storage and storage consolidation. However, organizations are often concerned about the cost and complexity of deploying and managing a SAN. HP provides a technology that simplifies the migration of storage data from a DAS infrastructure to a SAN.

The HP DAS to SAN (DtS) technology enables you to remove drives from specific HP directly attached drive arrays and place them inside an HP StorageWorks Modular SAN Array (MSA), providing seamless migration from one type of architecture to another.

Identifying Fibre Channel components

When storage requirements evolve and a Fibre Channel solution becomes more attractive for additional scalability such as multi-cluster functionality, you can easily convert the MSA500 to a SAN. To learn to recognize Fibre Channel components, begin by identifying the SCSI cable connecting the server blade enclosure with the MSA500. Then answer the following questions:

1. What are the disadvantages of SCSI in a SAN, when compared to Fibre Channel?

   ....

   ....

2. What do you need to make a Fibre Channel connection between the server blade and the MSA500?

   ....

   ....

3. What must be removed to make room for this new equipment?

   ....

4. Do you need a Fibre Channel hub or switch for this connection? Why or why not?

   ....

   ....

   ....

   ....

Converting the MSA500 to an MSA1000

INTER NET

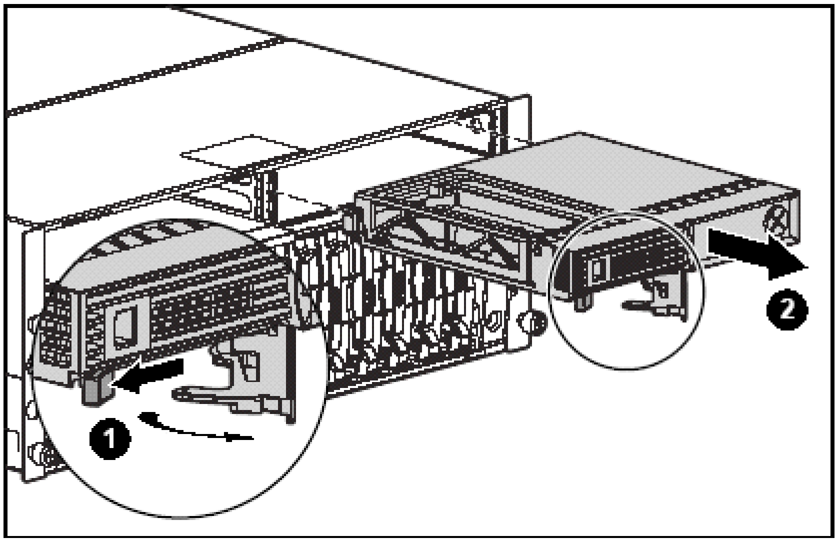
For more information on the HP StorageWorks MSA1000, visit:
h18006.www1.hp.com/products/storageworks/msa1000/index.html

For more information on the DtS function of the MSA1000, visit:
ftp://ftp.compaq.com/pub/products/storageworks/whitepapers/15D6-0801A-WWEN.pdf

Removing the MSA500 controller

To remove the controller from the MSA500 storage system, perform the following steps:

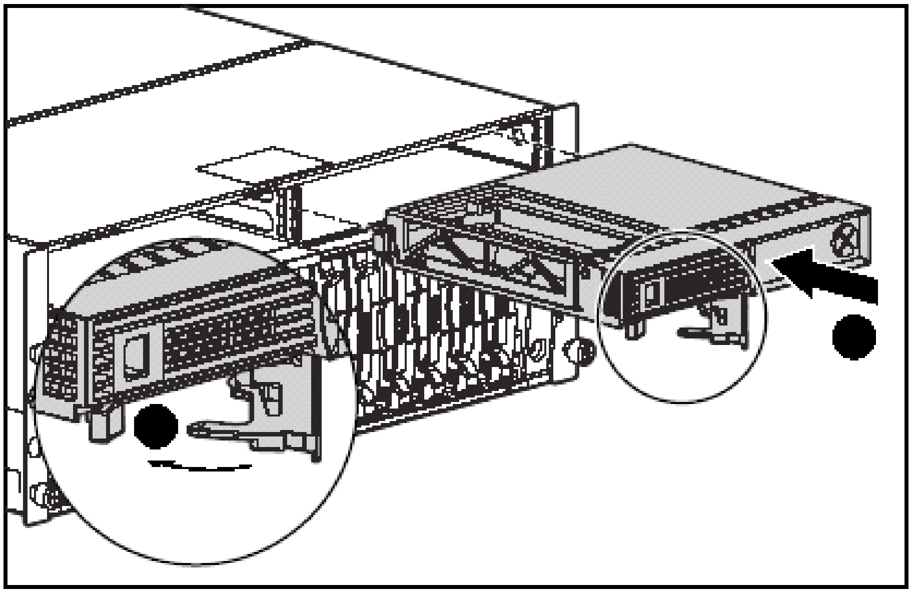
1. Press the thumb latch on the controller and pull the latch handle toward you.
2. Remove the MSA500 controller by pulling it straight out of the chassis.



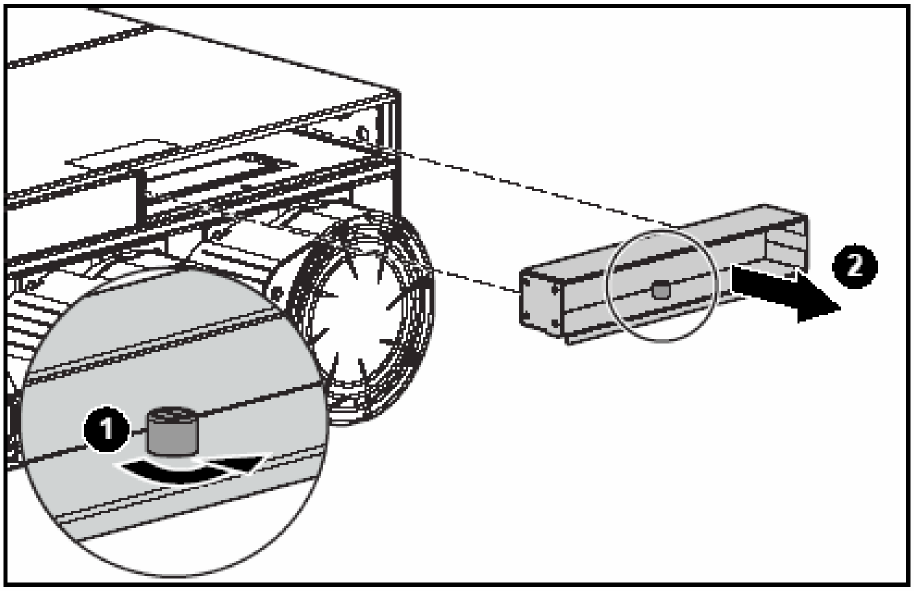
Inserting the MSA1000 controller

To insert the new controller into the MSA500 storage system, perform the following steps:

1. Position the MSA1000 controller in the chassis.
2. Push the controller in as far as it will go. Press the latch inwards until it is flush against the front panel.



3. To install the MSA Fibre Channel I/O Module (or MSA Fabric Switch 2/8) into the corresponding slot on the back of the storage system, remove the blanking panel from the back of the storage system by loosening the thumbscrew that holds the panel in place and removing the panel from the back of the unit.

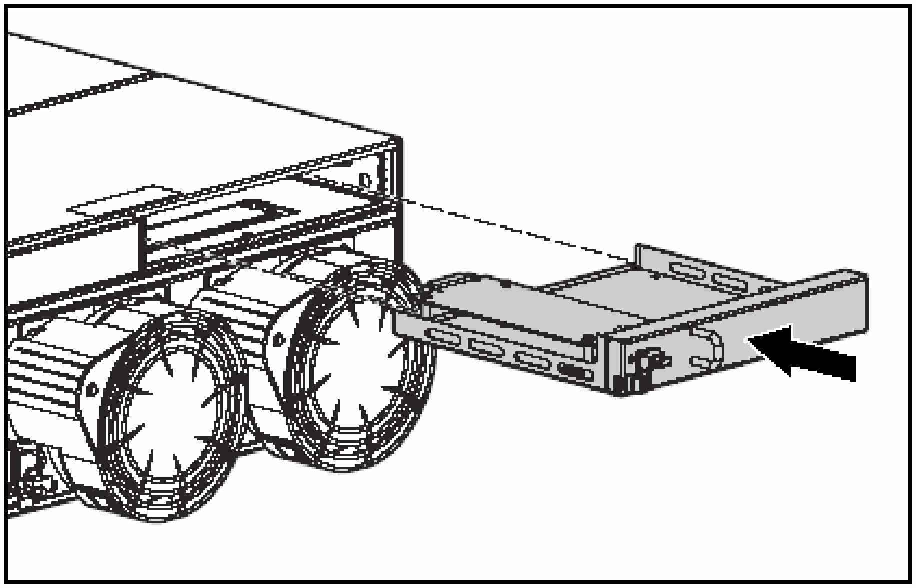


Note

The MSA SAN Switch 2/8 is an optional eight-port 2GB/s Fibre Channel fabric switch. Use this switch or the MSA Hub 2/3 to replace the standard single-port Fibre Channel connection provided by the MSA Fibre Channel I/O Module. For more information, refer to the product user guides available online at: **http://h18000.www1.hp.com/products/storageworks/msa1000/documentation.html**

---

4. Slide the I/O Module in as far as it will go and press in firmly to ensure that the module is securely seated in the storage system.



5. Disconnect the SCSI cables from the storage system and servers.
6. Install the FCA2214 HBA in the slot in the server and attach the fiber optic interconnect component for appropriate communication with the storage system. Ensure that all interconnect components are in place for proper connection to the storage system. Repeat this step for additional servers.
7. Connect the FCA2214 HBA in the server to the MSA Fibre Channel I/O Module in the back of the storage system using Fibre Channel cables. Repeat this step for additional servers.

> **Note**
>
> If using a switch (or dual switches), connect the Fibre Channel HBAs from the server and the MSA Fibre Channel I/O Module to the switches.

8. Power on the storage system. The LCD should display a message stating *MSA1000 Startup Complete*.
9. Power on the server.
10. After the server reboots, a New Hardware Found message displays. Click the *Cancel* button.
11. Right-click *My Computer* and select *Manage*.
12. Select *Disk Management* under *Storage*. You should now be able to see the volumes on the MSA1000.

Exercise 8 — Configuring MSA1000 support in Red Hat Enterprise Linux

Complete the following steps if you are using an MSA1000 for external storage.

1. Verify that the MSA1000 firmware is version 2.38 or later.
2. Download the latest FCA2214 Fibre Channel HBA driver for Linux.

Note

This driver can be obtained from HP website at:
http://h18000.www1.hp.com/products/storageworks/fca2214/index.html

---

3. Using the following command, untar the driver file into a temporary directory such as /tmp.

```
tar xzvf /tmp/qla604_rdp_kit.tar.gz
```

4. Use the rpm command to install the FCA2214 HBA driver, where *X.X.X.X* represents the version of the driver you downloaded previously.

```
rpm –ivh qla2x00-X.X.X-X.Redhat-AS-2-1.i386.rpm
```

5. Run the lsmod command and verify that the driver loaded. You should see results similar to the following:

```
Module                   Size  Used by  Not tainted
qla2300                246528        0  (unused)
nls_iso8859-1            3520        0  (autoclean)
ide-cd                  35296        0  (autoclean)
cdrom                   35520        0  (autoclean) [ide-cd]
soundcore                7940        0  (autoclean)
pcmcia_core             57440        0
autofs                  13796        0  (autoclean) (unused)
bcm5700                107780        2
usb-ohci                23392        0  (unused)
usbcore                 68864        1  [usb-ohci]
ext3                    73536        2
jbd                     55048        2  [ext3]
cciss                   44992        3
sd_mod                  13468        0  (unused)
scsi_mod               124988        2  [qla2300 cciss sd_mod]
```

6. Using the MSA 1000 Support Software CD, install the Array Configuration Utility (ACU) by placing the CD into the CD-ROM drive and executing the following commands: (replace *X.X.X.X* with the version of ACU you are installing.)

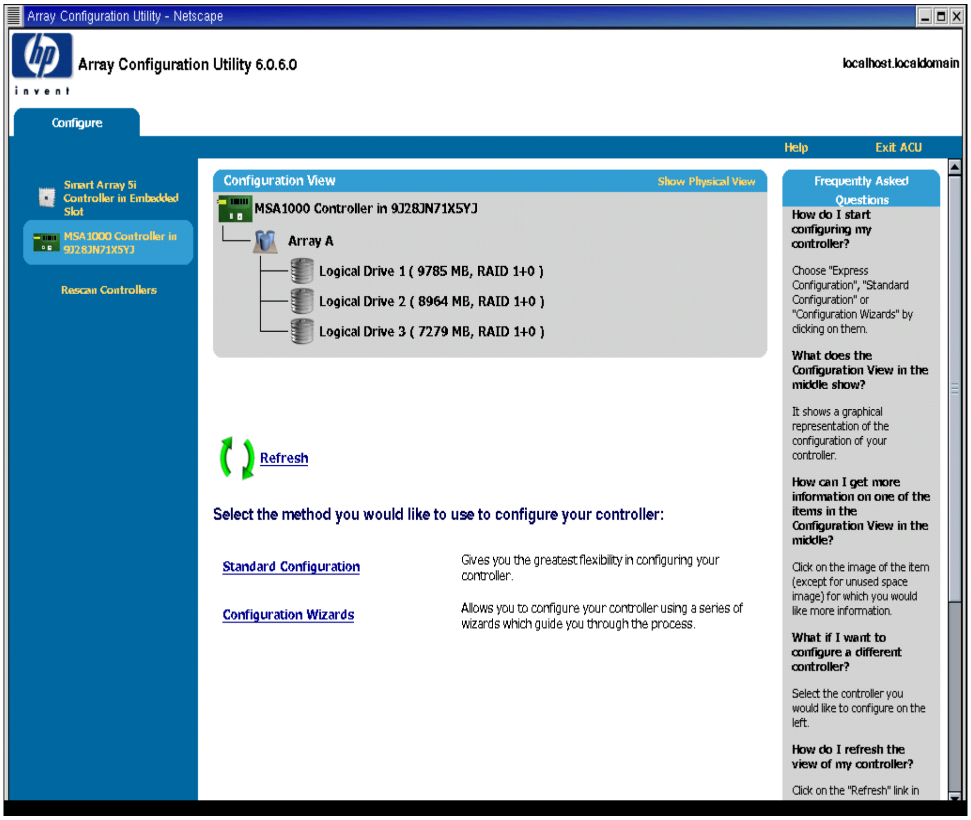
   ```
   mount /mnt/cdrom

   cd /mnt/cdrom/LINUX/onacu

   rpm –ivh cpqacuxe-X.X.X.X.i386.rpm
   ```

7. Start the cpqacuxe service.

   ```
   cpqacuxe -R
   ```

8. If the HP HyperMedia Managed Object (HMMO) administrator password is not set, you will be prompted for the password the first time you start the service. Enter a new password and press *Enter*.
9. Open a web browser that supports Secure Sockets Layer (SSL) and navigate to the URL: **https://localhost:2301**
10. Log in to HP Web-Based Management with the user *administrator* and the password you entered in step 8.
11. Click *Array Configuration Utility* from the Device Home Page.
12. Select *MSA1000 Controller*.

13. Create three logical drives using the standard configuration method provided by ACU. When you are finished the configuration view should resemble the following screen shot.


Array Configuration Utility - Netscape
Array Configuration Utility 6.0.6.0
localhost.localdomain
invent
Configure
Help
Exit ACU
Smart Array 5i Controller in Embedded Slot
MSA1000 Controller in 9J28JN71X5YJ
Rescan Controllers
Configuration View
Show Physical View
Refresh
Standard Configuration
Configuration Wizards
Frequently Asked Questions

MSA1000 Controller in 9J28JN71X5YJ
- Array A
  - Logical Drive 1 (9785 MB, RAID 1+0)
  - Logical Drive 2 (8964 MB, RAID 1+0)
  - Logical Drive 3 (7279 MB, RAID 1+0)

Select the method you would like to use to configure your controller:

Standard Configuration	Gives you the greatest flexibility in configuring your controller.
Configuration Wizards	Allows you to configure your controller using a series of wizards which guide you through the process.

How do I start configuring my controller?

Choose "Express Configuration", "Standard Configuration" or "Configuration Wizards" by clicking on them.

What does the Configuration View in the middle show?

It shows a graphical representation of the configuration of your controller.

How can I get more information on one of the items in the Configuration View in the middle?

Click on the image of the item (except for unused space image) for which you would like more information.

What if I want to configure a different controller?

Select the controller you would like to configure on the left.

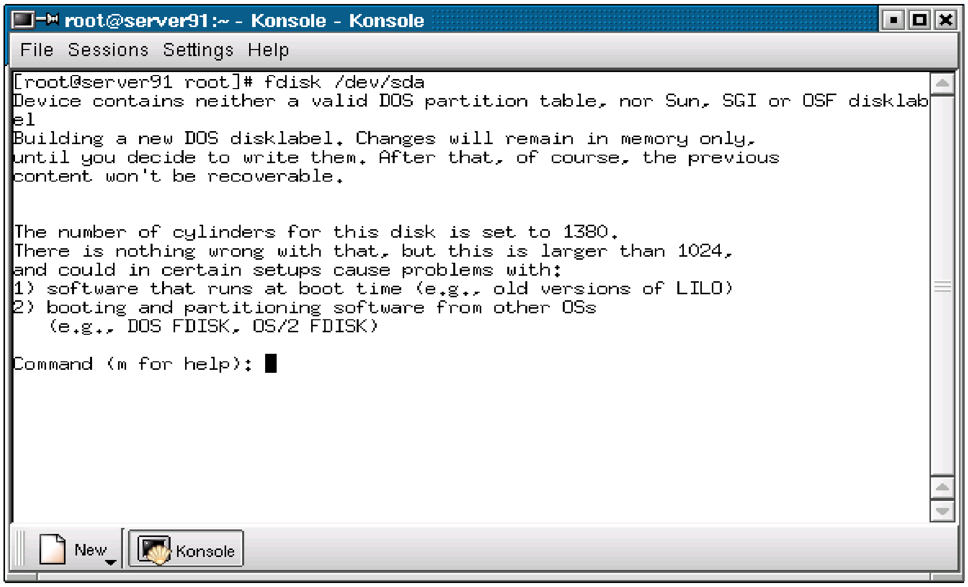
How do I refresh the view of my controller?

Click on the "Refresh" link in

Creating the extended partition and logical drives

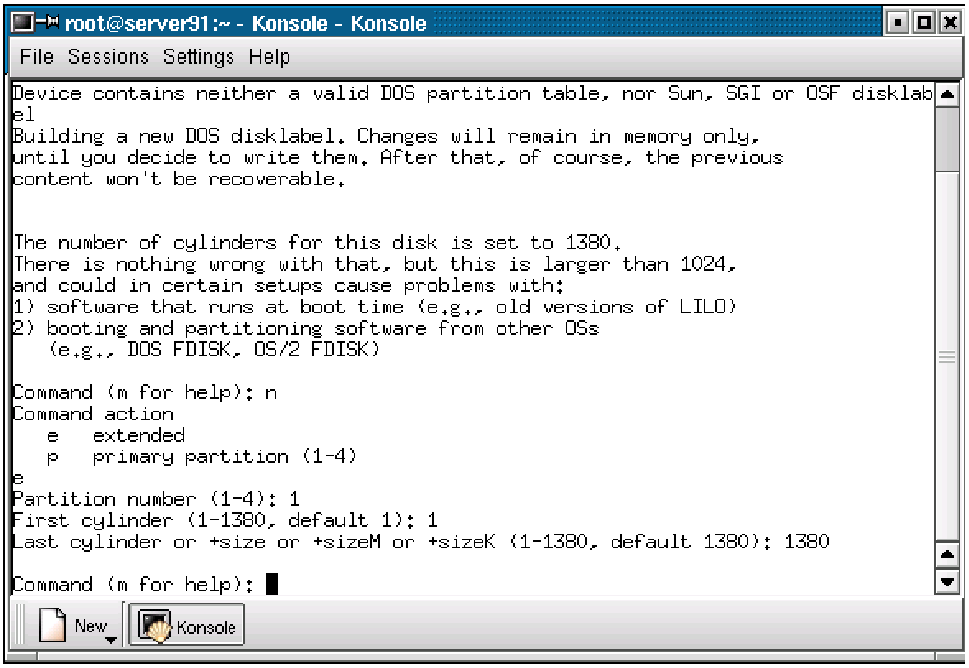
Complete the following steps to configure the raw devices and to create the extended partition and logical drives necessary for shared storage.

1. Ensure that you are logged in the operating system as the root user. Run the `fdisk /dev/sda` command.


root@server91:~ - Konsole - Konsole
File Sessions Settings Help
New
Konsole

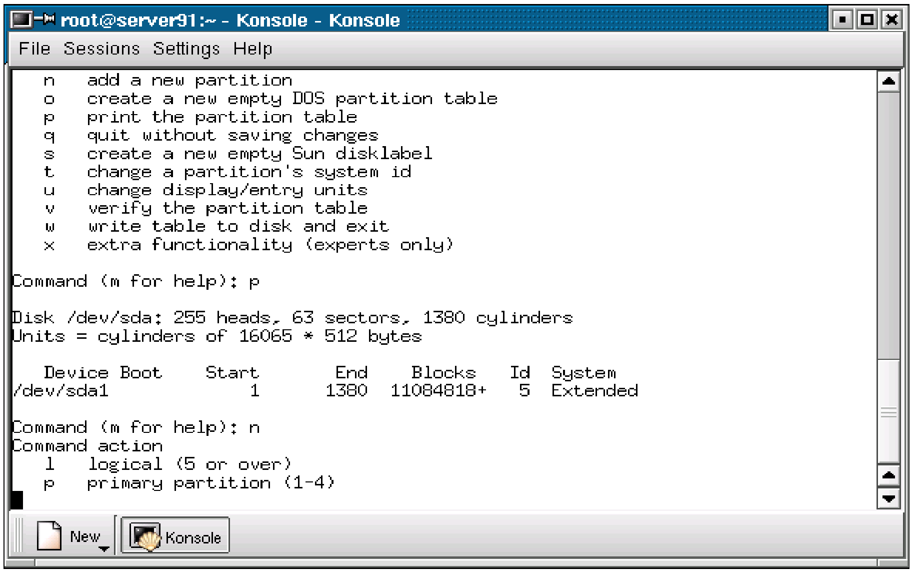
```
[root@server91 root]# fdisk /dev/sda
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklab
el
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previous
content won't be recoverable.


The number of cylinders for this disk is set to 1380.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): 
```

2. To create the extended partition, enter *n* and press *Enter*.
3. Enter *e* and press *Enter.*
4. Enter *1* for the partition number. Enter *1* for the first cylinder. Accept the default for the last cylinder and press *Enter*.


root@server91:~ - Konsole - Konsole
File Sessions Settings Help
New
Konsole

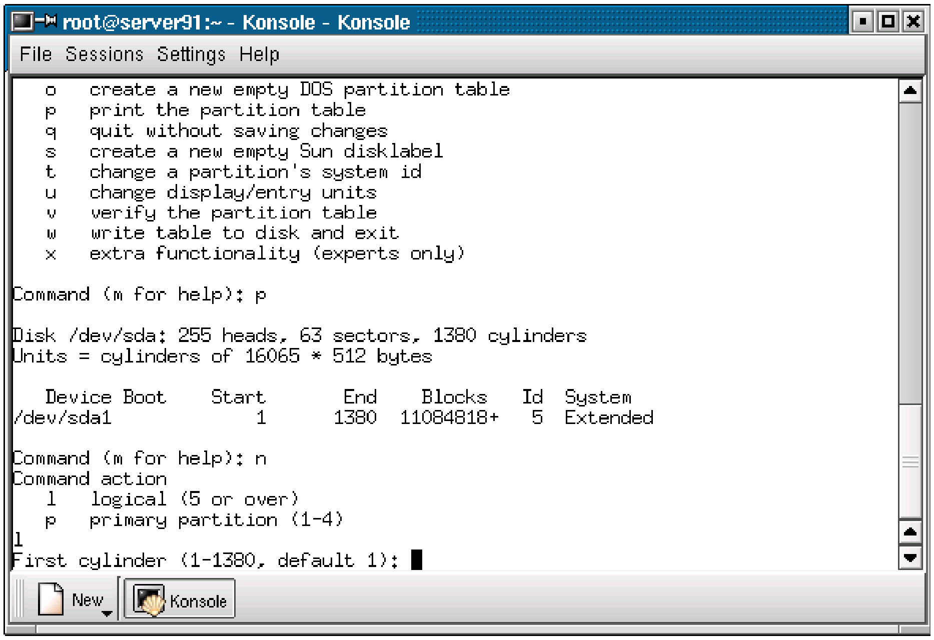
```
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklab
el
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previous
content won't be recoverable.


The number of cylinders for this disk is set to 1380.
There is nothing wrong with that, but this is larger than 1024,
and could in certain setups cause problems with:
1) software that runs at boot time (e.g., old versions of LILO)
2) booting and partitioning software from other OSs
   (e.g., DOS FDISK, OS/2 FDISK)

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
e
Partition number (1-4): 1
First cylinder (1-1380, default 1): 1
Last cylinder or +size or +sizeM or +sizeK (1-1380, default 1380): 1380

Command (m for help): 
```

5. To create the logical drives for the shared storage, enter *n* and press *Enter*.


root@server91:~ - Konsole - Konsole
File Sessions Settings Help
New
Konsole

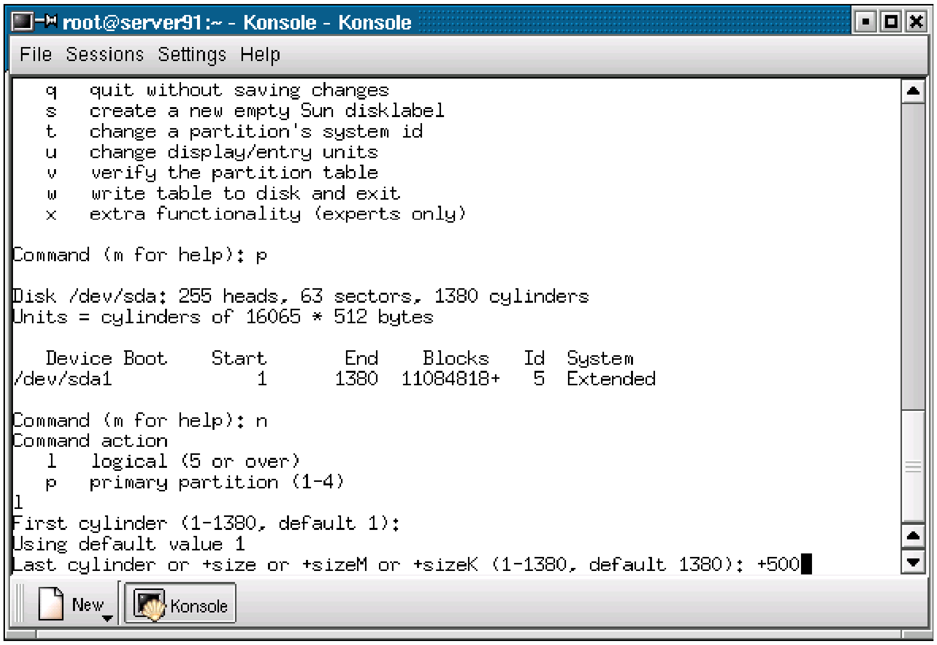
```
    n   add a new partition
    o   create a new empty DOS partition table
    p   print the partition table
    q   quit without saving changes
    s   create a new empty Sun disklabel
    t   change a partition's system id
    u   change display/entry units
    v   verify the partition table
    w   write table to disk and exit
    x   extra functionality (experts only)

Command (m for help): p

Disk /dev/sda: 255 heads, 63 sectors, 1380 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/sda1             1      1380  11084818+   5  Extended

Command (m for help): n
Command action
   l   logical (5 or over)
   p   primary partition (1-4)
```

6. Enter *l* for a logical drive.


root@server91:~ - Konsole - Konsole
File Sessions Settings Help
New
Konsole

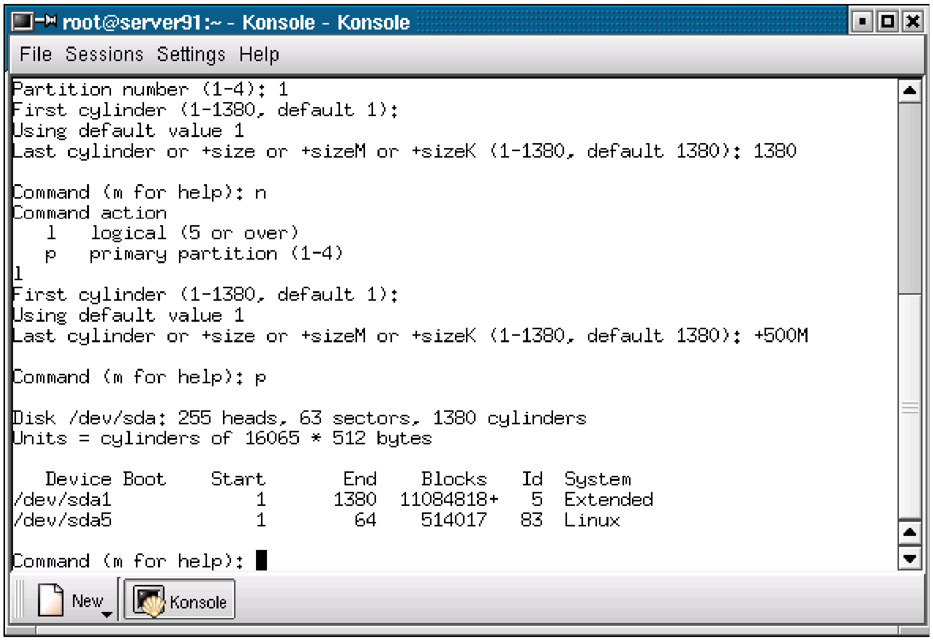
```
    o   create a new empty DOS partition table
    p   print the partition table
    q   quit without saving changes
    s   create a new empty Sun disklabel
    t   change a partition's system id
    u   change display/entry units
    v   verify the partition table
    w   write table to disk and exit
    x   extra functionality (experts only)

Command (m for help): p

Disk /dev/sda: 255 heads, 63 sectors, 1380 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/sda1             1      1380  11084818+   5  Extended

Command (m for help): n
Command action
   l   logical (5 or over)
   p   primary partition (1-4)
l
First cylinder (1-1380, default 1):
```

7. Accept the default for the first cylinder and press *Enter*.


root@server91:~ - Konsole - Konsole
File Sessions Settings Help
New
Konsole

```
   q   quit without saving changes
   s   create a new empty Sun disklabel
   t   change a partition's system id
   u   change display/entry units
   v   verify the partition table
   w   write table to disk and exit
   x   extra functionality (experts only)

Command (m for help): p

Disk /dev/sda: 255 heads, 63 sectors, 1380 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/sda1             1      1380  11084818+   5  Extended

Command (m for help): n
Command action
   l   logical (5 or over)
   p   primary partition (1-4)
l
First cylinder (1-1380, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-1380, default 1380): +500
```

8. Enter *+500M* and press *Enter* to create a 500MB partition. At the command prompt, enter *p* and press *Enter*.


root@server91:~ - Konsole - Konsole
File Sessions Settings Help
New
Konsole

```
Partition number (1-4): 1
First cylinder (1-1380, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-1380, default 1380): 1380

Command (m for help): n
Command action
   l   logical (5 or over)
   p   primary partition (1-4)
l
First cylinder (1-1380, default 1):
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-1380, default 1380): +500M

Command (m for help): p

Disk /dev/sda: 255 heads, 63 sectors, 1380 cylinders
Units = cylinders of 16065 * 512 bytes

   Device Boot    Start       End    Blocks   Id  System
/dev/sda1             1      1380  11084818+   5  Extended
/dev/sda5             1        64    514017   83  Linux

Command (m for help): 
```

Note

Actual block size can vary from system to system. Use the screen shots in this exercise as guideline only.

9. Enter *w* at the command prompt to write the partition table and quit fdisk.
10. At the Linux prompt, enter *mke2fs –j /dev/sda1* to format the newly created logical drive. Repeat this step for all the logical drives you created.
11. Create a new mounting point for the MSA1000 storage by entering: *mkdir /msa1000*
12. Mount the logical drive to /msa1000 by entering: *mount /dev/sda1 /msa1000*

> **Note**
>
> Mounting a drive with the *mount* command makes the storage available for this session only. After a reboot, you must mount the drive again to use it. To make a mount persistent, you must edit the */etc/fstab* file. For more information, you can enter *man fstab* at the Linux console.

13. You can test this new storage by writing a file to the MSA 1000 and then reading it. Enter: *cat /proc/cpuinfo > /msa1000/test*
14. To read the file, enter: *cat /msa1000/test*
15. The new storage should also be viewable in the output of the Linux command *df*. Enter *df* at the command line to view all of the available mounted storage. If the storage has been properly mounted, there will be a line that begins with */dev/sda1* and shows the:
    - Total amount of storage available
    - Amount used
    - Amount remaining
    - Percentage remaining
    - Mount point

    In this case, the line should end with: */msa1000*
16. When you are ready, shut down the Linux server by entering (as the *root* user) *shutdown –h now*

Exercise 9 — Booting from the SAN (MSA1000)

Before beginning the MSA1000 configuration, ensure the following:

- Firmware upgrades should be performed from a DOS boot to avoid loss of connectivity to the MSA1000.
- Secure Path is not supported when the operating system is installed on the MSA1000.
- You must copy the FCA2214 driver files from the HP StorageWorks MSA 1000 Support Software CD to a diskette for part of the operating system installation.
- Do not perform any configuration on internal drives until the installation of the operating system has been completed on the MSA1000. Upon system reboot, execute the Online RAID Configuration Utility and enable the internal drives.
- The pagefile for the operating system should be installed to an internal drive per Microsoft recommendation.
- You must use Selective Storage Presentation (SSP) if multiple servers are to contain volumes on the same MSA1000.
- Do not use SmartStart to install the operating system on the server.

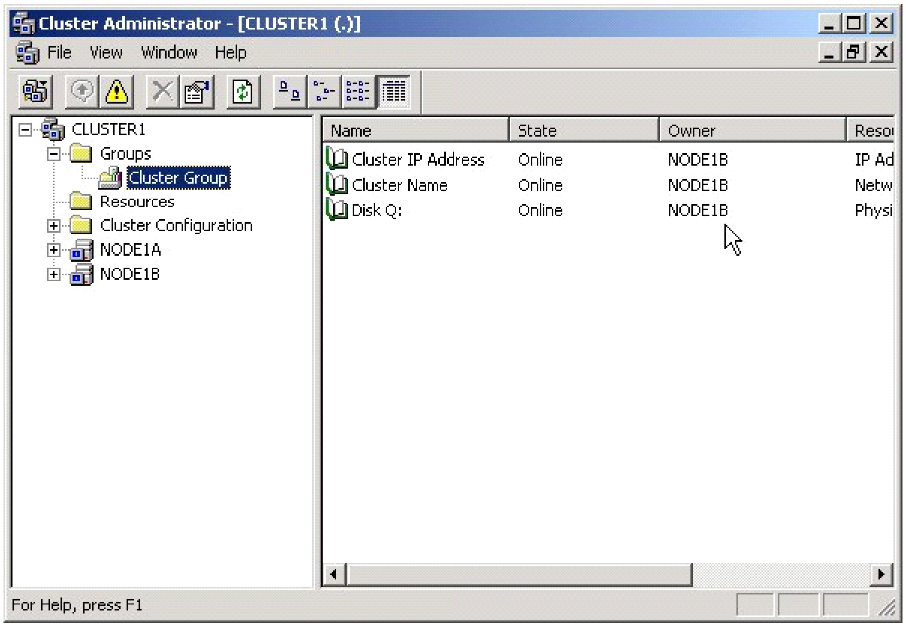
Removing node A from the cluster

To prepare the physical server to boot from the MSA1000, follow these steps:

1. Start Cluster Administrator by running *CluAdmin.exe*.
2. Right-click the node and then click *Stop the Cluster service*.

> **! Important**
> Do not perform this step if this server is the last node in the cluster. For more information, see Microsoft Knowledge Base Article 282227.

3. Right-click the node and then click *Evict Node*.



Name	State	Owner	Resoı
Cluster IP Address	Online	NODE1B	IP Ad
Cluster Name	Online	NODE1B	Netw
Disk Q:	Online	NODE1B	Physi

> **Note**
> If you cannot start the Cluster service or if you have trouble removing the node, you can manually unconfigure the Cluster service:

4. Run the *Cmd.exe* program to open a command prompt.
5. At the command prompt, enter *cluster node node1a /forcecleanup*, and then press E*nter*.

Configuring physical disks for external boot

To prepare the physical server to boot from the MSA1000, follow these steps:

1. Shut down the node A server.
2. From the MSA1000, remove all of the drives and set them aside.
3. From the server, remove the drives that contain the array with the server operating system.
4. Place the drives from the server into the MSA1000. The order that they are replaced in the MSA1000 is no longer important. The array controller will recognize the drives from the foreign array and make them available.

Configuring the server BIOS

To redirect the server BIOS to boot from the HBA port, follow these steps:

1. When the system is booting, press *F9* to start the ROM Setup Utility.
2. Choose *Boot Controller Order*.
3. Select the primary HBA and move it to Controller Order 1.
4. Exit the utility.

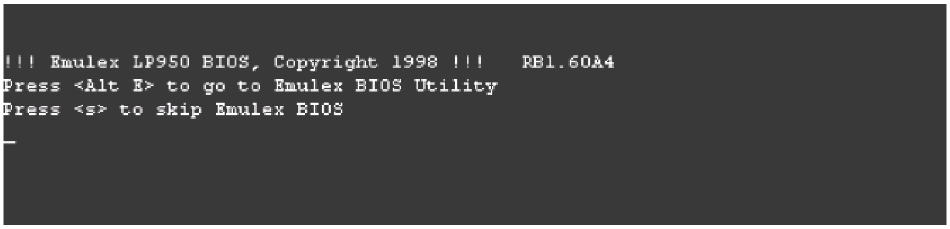
Configuring the HBA for boot

Configuring the server for Qlogic Fibre Channel HBA boot

1. During the boot process, a Qlogic HBA message displays. At the prompt to enter Fast!util, press *ctrl+Q*.
2. In the Select Host Adapter Menu, choose the adapter you want to boot; then press *Enter*.
3. In the Fast!Util Options Menu, choose *Configuration Settings*; then press *Enter*.
4. In the Configuration Settings menu, choose *Host Adapter Settings*; then press *Enter*.
5. In the Host Adapter Settings menu, change the Host Adapter BIOS to *Enabled* by pressing *Enter*.
6. In the Selectable Boot Settings menu, enable the *Selectable Boot* option; then move the cursor to the Primary Boot Port Name, LUN. Press *Enter*.
7. In the Select Fibre Channel Device menu, choose the device to boot from; then press *Enter*.
8. In the Select LUN menu, choose the supported LUN. Save the changes by pressing *Esc* twice.
9. Exit Fast!Util.

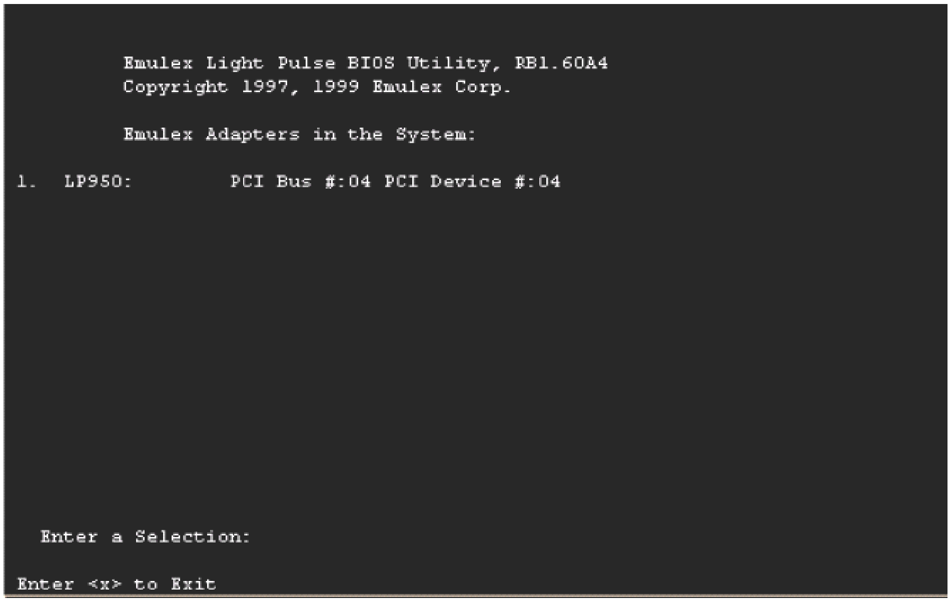
Configuring the boot BIOS with the Emulex BIOS utility

1. When the server boots, the menu for the HBA displays. Press *Alt+E* to start the Emulex BIOS Utility.



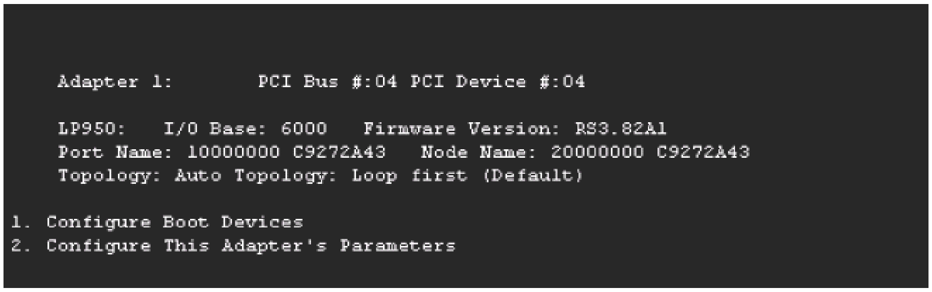
```
!!! Emulex LP950 BIOS, Copyright 1998 !!!   RB1.60A4
Press <Alt E> to go to Emulex BIOS Utility
Press <s> to skip Emulex BIOS
_
```

2. You are presented with a list of HBAs in the server. Press *1 → Enter* to select the displayed HBA.



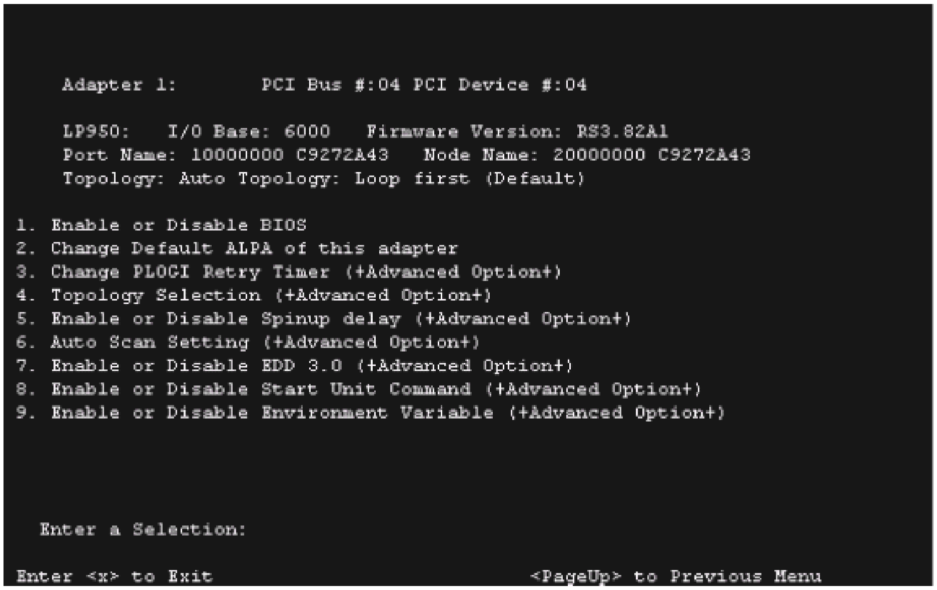
```
         Emulex Light Pulse BIOS Utility, RB1.60A4
         Copyright 1997, 1999 Emulex Corp.

         Emulex Adapters in the System:

 1.  LP950:        PCI Bus #:04 PCI Device #:04




   Enter a Selection:

 Enter <x> to Exit
```

3. You are presented with two selections. Note the options at the bottom of the screen to navigate through the menus. Press *2 → Enter* to select *Configure This Adapter's Parameters*.



```
    Adapter 1:       PCI Bus #:04 PCI Device #:04

    LP950:   I/O Base: 6000   Firmware Version: RS3.82A1
    Port Name: 10000000 C9272A43   Node Name: 20000000 C9272A43
    Topology: Auto Topology: Loop first (Default)

1. Configure Boot Devices
2. Configure This Adapter's Parameters
```

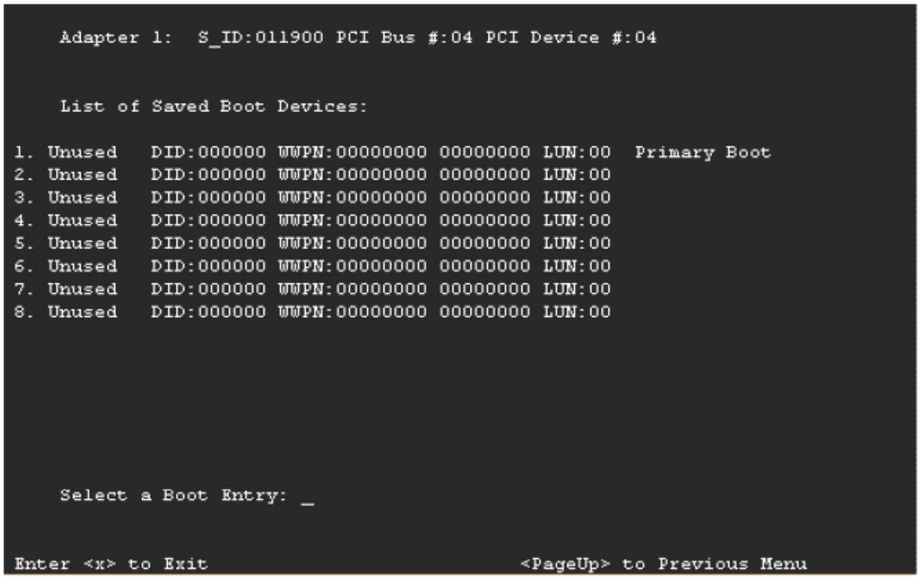
4. You are presented with several options. Press *1 → Enter* to enable or disable the BIOS.



```
    Adapter 1:       PCI Bus #:04 PCI Device #:04

    LP950:   I/O Base: 6000   Firmware Version: RS3.82A1
    Port Name: 10000000 C9272A43   Node Name: 20000000 C9272A43
    Topology: Auto Topology: Loop first (Default)

1. Enable or Disable BIOS
2. Change Default ALPA of this adapter
3. Change PLOGI Retry Timer (+Advanced Option+)
4. Topology Selection (+Advanced Option+)
5. Enable or Disable Spinup delay (+Advanced Option+)
6. Auto Scan Setting (+Advanced Option+)
7. Enable or Disable EDD 3.0 (+Advanced Option+)
8. Enable or Disable Start Unit Command (+Advanced Option+)
9. Enable or Disable Environment Variable (+Advanced Option+)



  Enter a Selection:

Enter <x> to Exit                            <PageUp> to Previous Menu
```

5. Press *1 → Enter* to enable the BIOS.
6. Press *PageUp* to return to the previous menu.
7. Press *PageUp* again to return to the first menu.
8. Press *1 → Enter* to configure boot devices.

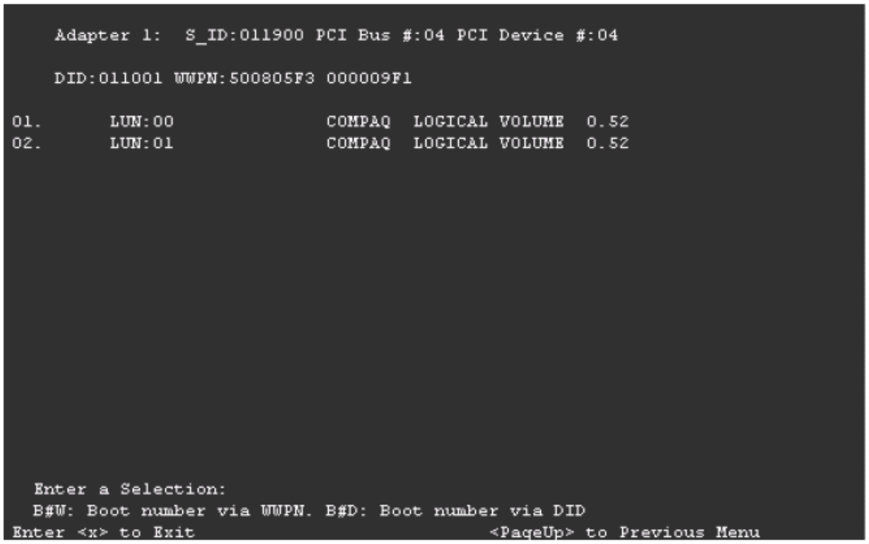
9. You are presented with several options. Press *1 → Enter* to enable the BIOS.
10. Press *1 → Enter* to select *Primary Boot*.



```
    Adapter 1:  S_ID:011900 PCI Bus #:04 PCI Device #:04


    List of Saved Boot Devices:

1. Unused   DID:000000 WWPN:00000000 00000000 LUN:00  Primary Boot
2. Unused   DID:000000 WWPN:00000000 00000000 LUN:00
3. Unused   DID:000000 WWPN:00000000 00000000 LUN:00
4. Unused   DID:000000 WWPN:00000000 00000000 LUN:00
5. Unused   DID:000000 WWPN:00000000 00000000 LUN:00
6. Unused   DID:000000 WWPN:00000000 00000000 LUN:00
7. Unused   DID:000000 WWPN:00000000 00000000 LUN:00
8. Unused   DID:000000 WWPN:00000000 00000000 LUN:00






    Select a Boot Entry: _

Enter <x> to Exit                          <PageUp> to Previous Menu
```

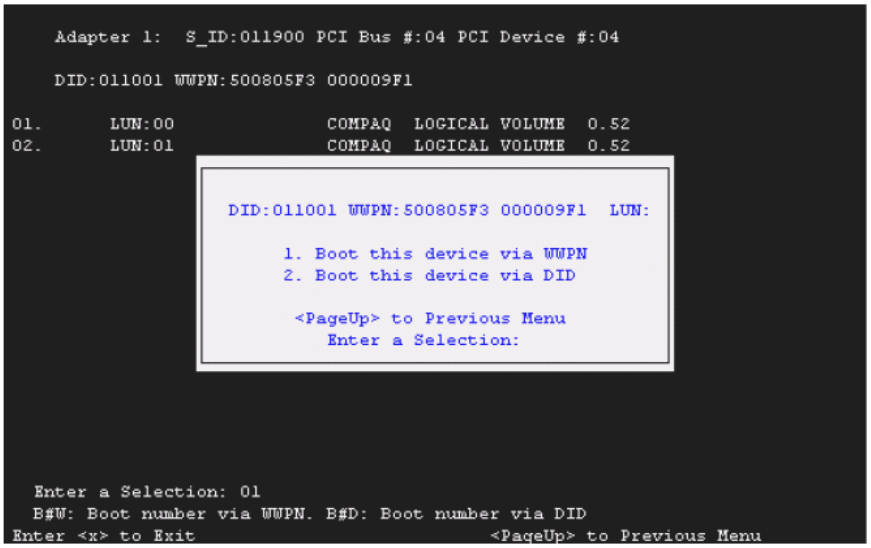
11. Press *01 → Enter* to select the entry with the LUN that is presented by the MSA1000 controller.
12. You are prompted to enter a two-digit LUN number. Enter *00 → Enter*.

13. You are presented with a list of available LUNs visible to the HBA. Press *01* → *Enter* to select the first LUN (logical drive 01 LUN 00) on the MSA1000.



```
    Adapter 1:  S_ID:011900 PCI Bus #:04 PCI Device #:04

    DID:011001 WWPN:500805F3 000009F1

01.       LUN:00              COMPAQ  LOGICAL VOLUME  0.52
02.       LUN:01              COMPAQ  LOGICAL VOLUME  0.52














  Enter a Selection:
  B#W: Boot number via WWPN. B#D: Boot number via DID
Enter <x> to Exit                            <PageUp> to Previous Menu
```

14. You are prompted to select how to boot the device. Press *1* → *Enter*.



```
    Adapter 1:  S_ID:011900 PCI Bus #:04 PCI Device #:04

    DID:011001 WWPN:500805F3 000009F1

01.       LUN:00              COMPAQ  LOGICAL VOLUME  0.52
02.       LUN:01              COMPAQ  LOGICAL VOLUME  0.52

                  DID:011001 WWPN:500805F3 000009F1  LUN:

                       1. Boot this device via WWPN
                       2. Boot this device via DID

                        <PageUp> to Previous Menu
                           Enter a Selection:






  Enter a Selection: 01
  B#W: Boot number via WWPN. B#D: Boot number via DID
Enter <x> to Exit                            <PageUp> to Previous Menu
```

15. You are returned to the list of saved boot devices. Press *x* → *y* to exit the menu and reboot the server. The server will now boot from the external storage.

Business continuity planning and disaster recovery

Lab 6

Objectives

After completing this lab, you should be able to:

- Follow best practices for thermal management in a datacenter
- Perform a backup needs analysis
- Use the HP Enterprise Backup Sizer Tool to design an Enterprise Backup Solution (EBS)

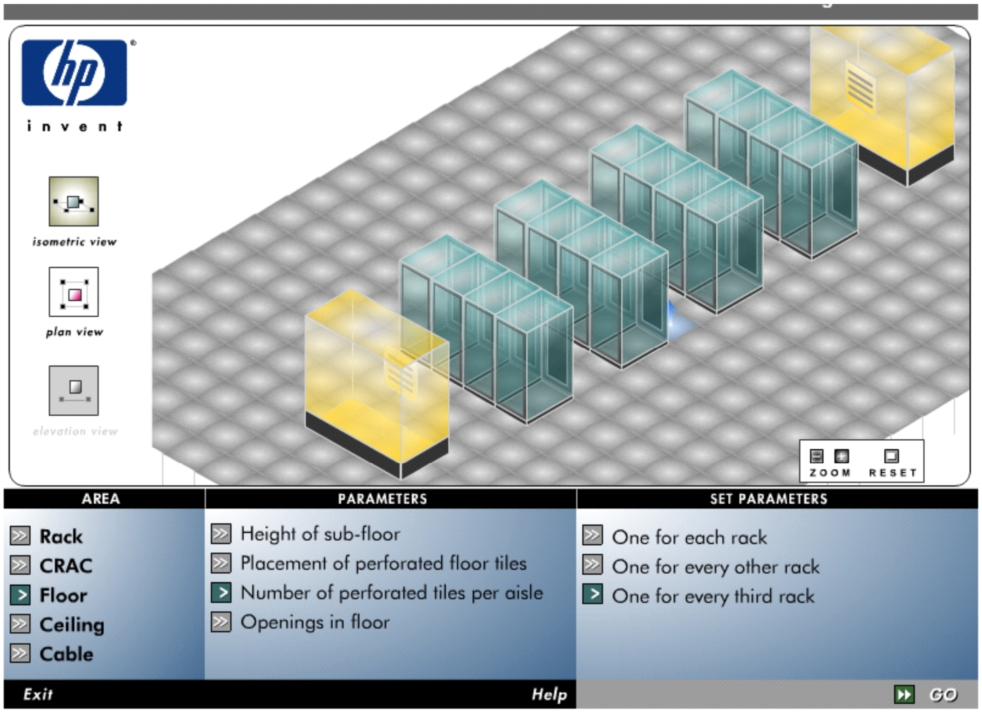
Introduction

RC Engineering has four racks in a datacenter that are populated with servers and storage. Recently, the RC Engineers have had problems with servers shutting down unexpectedly.

The company has hired you to determine the cause of the unplanned server shutdowns and resolve the problem. You suspect the problem could be that the servers are overheating. Your job is to analyze the current environment in the datacenter, change any parameters that you think might be causing the problem, and then see if the problem is resolved.

Hurricane Brent devastated RC Engineering's Seahaven office and taught them the costs associated with not having comprehensive backups. Seeking to correct from this disaster, the company has also asked you to perform a needs analysis to determine the type of backup strategy that best meets their requirements. Finally, you will implement the new backup strategy using Enterprise Backup Solution.

Exercise 1 — Thermal management in the datacenter



This exercise is software based and will be led by our instructor. Using the software provided, you can change parameters at the bottom of the screen. First, select an area of the datacenter on the left. Next, select a parameter in the middle. Finally, change the parameter on the right.

You can see how your changes affect the datacenter at the top of the screen. Choose one of three views at the top left.

When you are ready to see if your changes have resolved the problem, click the *Go* button in the bottom right corner.

Exercise 2 — Performing a backup needs analysis

In this exercise you will perform a backup needs analysis for three RC Engineering servers. Use the charts on the next page to document what you learn. Feel free to invent any information that is not included in the description.

Description

The IT staff at RC Engineering has asked you to determine the type of backup strategy that best suits three of their most-used servers:

- Server 1 is the RC Engineering FTP server. It an HP ProLiant DL380 G3 running Microsoft Windows 2000 Advanced Server. It has a Smart Array 6402 controller and a 64-bit PCI-to-Fibre Channel host bus adapter (HBA). It has two 500GB volumes in the server used as images.

  Company engineers use this server to share large CAD drawing files when they are collaborating on a project. Because the FTP site is accessed by employees from around the world, it must be available 24 x 7. The files stored on this server are not mission-critical, because the engineers always keep a local backup copy of their drawings.

  RC Engineering does not expect this data to grow in volume. Presently, the IT staff performs partial backups on this server once a week.

- Server 2 is a ProLiant ML570 running Novell NetWare 5.1. It has an embedded Smart Array 5i Plus controller and one 500GB volume with no RAID protection. It is used mainly as a file and print server to store administrative spreadsheets and word processing documents. It resides on the company LAN, which has a 100Base-T network connection.

  RC Engineering expects the data on this server to grow 10% over the next year. The IT staff performs incremental backups on it every day.

- Server 3 is a ProLiant BL20p G2 with an HP StorageWorks 2GB PCI-X to FC adapter. It has two 500GB volumes in shared storage used for Oracle9*i* databases. Because these databases contain the results of RC Engineering's genetic engineering research and must be highly available, this server is part of a Fibre Channel cluster.

  The company expects the data to grow 20% over the next year. The IT staff performs full backups on it every night.

Analysis

Answer the following questions to determine the best way to back up the RC Engineering data.

	Server 1	Server 2	Server 3
What operating system is running on each server?			
What type of HBA is being used?			
Which disk controller is being used?			
Is the server part of a cluster?			
Is the data business-critical?			
How much data will need to be backed-up?			

How fast is the LAN?..

....

How much will you be available to spend? ....

....

How reliable do the tapes and devices need to be? ....

....

	Vol 1	Vol 2	Vol 3	Vol 4	Vol 5
What is the feed speed of the hard drive system?					
What is the data compression ratio for the volume?					
How large are the files?					
What is the expected data growth rate? (Consider the present data)					
How much data does each volume hold?					
What percent growth do you expect in a year?					
What types of backups will you want?					
How many backup sets will you keep?					
How large must the backup window be?					
When will backups be done?					
What is the tape retention schedule?					
Where will partial backups be retained?					
Will partial backups will be differential or incremental?					
Can the volume to be backed up be taken offline?					
Which backup job will this data be in?					

Exercise 3 — Designing an Enterprise Backup Solution

Use your documented needs analysis and the HP Backup Solution Sizer to determine what you need to back up RC Engineering.

1. What type of drives does the sizer suggest is the best solution?

   ....

   ....

2. How many drives does it suggest RC Engineering purchase?

   ....

   ....

3. How many tapes does it suggest RC Engineering purchase?

   ....

   ....

4. What additional products does the sizer suggest RC Engineering purchase?

   ....

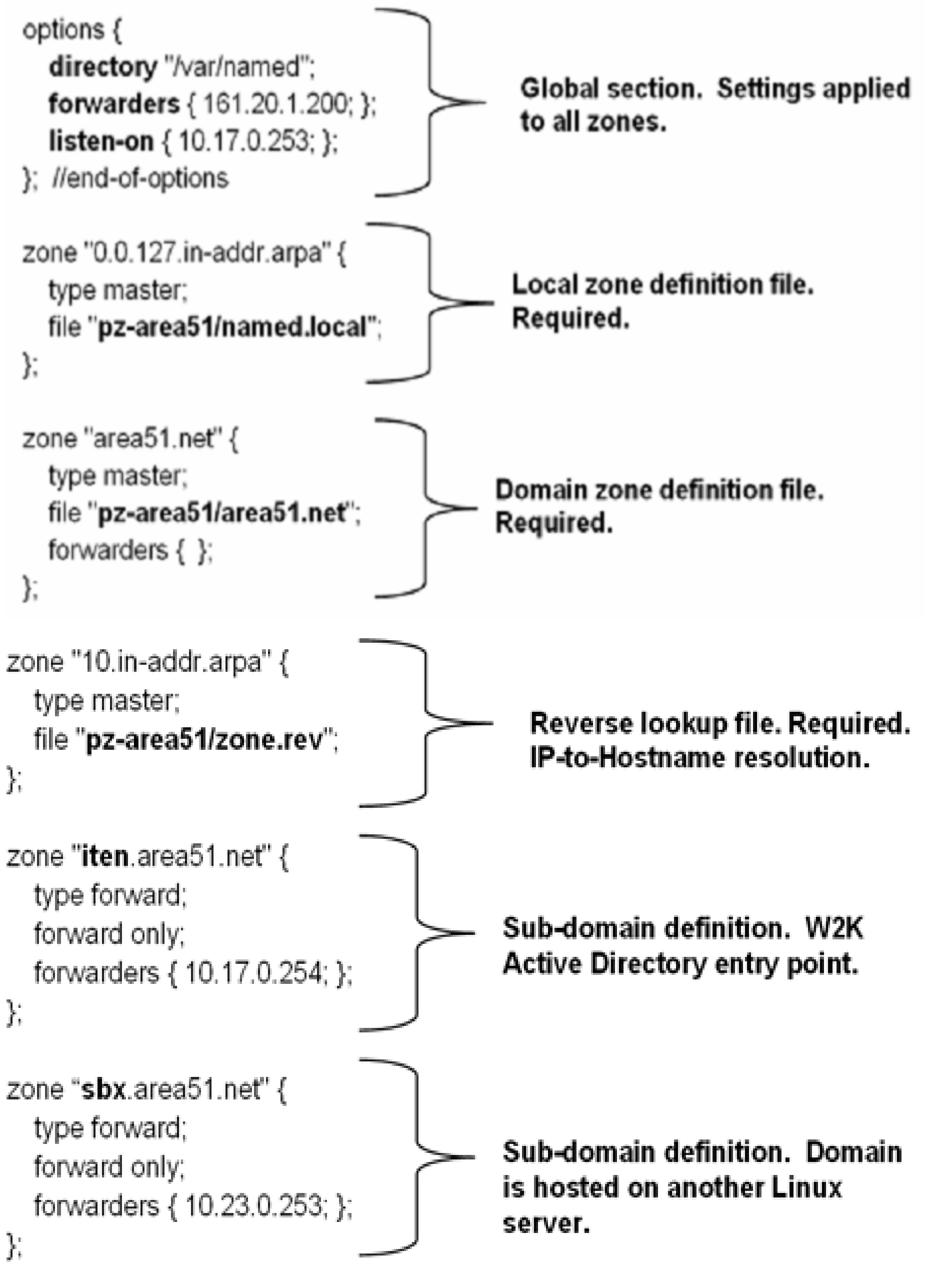
Linux DNS configuration

Appendix A

Linux DNS files

Several important Linux DNS files must be defined using the following text.

/etc/named.conf



```
options {
   directory "/var/named";
   forwarders { 161.20.1.200; };
   listen-on { 10.17.0.253; };
}; //end-of-options
```

Global section. Settings applied to all zones.

```
zone "0.0.127.in-addr.arpa" {
   type master;
   file "pz-area51/named.local";
};
```

Local zone definition file. Required.

```
zone "area51.net" {
   type master;
   file "pz-area51/area51.net";
   forwarders { };
};
```

Domain zone definition file. Required.

```
zone "10.in-addr.arpa" {
   type master;
   file "pz-area51/zone.rev";
};
```

Reverse lookup file. Required. IP-to-Hostname resolution.

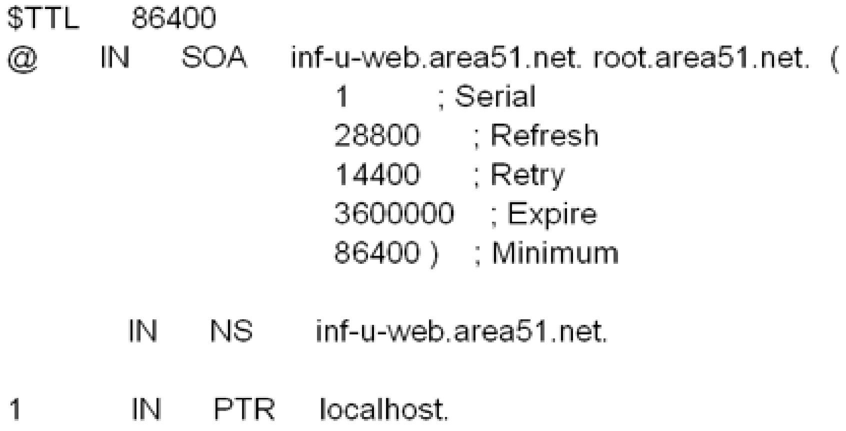
```
zone "iten.area51.net" {
   type forward;
   forward only;
   forwarders { 10.17.0.254; };
};
```

Sub-domain definition. W2K Active Directory entry point.

```
zone “sbx.area51.net" {
   type forward;
   forward only;
   forwarders { 10.23.0.253; };
};
```

Sub-domain definition. Domain is hosted on another Linux server.

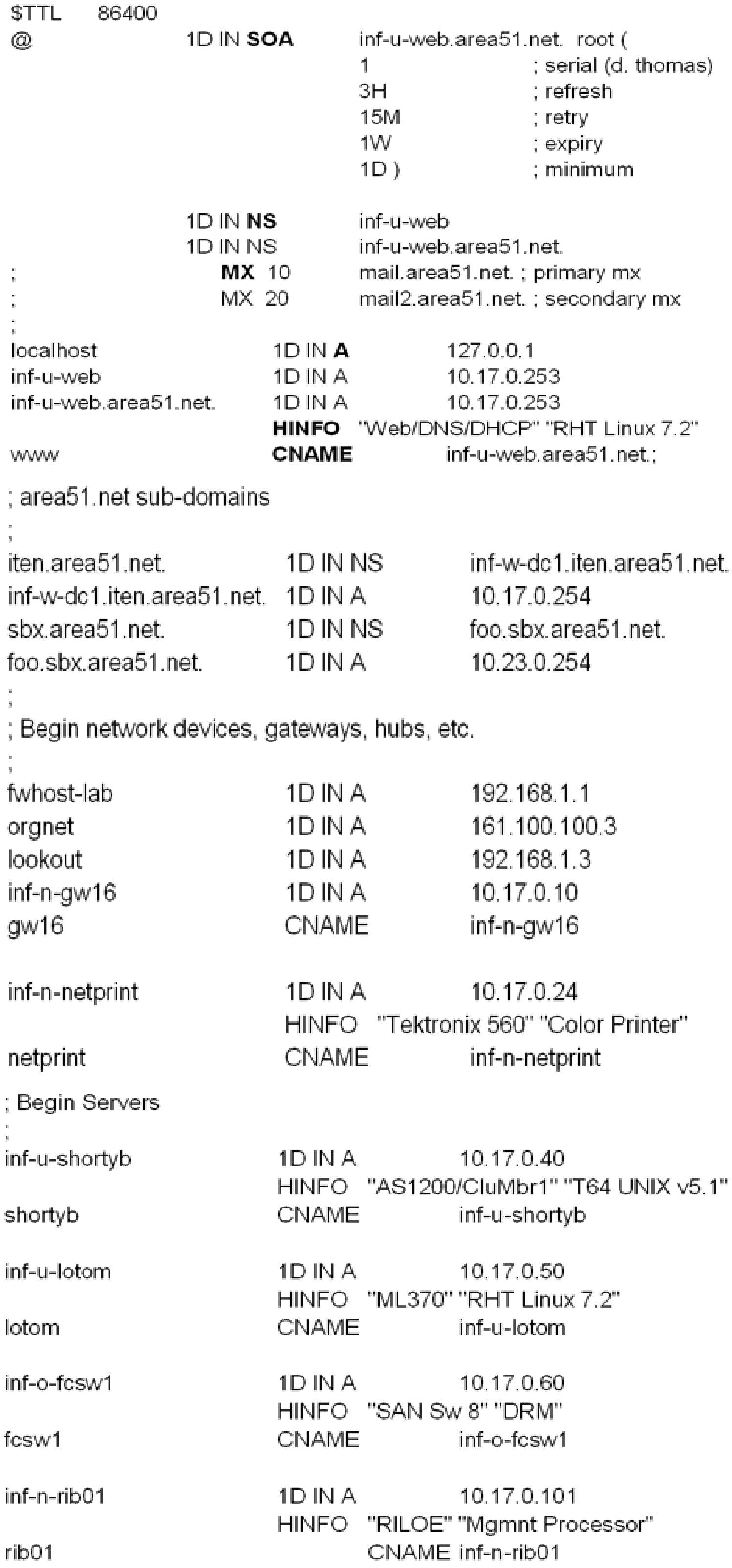
named.local



```
$TTL    86400
@       IN      SOA     inf-u-web.area51.net. root.area51.net.  (
                              1          ; Serial
                              28800      ; Refresh
                              14400      ; Retry
                              3600000    ; Expire
                              86400 )    ; Minimum

                IN      NS      inf-u-web.area51.net.

1               IN      PTR     localhost.
```

The preceding graphic is an example of the zone definition of area51.net.

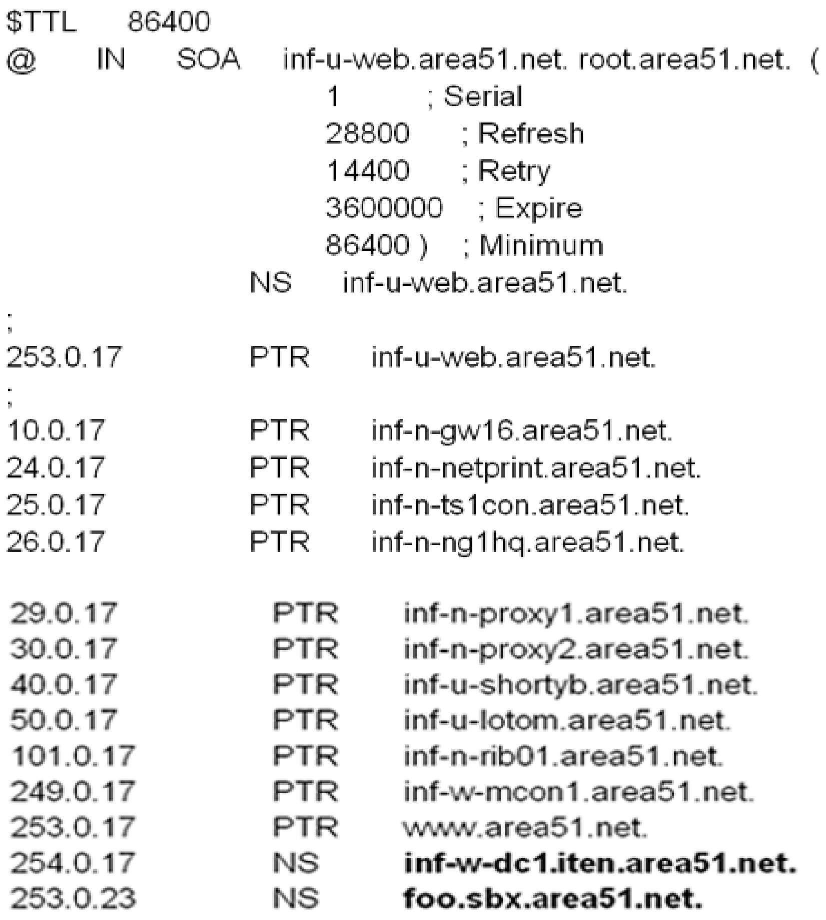
area51.net



```
$TTL    86400
@               1D IN SOA       inf-u-web.area51.net.  root (
                                1               ; serial (d. thomas)
                                3H              ; refresh
                                15M             ; retry
                                1W              ; expiry
                                1D )            ; minimum

                1D IN NS        inf-u-web
                1D IN NS        inf-u-web.area51.net.
;                  MX  10       mail.area51.net. ; primary mx
;                  MX  20       mail2.area51.net. ; secondary mx
;
localhost               1D IN A         127.0.0.1
inf-u-web               1D IN A         10.17.0.253
inf-u-web.area51.net.   1D IN A         10.17.0.253
                        HINFO  "Web/DNS/DHCP" "RHT Linux 7.2"
www                     CNAME           inf-u-web.area51.net.;

; area51.net sub-domains
;
iten.area51.net.                1D IN NS        inf-w-dc1.iten.area51.net.
inf-w-dc1.iten.area51.net.      1D IN A         10.17.0.254
sbx.area51.net.                 1D IN NS        foo.sbx.area51.net.
foo.sbx.area51.net.             1D IN A         10.23.0.254
;
; Begin network devices, gateways, hubs, etc.
;
fwhost-lab              1D IN A         192.168.1.1
orgnet                  1D IN A         161.100.100.3
lookout                 1D IN A         192.168.1.3
inf-n-gw16              1D IN A         10.17.0.10
gw16                    CNAME           inf-n-gw16

inf-n-netprint          1D IN A         10.17.0.24
                        HINFO  "Tektronix 560" "Color Printer"
netprint                CNAME           inf-n-netprint
; Begin Servers
;
inf-u-shortyb           1D IN A         10.17.0.40
                        HINFO  "AS1200/CluMbr1" "T64 UNIX v5.1"
shortyb                 CNAME           inf-u-shortyb

inf-u-lotom             1D IN A         10.17.0.50
                        HINFO  "ML370" "RHT Linux 7.2"
lotom                   CNAME           inf-u-lotom

inf-o-fcsw1             1D IN A         10.17.0.60
                        HINFO  "SAN Sw 8" "DRM"
fcsw1                   CNAME           inf-o-fcsw1

inf-n-rib01             1D IN A         10.17.0.101
                        HINFO  "RILOE" "Mgmnt Processor"
rib01                          CNAME inf-n-rib01
```

The preceding is an example of the forward zone file for area51.net.

zone.rev

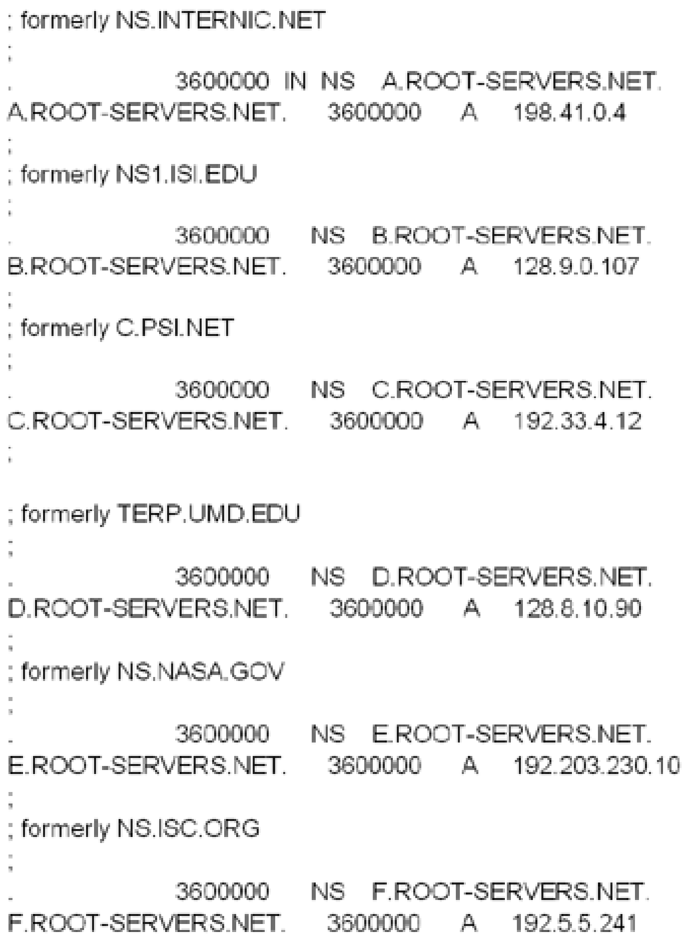


```
$TTL     86400
@        IN     SOA     inf-u-web.area51.net. root.area51.net.  (
                              1          ; Serial
                              28800      ; Refresh
                              14400      ; Retry
                              3600000    ; Expire
                              86400 )    ; Minimum
                        NS      inf-u-web.area51.net.
;
253.0.17                PTR      inf-u-web.area51.net.
;
10.0.17                 PTR      inf-n-gw16.area51.net.
24.0.17                 PTR      inf-n-netprint.area51.net.
25.0.17                 PTR      inf-n-ts1con.area51.net.
26.0.17                 PTR      inf-n-ng1hq.area51.net.

29.0.17                 PTR      inf-n-proxy1.area51.net.
30.0.17                 PTR      inf-n-proxy2.area51.net.
40.0.17                 PTR      inf-u-shortyb.area51.net.
50.0.17                 PTR      inf-u-lotom.area51.net.
101.0.17                PTR      inf-n-rib01.area51.net.
249.0.17                PTR      inf-w-mcon1.area51.net.
253.0.17                PTR      www.area51.net.
254.0.17                NS       inf-w-dc1.iten.area51.net.
253.0.23                NS       foo.sbx.area51.net.
```

The preceding is an example of the reverse lookup zone file.

The last two items are important because they are the reverse lookup for subdomains `iten` and `sbx`. SOA= Start of Authority; PTR = Pointer; NS = NameServer

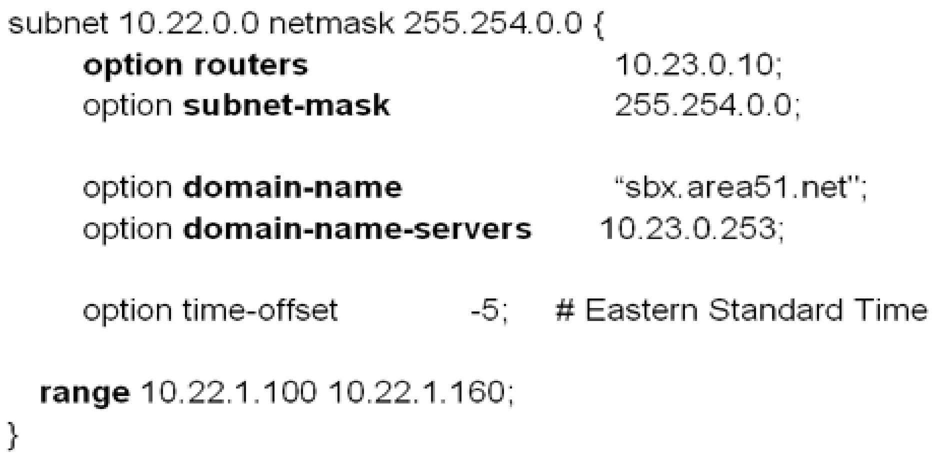
named.ca



```
; formerly NS.INTERNIC.NET
;
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     128.9.0.107
;
; formerly C.PSI.NET
;
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
;

; formerly TERP.UMD.EDU
;
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     128.8.10.90
;
; formerly NS.NASA.GOV
;
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
;
; formerly NS.ISC.ORG
;
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
```

The preceding graphic is a sample of the named.ca file.

/etc/dhcpd.conf



```
subnet 10.22.0.0 netmask 255.254.0.0 {
      option routers                          10.23.0.10;
      option subnet-mask                      255.254.0.0;

      option domain-name                      “sbx.area51.net”;
      option domain-name-servers             10.23.0.253;

      option time-offset            -5;    # Eastern Standard Time

   range 10.22.1.100 10.22.1.160;
}
```

The preceding graphic is a sample of what the dhcpd.conf file should look like:

Stress tools

Appendix B

Introduction

This appendix contains a list of tools that can be used to generate a workload on a target server and stress a desired subsystem.

CPU Stress

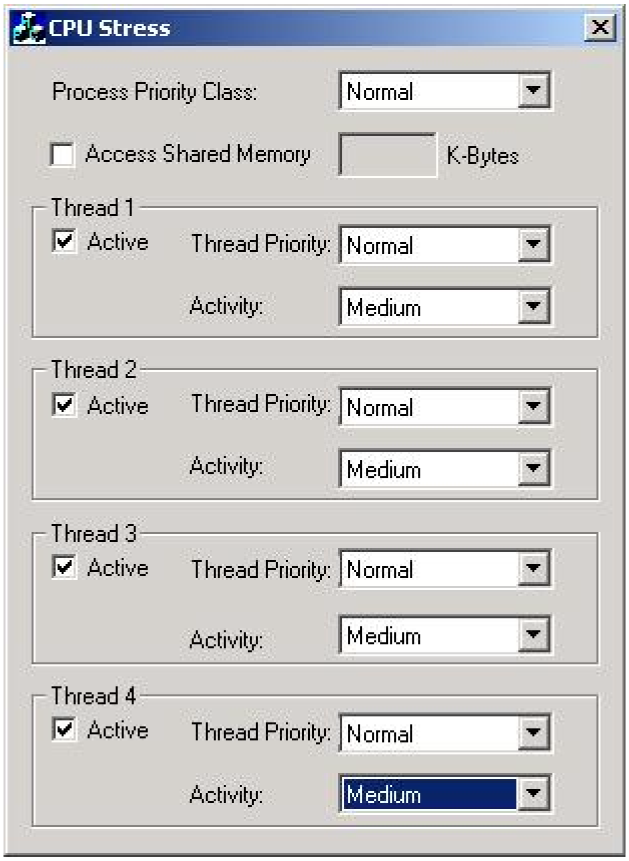
The CPU Stress utility places a variable load on the system processors. You can control the process priority class, number of active threads, thread priority, and the level of thread activity.

At the target server, perform the following steps to induce processor load:

1. Execute `cpustres.exe` to launch the utility.
2. At the CPU Stress screen, change the available options to vary the workload. Your changes become effective immediately.

   Example

   To create a moderate workload, modify the options as shown in the following graphic.



Process Priority Class: Normal

☐ Access Shared Memory K-Bytes

Thread 1
☑ Active Thread Priority: Normal
Activity: Medium

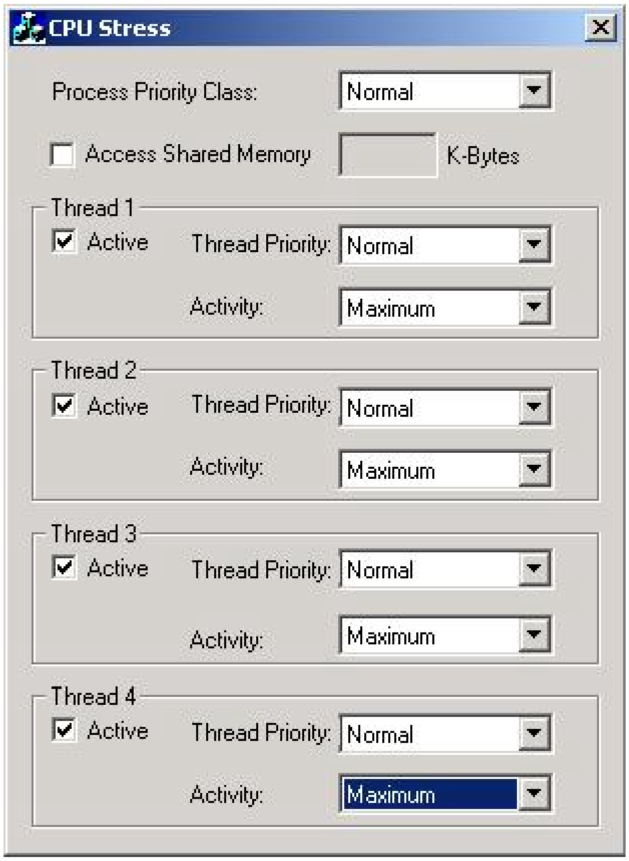
Thread 2
☑ Active Thread Priority: Normal
Activity: Medium

Thread 3
☑ Active Thread Priority: Normal
Activity: Medium

Thread 4
☑ Active Thread Priority: Normal
Activity: Medium

Example

To create a heavy workload, modify the options as shown in the following graphic.



Process Priority Class: Normal

☐ Access Shared Memory K-Bytes

Thread 1
☑ Active Thread Priority: Normal
Activity: Maximum

Thread 2
☑ Active Thread Priority: Normal
Activity: Maximum

Thread 3
☑ Active Thread Priority: Normal
Activity: Maximum

Thread 4
☑ Active Thread Priority: Normal
Activity: Maximum

3. Use Windows Task Manager or another monitoring tool to determine the actual workload on the system processors.
4. Close the CPU Stress utility to end the stress activity.

Eatmem

The eatmem utility consumes specified amounts of memory. It simulates an application with varying memory needs.

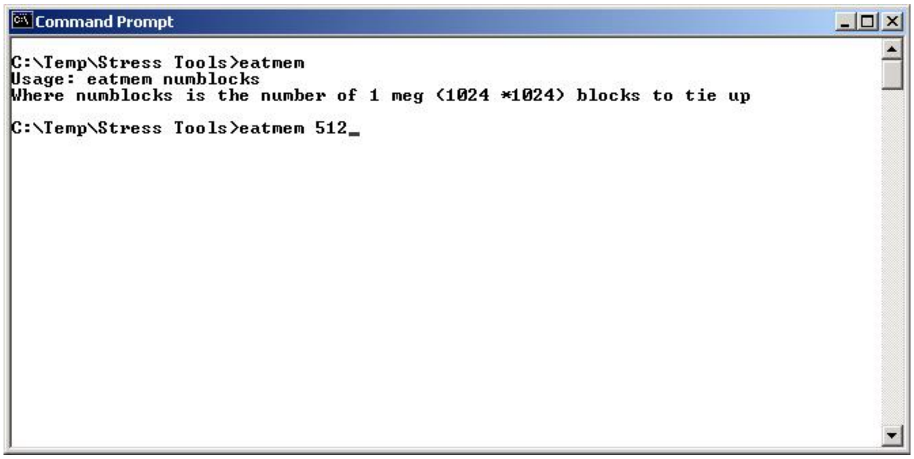
At the target server, perform the following steps to induce memory load:

1. Execute `eatmem.exe` to launch the utility. If you specify no parameters, the correct syntax displays. The amount of memory to be consumed is specified in 1MB blocks and is passed to the eatmem utility as its parameter.

   Example

   To consume 512MB of memory, use this command:

   `C:\Temp\Stress Tools>eatmem 512`



```
C:\Temp\Stress Tools>eatmem
Usage: eatmem numblocks
Where numblocks is the number of 1 meg (1024 *1024) blocks to tie up

C:\Temp\Stress Tools>eatmem 512_
```

Note

If necessary, start multiple sessions of the eatmem utility.

---

2. Use Windows Task Manager or another monitoring tool to confirm the desired memory usage.
3. Press *ctrl+C* to terminate the utility, or close the Command Prompt window.

IOmeter

IOmeter is an I/O subsystem measurement and characterization tool used for single and clustered systems. It measures the performance of a target server under a controlled load.

IOmeter is both a workload generator (performs I/O operations to stress the system) and a measurement tool (examines and records the performance of its I/O operations and their impact on the system). It can be configured to emulate the disk or network I/O load of any program or benchmark, or it can be used to generate synthetic I/O loads. IOmeter can generate and measure loads on single or multiple (networked) systems.

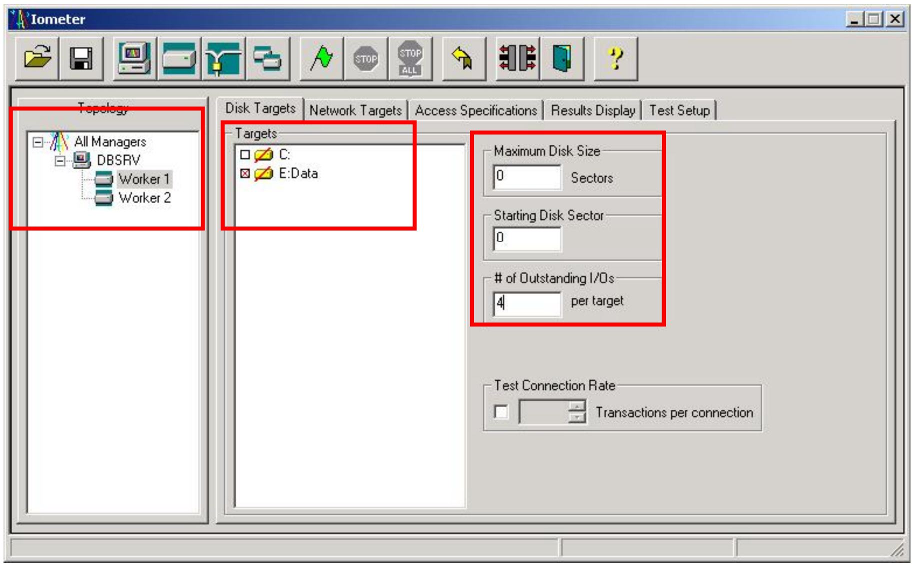
IOmeter was developed by the Intel Corporation. For terms and limitations of its use, refer to the documentation that came with the IOmeter. For additional information, click *About IOmeter → Intel Software License Agreement*.

Note
For more information, review the documentation in the DOCS folder.

At the target server, perform the following steps to induce a disk subsystem load:

1. Use Windows Disk Manager to create a small logical drive on the desired target array. Make this drive 1GB or smaller and label it *E*.
2. Execute `iometer.exe` to launch the utility.

3. At the following IOmeter screen, expand *All Managers* and modify the Worker 1 settings as follows:
   - **Targets** — Select logical drive E
   - **Maximum Disk Size** — 0
   - **Starting Disk Sector** — 0
   - **# of Outstanding I/Os** — 4 or 8, depending on the desired workload level



☐ C:
☒ E:Data

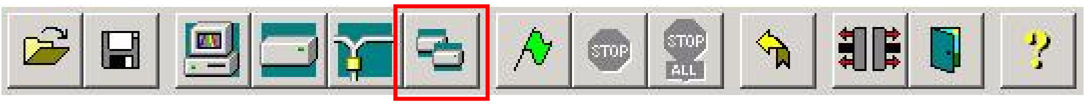
Maximum Disk Size: 0 Sectors

Starting Disk Sector: 0

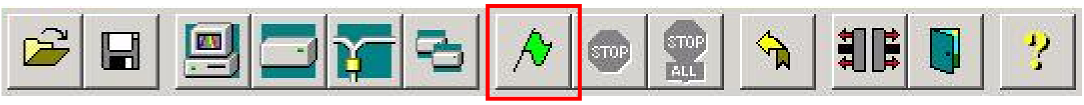
# of Outstanding I/Os: 4 per target

Test Connection Rate: ☐ Transactions per connection

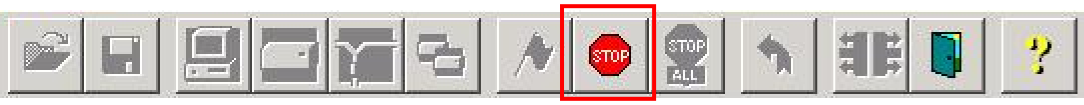
4. Repeat the preceding settings for the remaining worker threads. To duplicate any selected thread, click the *Start a Duplicate of This Thread on This Manager* button.



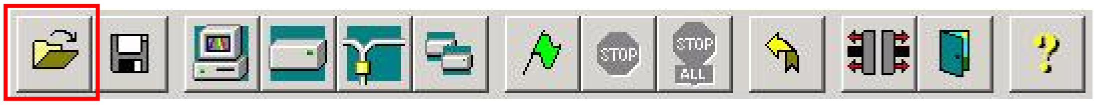
5. Click the *Start Test* button.

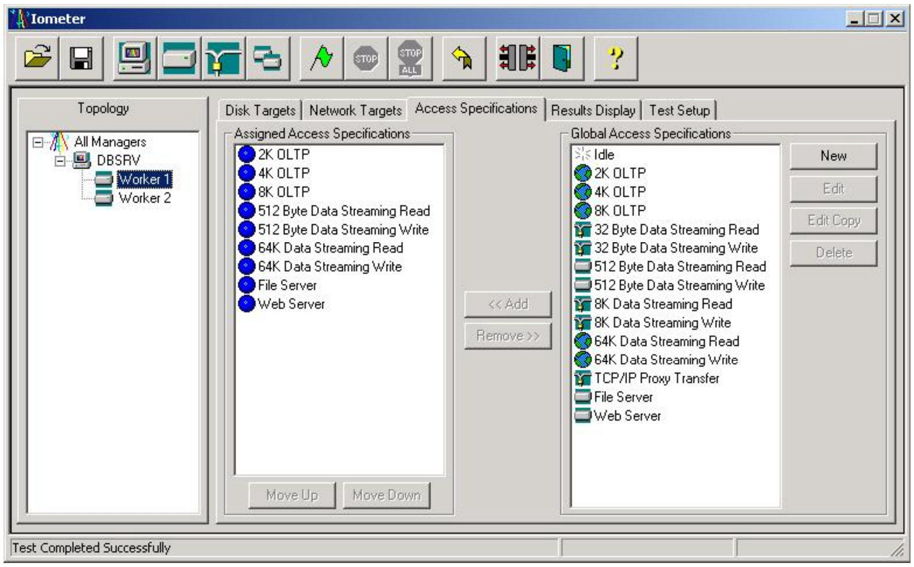


6. At the Save Results To screen, enter the appropriate information and click *Save*, or click *Cancel* to bypass saving the results.
7. IOmeter first creates the test file on the selected logical drive and then begins the stress test. To stop the test, click the *Abort Current Test and Save Results* button.



8. You can also import predefined workloads by clicking *Load Test Configuration* → *WRKLOADS* → *Open*. Then, select from a series of tests that can be assigned to each worker thread.





All Managers
- DBSRV
  - Worker 1
  - Worker 2

Assigned Access Specifications
- 2K OLTP
- 4K OLTP
- 8K OLTP
- 512 Byte Data Streaming Read
- 512 Byte Data Streaming Write
- 64K Data Streaming Read
- 64K Data Streaming Write
- File Server
- Web Server

Global Access Specifications
- Idle
- 2K OLTP
- 4K OLTP
- 8K OLTP
- 32 Byte Data Streaming Read
- 32 Byte Data Streaming Write
- 512 Byte Data Streaming Read
- 512 Byte Data Streaming Write
- 8K Data Streaming Read
- 8K Data Streaming Write
- 64K Data Streaming Read
- 64K Data Streaming Write
- TCP/IP Proxy Transfer
- File Server
- Web Server

Test Completed Successfully

Predefined Tests

9. During the stress test execution, use a monitoring tool of your choice to determine the actual workload on the disk subsystem.
10. Close the utility to end the stress activity.

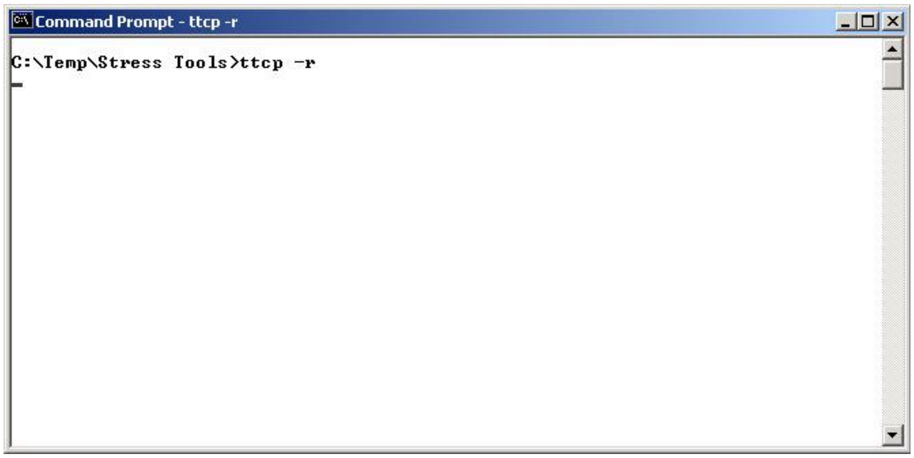
TTCP

TTCP is a benchmarking tool used to determine TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) performance between two systems. This tool was created at the US Army Ballistics Research Lab (BRL) and is in the public domain.

The following instructions assume that you have two servers, a host and a target. The host server generates the network traffic to the target server.

1. Determine the IP address of the target server.
2. Make the `ttcp.exe` utility available on both servers.
3. At the target server, open a Command Prompt window and issue this command:

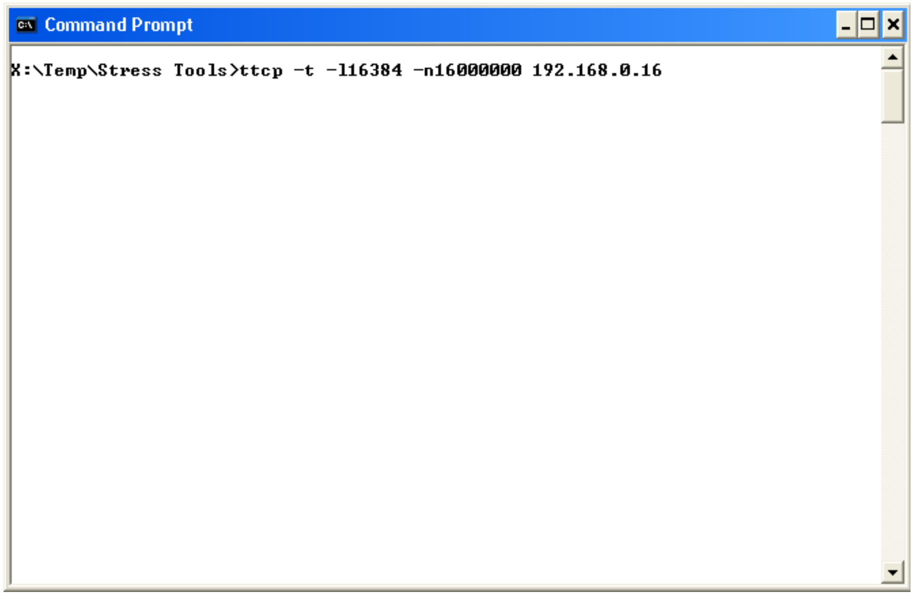
   ```
   C:\Temp\Stress Tools>ttcp -r
   ```



```
C:\Temp\Stress Tools>ttcp -r
_
```

4. At the host server, open a Command Prompt window and issue this command:

   ```
   X:\Temp\Stress Tools>ttcp -t -l16384 -n16000000
   192.168.0.16
   ```



```
X:\Temp\Stress Tools>ttcp -t -l16384 -n16000000 192.168.0.16
```

Note

The 192.168.0.16 IP address in the preceding example refers to the target server IP address. Substitute this address with the correct one. For a list of supported parameters, issue the *ttcp* command.

5. Use a monitoring tool of your choice to determine the actual workload on the network. Press *ctrl+C* to close the utility.

Interview guide

Appendix C

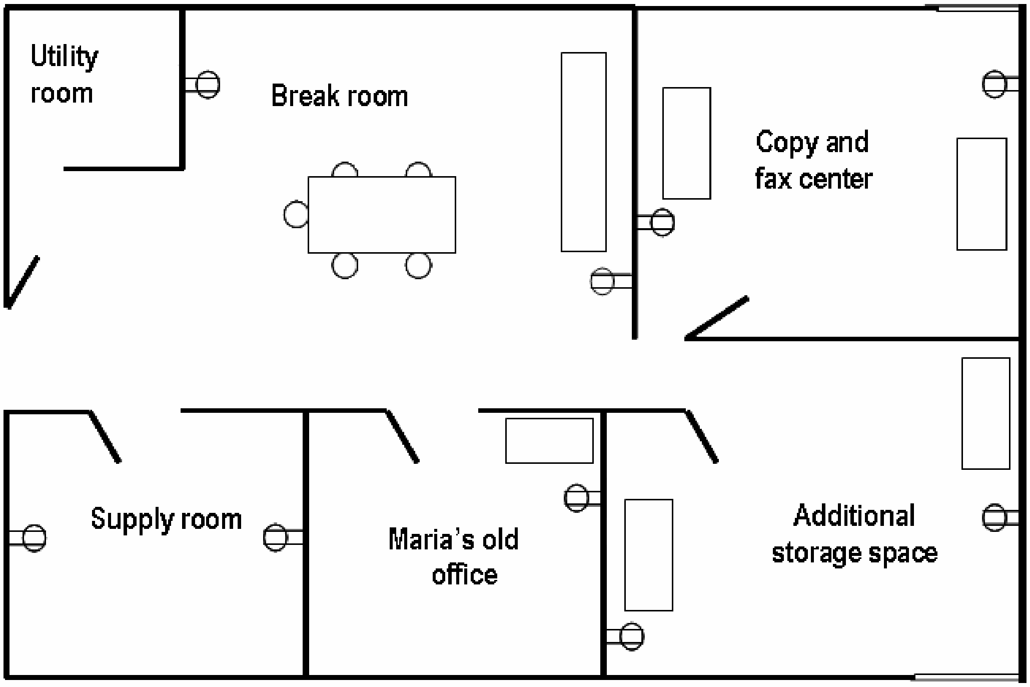
Introduction

To be able to complete the questions in Exercises 1 and 2 for ASE Module 3 — Security, students must ask Bob, the CEO of RC Engineering, and Jackie, the IT manager, questions about RC Engineering's security practices. This interview guide includes the detailed information about RC Engineering that will enable Bob and Jackie (and therefore the students) to answer those questions.

For Exercise 1, an instructor or student must assume the role of Bob by reading Synopsis 1 — RC Engineering's headquarters. That student or the instructor will then answer questions from the other students as they interview Bob to ascertain the information they need to determine the most secure location for the company's networking equipment.

For Exercise 2, an instructor or a student must assume the role of Jackie by reading Synopsis 2 — RC Engineering's security practices. That student or the instructor will then answer questions from the other students as they interview Jackie to ascertain the information they need to perform the risk analysis.

Syn



My name is Bob Ming and I am the CEO of RC Engineering. Until recently, the company had two locations, but we are closing our Silicon Valley office and moving people and equipment to the Houston headquarters. We are shipping quite a lot of IT equipment from the California location, including a mail server, a web server, and several servers in a multiplatform environment. These servers need to be integrated into the Houston network, which already comprises several servers and hundreds of workstations, laptops, printers, and other network-attached devices.

When the equipment arrives, I would like to put all the servers in the room that used to belong to my assistant, Maria, or the room directly adjacent to it that is presently used for storage. The existing wall between these rooms can be removed, if necessary. Both these rooms open off the break room, but each locks with the master key. Maria's old office has no windows, but the room next to it does. We are on the ninth floor, however, so I don't think this poses much of a security risk.

Even though I am excited about the growth of my company, I am worried about securing my assets. The California office handled security practices differently from the Texas office. I want to establish a security practice that can be followed by all people and organizations within the company regardless of the policies they were accustomed to.

I am partial to the security practices currently implemented at the RC Engineering's headquarters. Our headquarters has expanded substantially, although we have remained in our original building in Houston. This location is very secure from the outside. All employees are required to park in a garage that can only be accessed using a swipe card. The parking spaces that are located in front of the building are for visitors only.

All employees must have a badge to enter the building. Each department manager has one key, which is a master key. It opens all of the offices, the supply room, and the server room.

When visitors enter the building, they must sign in with the guard on duty. The guard then notifies the employee within the building that the visitor is scheduled to meet. Visitors must be accompanied by an employee at all times.

However, visitors have access to the lobby and the break area. The lobby contains a guest computer that allows visitors to connect to the Internet although they cannot connect to the company intranet. A password is not needed to use this workstation. Sometimes the employees use this workstation, too, because it is convenient. We also have network connections throughout the lobby, which allow visitors to connect to the Internet using their own laptops.

One room that greatly concerns me is the sales room. It is a large room that can be entered from the hallway that leads from the server and break rooms. There are no windows in the sales room. It contains 15 cubicles with a workstation in each cubicle. Each cubicle has a door that locks and walls that reach about a foot short of the ceiling. Although the sales department has been good about always remembering to wear their badges and locking their doors, lately they have been complaining about missing items.

I know the security practices at this organization can be modified to create a more secure environment. I have even required all employees to attend a security training class. But I realize there are probably security vulnerabilities that I am unaware of, and so I am asking for the help of an HP Accredited Systems Engineer (ASE). I am hoping that the ASE can evaluate the Houston location so that all changes and security practices can be implemented across the entire organization.

Synopsis 2 — RC Engineering's security practices

My name is Jackie Jones and I am the IT manager for RC Engineering.

Ever since our first experience with an email virus about a year ago, we have been aware that our company's network is vulnerable to attacks from outside intruders. If an outsider should successfully attack our network, he could retrieve credit card numbers, social security numbers, and other valuable customer data. In addition, an intruder could sabotage our work data, although we do make daily backups.

To address some of these issues, we implemented a firewall to protect our private network. This has been a successful tool so far, but I am interested in performing an intrusion test to evaluate the vulnerability of the firewall system. This test has never been performed at RC Engineering and I do not know how to get started. After I learn how to perform an intrusion test, I will then perform an audit of the network. I also plan to revisit network performance after we implement these security measures and retune the system for better performance, if necessary.

I also plan to update the encryption and decryption technology currently used. We currently implement a traditional public key cryptography that is complex and has not scaled well as the company has grown. I want to implement a simpler encryption solution for our current applications.

Although we took all recommended security measures to protect our network, we recently experienced a security breach. The CEO of RC Engineering, Bob Ming, recently received an email with the company's financials in an attachment from our accountants. Although each workstation, laptop, and server at RC Engineering has virus protection software installed, Bob did not save the file to his desktop and perform a virus scan, which is our standard procedure. Instead, he opened the file directly from his Microsoft Outlook window. The file contained a virus that spread across the entire RC Engineering network.

I was away on vacation at the time. Marcus, my assistant, was out for a family emergency and forgot to take his pager with him. Mario, a sales consultant, attempted to troubleshoot the problem. He ended up eliminating the virus, but he also erased the files needed to keep the company's website up and running. Mario should not have been able to access these files. The website was down for three days until the problem was resolved.

This breach of security has prompted me to re-evaluate our current security process. I have Bob's backing to create a standard of security policies for the entire company. Occasionally, we send out an email warning of possible security breaches and discuss ways to avoid them. The last such email contained:

- An updated list of currently known viruses
- RC Engineering's policy for saving suspect attachments to the hard drive and then running a virus scan

Generally the employees log on to the network using their user name and password. We require employees to change their passwords every 90 days. We encourage them to create a unique password using numbers, letters, and attributes. In fact, we posted the *Keys to Password Protection* poster in the break room.

Besides the employee, only network administrators should have access to the employee's workstation. But this has not always been the case. We have had at least one incident where a password has leaked out. For example, there was the time late last year when Jane Pinkerton, one of our account reps, called in sick. She emailed John Cinderblock, another account rep, with instructions for accessing a document that she had saved on her desktop. She included her password in the email. However, when she sent the email she accidentally sent it to the entire company. Everyone had access not only to her local workstation, but to all of her shared drives as well.

Because of this, we emailed a copy of the company's security policy information regarding user names and password vulnerabilities to everyone in the company. I only hope that everyone read this email.

In an effort to reduce operating expenses, the company is hiring contractors on a temporary basis and outsourcing some IT services. Currently all contractors must sign an agreement stating that all information at RC Engineering is confidential. Quite a few of our contractors have access to our intranet, for research purposes and for file sharing. We need to evaluate the security impact of these decisions.

I am asking an HP certified ASE to help me implement the appropriate security measures, so that I can do my part to ensure my company's data integrity and privacy. The information I learn from the ASE will help me hire a security program manager who can help maintain and enforce our security policies.

Linux commands

Appendix D

Introduction

Use the following page to familiarize yourself with some basic Linux commands. This page can be cut out of this lab guide and folded into quarters for convenient use in the field.

Linux Cheat Sheet

All you need to know
for daily life with Linux

Any suggestions for improvement / adding information / explaining commands on this document are much appreciated. Please e-mail to gfest@navcom.ch.

Editing and Shell-Scripting

VI editor

```
esc i           ; insert mode
esc a           ; append mode
esc A           ; append mode at the end of line
esc x           ; delete character to the right
esc :w          ; write file
esc :q          ; quit VI                  (esc q!    ; force quit)
crtl u          ; move cursor up one half page
ctrl d          ; move cursor down one half page
ctrl f          ; move cursor down by full page
ctrl b          ; move cursor up by full page
/string         ; search string forward
?string         ; search string backward
esc :set nu     ; display line numbers for debuging
```

Writing a shell - script

```
vi scriptname                       ; create a script
chmod 0777 scriptname               ; assign exec attributes
(where 0777 = 0  rwx  rwx  rwx      ; r = read, w = write,
                                    ; x = executable)
                owner group everyone
```

execute with:

```
./scriptname                        ; even if in same directory
```

Web and File Server

Apache Web Server

```
vi /etc/httpd/conf/httpd.conf            ; configure web server
                                         ; contains web-root info

/sbin/init.d/apache start / stop / status  ; SuSE version
/usr/sbin/httpd start / stop             ; RH version
          or
service httpd start                      ; RH version
```

Samba File Server

```
/etc/samba/smb.conf
service smb start                        ; RH version
/sbin/init.d/smb start / stop / status   ; SuSE version
```

Configuration using SWAT

```
/etc/services .... swat       ; vi and verify port 901
/etc/xinetd.d/swat            ; vi and verify SWAT
service xinetd restart        ; swat is under xinetd
useradd <username             ; create group & users for samba
smbpasswd –a <username>       ; enable user for samba
mkdir /shares                 ; create shared directory
chmod 2777 /shares
http://ipaddress:901
```

Miscellaneous

Firewall – simple iptables script

```
/etc/rc.d/init.d/iptables                    ; script interpreter
echo ‘’1’’ > /proc/sys/net/ipv4/ip_forward   ; turn on routing
echo ‘’0’’ > /proc/sys/net/ipv4/ip_forward   ; turn off routing
# -F    flush all rules
# -A    add rule
# -b    bidirectional s + d
# -p    protocoll
# !    invert (use the oposite)
# -s    source ip
# -d    destination ip
# -j    jump to ACCEPT/REJECT/DROP
iptables -F INPUT                            ; flush all input rules
iptables -F FORWARD                          ; flush all forward rules
iptables -F OUTPUT                           ; flush all output rules
```

```
# continued
iptables -P INPUT DROP
# do not forward anything by default = set policy
iptables -P FORWARD DROP
# deny everything from the "world" side to eth0 on Firewall
iptables -A INPUT  -j DROP -d eth0

# deny TELNET (23) access to firewall on eth0
iptables -A INPUT -j DROP -p TCP -d 192.168.1.3/32 - - dport 23
# deny ROUTING of any TELNET into the Intranet 192.168.1.x
iptables -A FORWARD -j DROP -p TCP -d 192.168.1.0/24 - - dport 23
```

Storage & EVA

```
probe-luns –i –l        ; check SCSI on EVA and MSA
dmesg ¦ less            ; see SCSI / LUN association
```

Basic Configuration

Logs

```
/var/log/messages                        ; generic
```

IP and Network

```
netconfig                                ; script
/etc/rc.d/init.d/network stop / start    ; stop/start network
vi /etc/sysconfig/network-scripts/ifcfg-eth0      ; all IP parameters
/sbin/lsmod                              ; view interface module
/sbin/rmmod                              ; remove if module
/sbin/insmod                             ; insert if module
ifconfig eth0 up / down                  ; stop / restart interface
```

User Administration

```
useradd username                         ; create user
passwd username                          ; retype password
ls /home                                 ; show known users
users                                    ; show logged in users
```

HP Specific

```
mount /dev/cdrom /var/temp               ; Management CD
./var/temp/agents/linux/eng/compaq/install
service xx restart / stop / start        ; control services
          where xx services are cmanic, cmasvr, cmastor, cmafdtn
/opt/compaq/                             ; installed files
/etc/rc.d/init.d/                        ; starting daemons
```

Services

DHCP

```
/etc/dhcpd.conf               ; configure settings
/var/state/dhcp.leases        ; (RH: this file must be manually created)
ps –A | grep dhcpd            ; to see dhcp running
kill (process id)             ; if need to restart
dhcpd                         ; start dhcp
```

TELNET, FTP ...

```
/etc/xinetd.d/      and       /etc/xinetd.conf
/etc/services                 ; check if not hashed (#) out
                    e.g.      cat /etc/services | grep telnet

Xconfigurator                 ; change display resolution (after init 3)!
```

dhcpd.conf (example)

```
server-identifier ProLiant1;
subnet 192.168.1.0 netmask 255.255.255.0{
          range  192.168.1.115 192.168.1.119;
          default-lease-time             65000;
          max-lease-time                 65000;
          option domain-name             "DOMAIN1";
          option domain-name-servers 192.168.1.1;
          option routers                 192.168.1.104;
          option subnet-mask             255.255.255.0;
}
```

Simple Info Tools

```
find . –name ’filename’       ; find filename starting at .
apropos <subject>             ; reference pages by keyword
info <subject>                ; generic help
service - - status-all        ; RH status of all running services
chkconfig - -list             ; RH show services start configuration
which *                       ; display path info
$env                          ; display path & other env. variables
/proc/                        ; cat files to check status, version, etc
/etc/modules.conf             ; show all installed modules incl. NIC
who                           ; who is logged in
finger                        ; who is logged in with user detaills
/etc/motd                     ; Message of the day
vi /boot/grub/grub.conf       ; check for ’mem= maxsize’ (e.g. 1024M)
tail /var/log/messages        ; check error- & audit messages
```

Network Monitoring

```
ifconfig –a                              ; show IP configuration
/etc/sysconfig/network                   ; vi for Server-Name change
/etc/sysconfig/network                   ; vi for Server-Name change
service network restart                  ; restart network after change
tcpdump host 16.184.41.83                ; all traffic for selected host
tcpdump ip host 16.184.41.83             ; only IP traffic for selected
tcpdump net 16.184.41.83/32              ; only selected network
tcpdump -i eth0–q –t                     ; only eth0 quiet, no time stamp
tcpdump arp                              ; shows only one proto type
tcpdump port 23                          ; shows only FTP traffic
tcpdump -i eth0 host 16.184.41.83 –q –t  ; any combination of the above
netstat –a                               ; show all network services
netstat –s                               ; show all network statistics
nmap <ip>                                ; scan open ports
```

Storage & NFS

NFS

On the host:

```
/etc/exports          ; add entry: ’/directory      ip-addr of client (rw)’
/etc/hosts.allow      ; add entry: ’all:ip-addr’

service nfs restart           ; RH restart NFS server
                              ; or ... stop and ... start
/sbin/init.d/nfsserver restart  ; SuSE restart NFS server
```

On the client:

```
mount –t nfs  host-ip:/directory  /local-directory
```

Mounting Storage

```
mount –t smbfs –o username=xyz  //ip-address/share  /mnt
mount –t nfs  ip-address:/share   /mnt
mount /dev/cdrom /mnt          ; mount cdrom
mount /dev/fd0 /mnt            ; mount floppy
mount /dev/hdc1 /mnt           ; mount disk hdc1
mount                          ; show all mounted storage
/etc/fstab                     ; vi for automounting
```

Disk Management

```
sfdisk –l                      ; display all partitions
df –m                          ; display disk usage in MB
```