nPartition Management for HP Integrity Servers using Microsoft® Windows®

HP Par Commands Wizard (Par Wrapper) and Par Command Line Interface (ParCLI) Installation and Troubleshooting Guide

January 2004 (First Edition)
Part Number 359989-001
Version: 2.1-01/08/04

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided “as is” without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

nPartition Management for HP Integrity Server using Microsoft® Windows®
January 2004 (First Edition)
Part Number 359989-001

Contents

Introduction

Advanced HP systems, such as the Superdome and IPF Integrity series of servers, may be partitioned into one or more “nPartitions”, each containing a portion of available system CPU, memory, and I/O resources. This document describes the selection, installation, operation, and troubleshooting procedures used to configure nPartitions on HP partitionable systems running or using Microsoft Windows. The primary audience for this document is HP technical support engineers and technical support personnel for HP customers using Windows.

Note that while some of the operational issues described may also occur when the commands are executed from an HP-UX 11i version 2 system, this document covers only Windows operating system configurations.

Definitions

Cell	A component of a partitionable complex consisting of processors, memory, and an I/O bus.
Complex	A server containing one or more cells that can be divided into multiple nPartitions.
I/O chassis	A component of a partitionable complex consisting of a number of PCI or PCI-X I/O card slots, which can be connected to the I/O bus of a particular cell.
nPartition (nPar, partition)	A collection of cells (and their connected I/O chassis) that functions together as a computer system. Think of this as a logical grouping of one or more cells together to form a single computer system. Of course it is an electrical/physical grouping as well.
nPar Tools	The nPar Commands (“par commands”) and the Par Commands Wizard (“par wrapper”)

Getting Started

To begin configuring nPartitions and perform partition management tasks using Windows, several fundamental questions must be answered based on your situation:

- What Windows configurations support nPartition management tools?
- What tools are provided for nPartition management using Windows?
- What additional components are required for nPartition mamagement using Windows?
- How will nPartition management be performed?

After questions have been answered for your situation, installation and nPartition management can begin.

IMPORTANT: It is very important that administrators review nPartition management options carefully in order to install and run nPartition management tools correctly!

What Windows configurations support nPartition management tools?

The nPartition management tools are supported on the following Windows platforms:

1. Any PC on the supported hardware list for Windows 2000 Professional or Server, with Service Pack 3 or greater.
2. Any PC on the supported hardware list for Windows XP Professional, with Service Pack 1 or greater.
3. Any PC on the supported hardware list for Windows® Server 2003 for IA-32.

Reference PC platforms include:

1. HP D530 PC workstation with Windows XP Professional, Service Pack 1.
2. Compaq Evo n610c laptop computer with Windows XP Professional, Service Pack 1.
3. HP Omnibook 4100 laptop computer with Windows 2000 Professional, Service Pack 3.
4. HP PC System Management Station (SMS) server, with Windows 2000 Server, Service Pack 4.
5. HP ML350 server with Windows® Server 2003.

What tools are provided for nPartition management using Windows?

On Windows, two nPar Tools are available to manage the nPartition configuration on a partitionable complex, the Par Commands Wizard and the nPar Commands.

Which one should you use? If you are an experienced administrator of partitionable systems, or if you would like to perform advanced partition configuration, then you will find using the par commands directly a better solution. If however, you are new to partitionable systems, or you want to perform simple, but powerful complex management, the par wrapper may be a better tool to use.

Par Commands Wizard ("par wrapper")

The Par Commands Wizard is a simplified graphics interface for nPar management which runs only on Windows. It is recommended as the default nPar Tool, and is capable of performing most partition management operations. This tool allows administrators to manage nPar configurations graphically, and will generate and execute nPar Commands based on user selections. It "wraps" common nPar command line actitivies into an enhanced user interface.

nPar Commands ("par commands" or "ParCLI")

The nPar Commands is a set of command line utilities (CLI) which run from the Windows command shell. Designed for advanced partition management, fast operation, and greater administrative control, the nPar Commands can be used directly in place of the Par Commands Wizard by experienced administrators.

What additional components are required for nPartition management using Windows?

Depending on your connection scenario, administrators must install one or more nPartition components, in addition to the nPar Commands and Par Commands Wizard tools, in order to perform partition management activities in Windows:

nPar Provider ("par provider")

The nPar Provider is used to communicate with a complex management processor locally or over a network using IPMI. All nPar Tool operations will require access to an nPar provider. Usually, the nPar provider is installed and used on the Windows PC along with the nPar Tools. Alternately, some administrators may choose to use the nPar Commands to connect to an nPar Provider on an HP-UX 11i version 2+ nPartition within a target managed complex.

WMI Mapper

All Windows nPar operations require the WMI Mapper to communicate with an nPar provider.   It must be installed along with the nPar tools to allow Windows WMI, the default Windows management communications protocol, to interact with WBEM. WBEM is the management protocol used by the nPar Provider. It is not required by nPar Tools running on HP-UX.

How will nPartition management be performed?

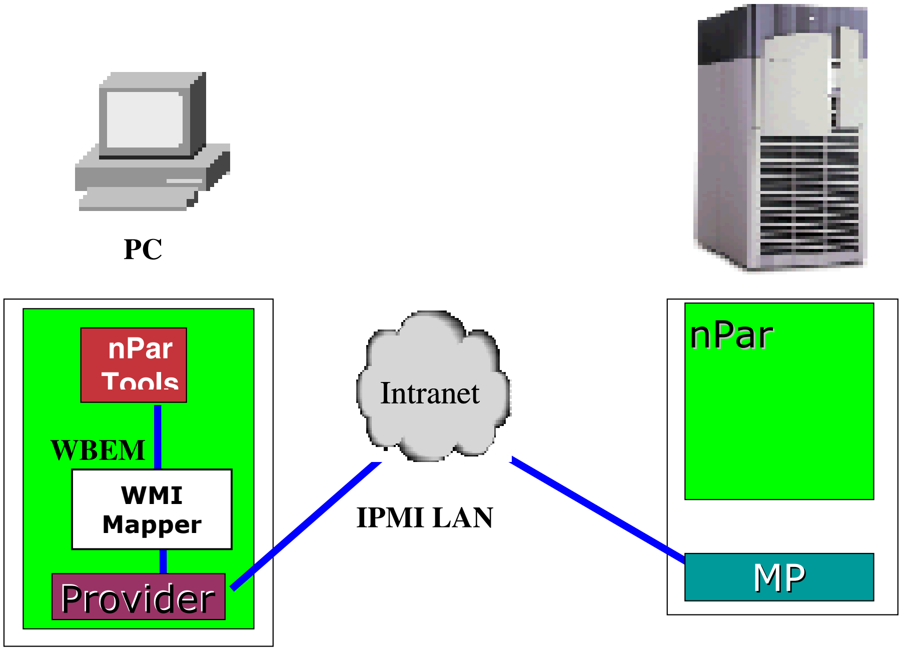
Several possible scenarios exist for partition management using Windows.   The tools used and options selected will depend upon the connection to the complex that is being managed.

Important note: Any partitionable complex that supports remote configuration can be managed from either a supported Windows PC or a computer running HP-UX 11i version 2. This can be done regardless of the operating system running in any nPartition on the complex. Thus, a Windows PC could be used to remotely configure a complex where all nPartitions on that complex run HP-UX. Similarly, an HP-UX 11i version 2 system could be used to configure a complex where all nPartitions are running a supported version of Windows for Itanium® 2. Why is this possible? Because the nPar tools can communicate directly to the complex Management Processor, or MP.

In addition, HP-UX provides a powerful graphics interface for partition management, called ParMgr. See the *HP System Partitions Guide* (Reference 1) for more information on using the HP-UX par commands or parmgr to configure nPartitions on a complex.

SCENARIO 1: REMOTE MP CONNECTION

Configure a remote complex using IMPI over LAN connection to complex MP



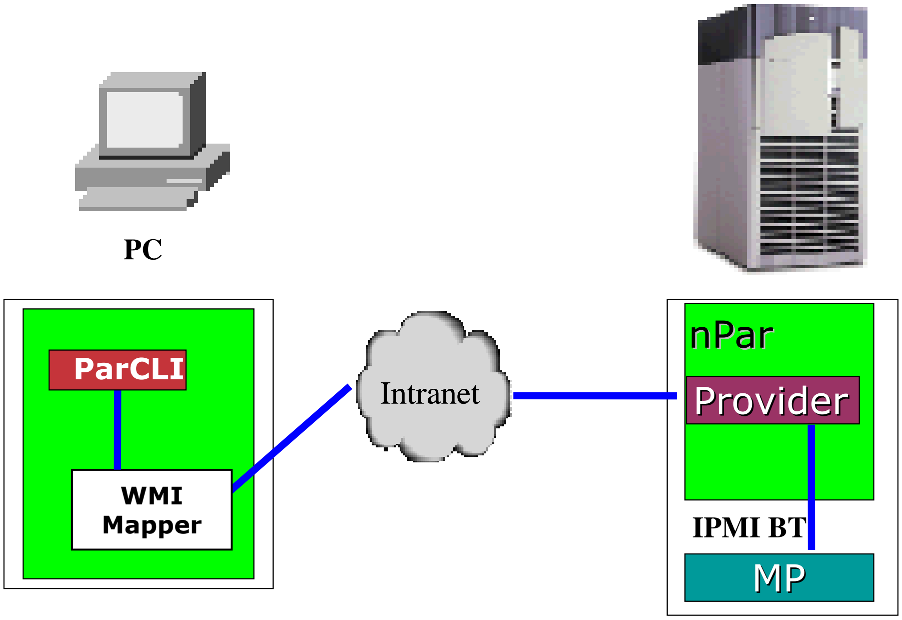
The nPartition Commands or Par Commands Wizard can be executed on a remote IA-32 PC management station running a supported Microsoft Windows OS as described in the previous section.

The nPar Tools communicate with the local nPar provider using a local WBEM connection. The nPar provider then communicates with the MP on the remote complex using the IPMI protocol over a LAN connection.

This is the primary mode in which nPar Tools run on a supported Windows PC would be used to configure a remote complex. It is the only mode in which commands run on a supported Windows PC can configure a remote complex where all nPartitions are not booted, or were all active nPars are running Windows 2003 for Itanium® 2.

SCENARIO 2: REMOTE NPAR CONNECTION (REMOTE HP-UX 11i V. 2+ NPAR ONLY)

Configure a remote complex using an HP-UX 11i version 2 nPartition on that complex



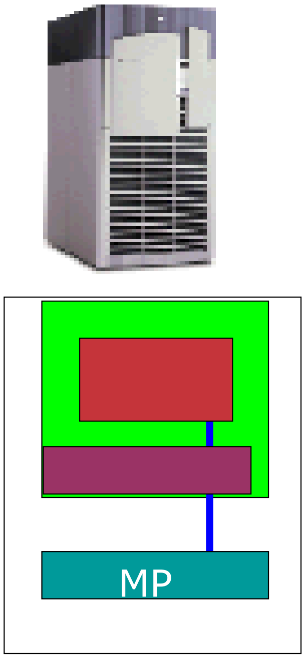
A partitionable complex can also be configured remotely using an nPar on that same complex. The Microsoft Windows ParCLI can use the WBEM protocol to communicate with a provider on a remote nPartition, allowing the ParCLI to be run on any platform where they are supported. **The Par Commands Wizard (ParWrapper) cannot be used in this configuration.**

The command sends a WBEM request to the provider by secure HTTP. The provider on the target nPartition communicates with the MP as in the previous scenario.

While the nPar Commands may be run anywhere that it is supported, the remote nPartition must be running HP-UX 11i version 2 or later, as the provider has not yet been ported to Windows® Server 2003 for Itanium® 2. The PC must also have SSL certificates properly configured to permit the secure HTTP communication to take place. The procedure to configure SSL certificates is described in Appendix A.

SCENARIO 3: LOCAL CONNECTION (UNSUPPORTED FOR WINDOWS)

nPartition Management of the local complex using an nPartition on the complex



The simplest nPartition management configuration is when all software components run on an nPartition in the complex. The commands require no command line arguments giving the target of the operation, as the default is the complex where the local operating system is running. The par commands communicate with the provider by a local WBEM connection, which in turn connects to the complex MP through the IPMI block transfer (BT) protocol, via a dedicated controller in the MP.

Currently, this configuration is supported only for HP-UX. The nPar tools have not yet been ported to Windows® Server 2003 for Itanium® 2. If partition management tools are currently run without options that specify a remote complex, it will return an error message indicating that the platform is unsupported or not partitionable.

Note that on older partitionable systems, such as the SD-32000 or rp8400, where HP-UX 11i version 2 is not supported, this is the only method of configuring the complex using the nPartition tools. In that case, local HP-UX nPar Commands must be used, which communicate directly with the MP through a proprietary system firmware interface rather than IPMI/BT.

Installation and Troubleshooting Installation Problems

Installation Process for the Windows nPar Tools and nPar Components

NOTE: Installation files below may be found on the Smart Setup media delivered with your platform.

1. Prepare the target complex for remote partition management, if not already done. On the target complex MP, enable IPMI LAN access with the SA command, and set an IPMI password with the SO command. See the *HP System Partitions Guide* (Reference 1) for more information.
2. On the local management station, install necessary patches, if not already done. Note that all required patches are pre-installed on a PC-SMS system, but must be manually installed on other PCs that might be used as a remote management station. See Appendix A for details.
3. On the local management station, install the WMI Mapper component. Double-click or select **Install** from the context menu for file **WMIMapper.msi**. Follow the installation wizard instructions.
4. On the local management station, install the nPartition commands component. Double-click or select **Install** from the context menu for file **nParCommands.msi.** Follow the installation wizard instructions.
5. On the local management station, install the nPartition provider component. Double-click or select **Install** from the context menu for file **WMInParProvider.msi.** Follow the installation wizard. Reboot the system if requested.
6. On the local management station, install the Par Commands Wizard tool. Double-click or select **Install** from the context menu for file **ParCommandsWizard.msi.** Follow the installation wizard instructions
7. If management of a remote nPartition via WBEM will be needed, configure the SSL Trusted Certificate Store on the local management station PC. Instructions for this are in Appendix A of this document and in the on-line README file.

Notes:

1. Steps 4 and 5 above can be performed in any order. The order above places the reboot at the end of the installation procedure. If the nPartition provider is installed before the commands, the reboot, if requested, can be deferred until after the commands are installed.
2. If only remote management via WBEM will be used from the PC, the provider component is not required. Install only the WMI Mapper and commands components, and configure the SSL Trusted Certificate Store. Skip steps 5 and step 6, but perform step 7 in this case.
3. If only remote management via IPMI over LAN will be used from the PC, the SSL Trusted Certificate store need not be configured. Skip step 7 in this case.

The installation packages will check that the proper versions of prior components and all required patches are installed before proceeding.

Operation: Performing nPartition Management

The Par Commands Wizard is recommended as the primary interface for most partition management operations. Review the Par Commands Wizard Manual at **Start** > **Programs** > **Hewlett-Packard > nPar Management** for complete usage details

The par commands can be run from any command prompt after the PC is rebooted following the installation, as the directory containing the commands will be in the system PATH. When using remote configuration via IPMI (SCENARIO 1), the `-g` and `-h` options must be used on the command line. When using remote configuration via WBEM (SCENARIO 2), the `-u` and `-h` options must be used on the command line. At the current time, one of these two methods must be used when running the par commands from a Windows PC.

See the *HP System Partitions Guide* (Reference 1), the par commands manual available from the Start menu (**Start** > **Programs** > **Hewlett-Packard** > **nPar Management** > **nPar Commands Manual**), and the README file also available from the Start menu (**Start** > **Programs** > **Hewlett-Packard** > **nPar Management** > **README**) for more information on command options and operation, along with applicable release notes.

△ **CAUTION: Several steps may be required for partition management changes to take effect and function correctly on Windows nPartitions.**

Windows nPartitions must be placed in reset for reconfig state for partition management changes to take effect. In addition, the Par Commands Wizard **requires** that partitions that will be managed are placed in reset for reconfig state before beginning. This can be done using the MP telnet Commands Menu (CM) to run the 'RR' command. **It is recommended that Windows partitions that will be modified are placed in reset for reconfiguration state before using the nPar Tools. If you have existing partitions that you do not want to remove or modify, do not select them for "reset for reconfig".**

In addition, the ACPI flag must be set on Windows partitions using the EFI 'acpiconfig windows' command followed by a reset.

Review *Configuring Microsoft® Windows® Server 2003 on the HP Integrity Server, Enterprise Edition, Configuring Microsoft® Windows® Server 2003* on the *HP Integrity Server, Datacenter Edition* or the *Pre-OS Setup Guide* issued with your platform for details on these issues.

Troubleshooting Operational Problems

Common Windows nPartition Management Issues

Shutdown and reset instructions after using parremove

After using the parremove command to remove an active partition, you may see the following message:

```
   C:\>parremove -x x -x -x xx.xxx.xx.xxx -g Admin
```

NOTE: The -g option may require up to 2 minutes to complete. Please wait...

NOTE: The specified partition has been marked for removal.

Start by performing a Windows OS shutdown (using the **Shutdown** command or **Start** menu action) for this partition. Next, go into the MP menu and use the **RR** command to reset your partition in "reset for reconfiguration" mode. HP recommends that the OS on the partition be placed in this mode before using the parremove command.

Warning message displayed when creating or modifying partitions using parcreate or parmodify

When using parcreate or parmodify and the option to set or modify the amount of Cell Local Memory (CLM) are used, you may see the following warning message:

WARNING: Unable to determine if the target partition supports cell local memory.

NOTE: This is normal behavior. The OS that is running or will be installed on the partition cannot be determined remotely by parcreate or parmodify. The commands display this warning if the OS on the target partition does not support CLM then the memory allocated as CLM will not be usable by the OS. Note that both HP-UX 11i version 2 and Windows® Server 2003 support CLM.

HP recommends that the OS on the partition be placed in "reset for reconfiguration" mode before performing these operations.

Error messages when using frupower

When using frupower, you may see the following error messages:

```
ERROR:  Cannot power off I/O chassis x/x/x (your chassis #).
        Chassis is attached to inactive cell x (your cell #).
        Please turn cell power off."
```

You will see this error message if you attempt to power off an I/O chassis independently from its attached cell. An I/O chassis can be powered off independently from its attached cell only in very limited circumstances. See the on-line documentation for the frupower command for these circumstances. HP recommends that customers power off the cell, which will automatically power off the I/O chassis.

Par Tools fail to update the Stable Complex Configuration Data (SCCD)

You may see the following errors when using parcreate or parmodify to add or remove cells from a partition, or to modify the CLM values on cells in a partition, or to use parremove to remove a partition.

ERROR: The Partition Configuration Data was written out, but could not write Stable Complex Configuration Data.

Attempts to undo the Partition Configuration Data changes have failed. As a result, options which cause partition reconfiguration i.e., addition or deletion of cells have failed, all other options have succeeded.

Subsequent attempts to run other commands may result in either:

ERROR: Unable to update the Stable Complex Configuration Data.

Or, failed to connect to target partition or complex.

This error can occur when the command attempts to update the SCCD with the complex name set to its initial default value of 20 blank spaces.

To troubleshoot this problem take the following steps: If the IPMI LAN access is not enabled, it must be enabled first. Review the installation steps in this document for more details.

1. If you see "**Failed to connect to the target partition or complex**", verify you have network connectivity by telnetting to the MP and successfully logging in.
2. Additionally, verify that the nPartition provider is running. To do this, go to the Windows Service Management Console in **Start** -> **Control Panel** -> **Administrative Tools** -> **Services**. Find the service named **WMINParProvider** and make sure it is started. If not, click on the **WMINParProvider** service and use the **Start context** menu action to start it. If it is missing, you may need to reinstall as described above.
3. If you see errors in updating the SCCD, ensure that the SCCD is unlocked with the command: `parunlock –s –g –h <hostname of MP>`
4. Check whether the complex name has been set with parstatus **–X –g –h** <hostname of MP>. Set the complex name to any string other than all blanks (this is the default setting) using the `cplxmodify` command:

   e.g. `cplxmodify –N yourcomplexname –g –h <hostname of MP>.`

See the on-line documentation of the cplxmodify command for details on the valid syntax of complex names.

You may then continue to successfully create and modify your partitions.

HP recommends that the complex name be set to as the first action when the complex is set up to prevent these errors.

NOTE: The message "Error: Unable to update the Stable Complex Configuration Data" can occur if some other administrator or application has locked the SCCD at the time the parcreate, parmodify, or parremove command was run.

Incorrect Parstatus -p -V output

Issue: parstatus -p -V incorrect output.

In the output from parstatus -p -V, the value for "PDC revision" should be interpreted as "System firmware revision".

Also, the value "IODCH version" is valid only for PA-RISC cells and will be FFFF for partitions with Itanium®-based cells.

Incorrect Parstatus -c -V output

Issue: parstatus -c -V incorrect output.

In the output from parstatus -c -V, the value "CPU Type" is valid only for PA-RISC processors. It will always be FFFF for Itanium®-based processors.

Environment variables

On the management station, the commands and provider require that the %PEGASUS_HOME% environment variable be set. In addition, the %PATH% environment variable must contain the directory in which the par commands are installed, or the command must be run with its full directory path listed, e.g.

```
"c:\Program Files\Hewlett-Packard\nPar Management\parstatus.exe".
```

Error messages

See Appendix B for a full list of error messages that can occur during operation of the commands. Note that due to limitations in the Microsoft WMI implementation, some of the error message data returned by the nPartition provider is not transmitted through the WMI server to the client command when an error occurs. However, under Windows, the provider logs the error data in the Application Event Log (AEL). Additional information about an error can be obtained by examining the most recent entries logged by the nPartition provider in the AEL. The AEL can be accessed from the context menu on the “My Computer” desktop object. Select My Computer\Manage, then when the application opens, select System Tools\Event Viewer\Application in the left hand pane. Select an entry in the right hand pane and then choose the Properties action from the context menu to see the message itself.

Testing the nPar Tools

To verify the correct operation of the complete software stack, one can perform the following simple tests.

1. Open a command prompt window, for example by selecting **Start • Programs • Accessories • Command Prompt**. Then type the command

   ```
   C:\Windows> parstatus -X
   ```

This command will attempt to display complex-wide attributes for the management PC itself, which is not a partitionable system. The command should be found in the PATH, but result in the following message.

```
Error: unsupported platform
```

Since the management PC is not a partitionable platform, the command will fail as above, but to do so the command must have successfully contacted the provider through the WMI Mapper.

2. If access to an partitionable complex that supports remote management is available, e.g. HP Integrity Superdome, HP Integrity rx8620, or HP Integrity rx7620, type the following command:

   ```
   C:\Windows> parstatus –X –h <mp> -g <password>
   ```

Where `<mp>` is either the IP address or the hostname of the MP of the partitionable system, and `<password>` is the MP IPMI password. This command should result in the display of approximately 10 partitionable complex attributes, including the complex name, model number, and so on. There may be a delay of a few seconds up to a minute or more, depending on network distance from the management PC to the partitionable system.

Locating the source of a problem

With a set of 3 software components, locating the source of a problem can sometimes be difficult. In cases where the error message does not describe the source of the problem, or when the error can result from multiple causes, the “wmiop.exe” utility included with the WMI Mapper component can be used to assist in this process. Use of this utility to locate problems is described in Appendix C.

Some issues with IPMI over LAN operation

The IPMI specification requires that LAN traffic be sent as datagrams with the UDP protocol, which does not guarantee delivery of a datagram. In addition, a large data structure containing static configuration information about the target complex must be downloaded from the complex MP by the nPartition provider. This data gives the provider the necessary information to request dynamic information about the complex. This can cause the following issues:

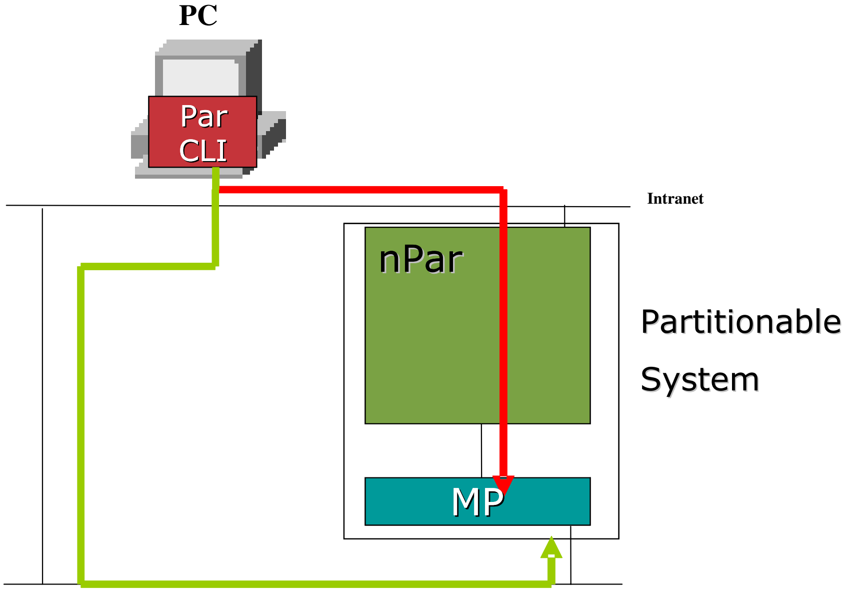
1. The first time that a particular remote complex is accessed by a par command, using IPMI over LAN, the command can take significantly longer to complete, as much as 2 minutes or more, depending on the speed of network communication between the remote management PC and the complex MP. The provider caches the static data and reuses it for subsequent requests, so future invocations of any par commands will not incur this initial overhead. However, if the nPartition provider is restarted for any reason, this cached data is lost. The first data request to the MP after the restart will incur the same startup overhead.

2. The speed and reliability of network communication between the remote management PC and the complex MP has a large effect on the reliability of command execution. Since the UDP protocol does not guarantee datagram delivery, the provider will retry a number of times when packets fail to arrive in a reasonable time, but if the network connection between the PC and MP is too unreliable or slow, the provider will eventually time out and return an error to the par command. This is often seen as a display of the message "[X] data is not available", where [X] might be cell, I/O chassis, cabinet, or other data about the complex. Best performance and reliability is obtained when the PC and MP are on the same subnet, in close network proximity. Long distance network access is possible, but may be unreliable or slow. The longer the distance, and the slower or more unreliable the connection, the worse this effect will be. In the worst case, it can cause the commands to be effectively unusable. This effect is noticed most often when using the parstatus command, which has the highest required data volume. Other commands tend to require less data, and so may be more reliable in situations where parstatus is problematic. However, since parstatus displays the current complex configuration, its use is normally critical to getting the correct configuration settings. When this occurs, but remote management is required, it is better to remotely access a PC on the same subnet as the complex MP using Remote Desktop Services, or other methods as described later, and configure the complex from that "closer" PC.

Remote Management Network Options and Issues

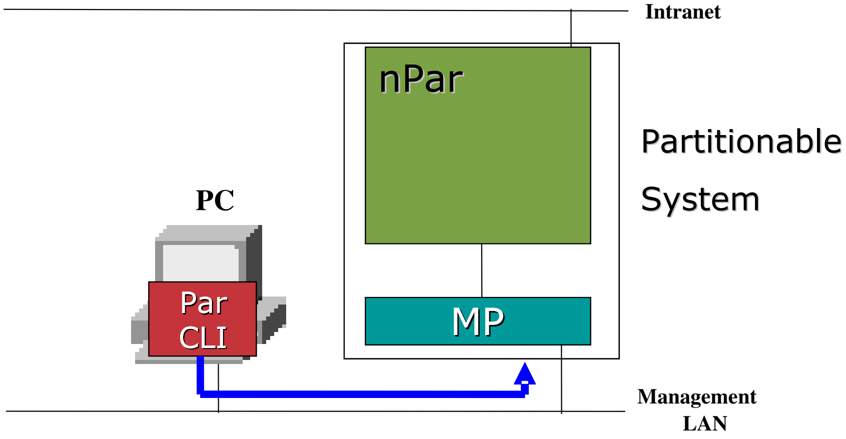
The network configuration of the partitionable complex with respect to the PC where the partition commands will be executed will affect the methods by which the commands can be executed. Generally, there are three options. Selection of a method will depend on the hardware available and security concerns for the particular installation.

Management station PC on general use LAN



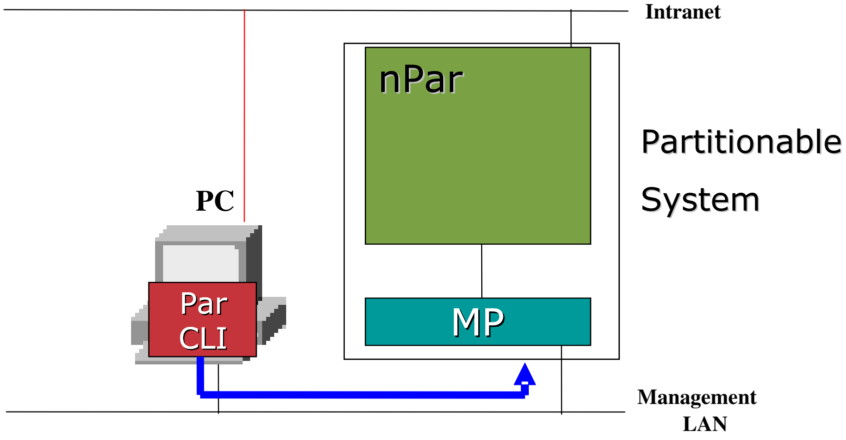
The simplest option is to connect the remote management PC, the nPartition and the MP to a general purpose LAN. In this configuration, the PC used for remote management can access both the nPartition (if running HP-UX 11i version 2 or later) using the `-u` and `-h` options and the MP using the `-g` and `-h` options. The PC need not be dedicated to nPartition management and can be used for other work. However, this is the least secure method. It depends on the encryption used in the secure HTTP connection to the nPartition or that used in the IPMI LAN session to prevent passwords and other data from being extracted, and makes the MP widely accessible.

Management station PC on dedicated management LAN



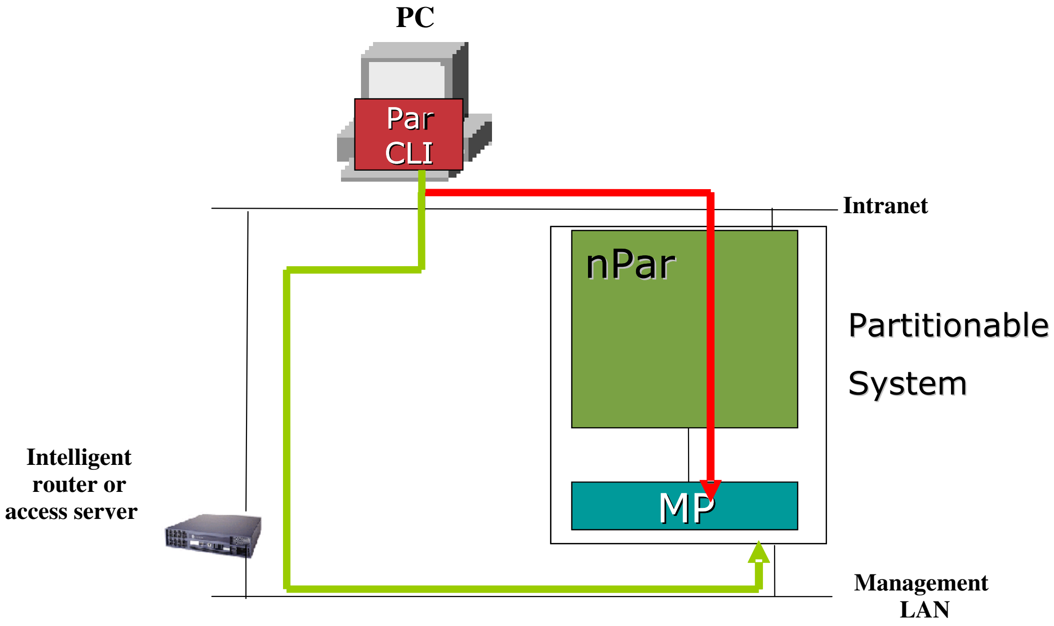
A more secure method is to place the remote management PC and the MP on a dedicated management LAN, physically separate from the general use LAN. This is more secure, but also less flexible, as the PC used for partitionable complex management must be dedicated for that purpose.

Management station PC on both dedicated management LAN and intranet LAN



A third option is to have physically separate LANs and connect the PC used for remote management to both of them. This requires that the PC contain two network interface cards. With supported Windows operating systems, no special configuration of the commands is required, as long as the network interfaces themselves are configured to access the correct set of network addresses. Windows will route network traffic appropriately. The general purpose LAN would be used for remote WBEM connectivity to an HP-UX 11i version 2 nPartition (`-u` and `-h` options), and the management LAN would be used for IPMI over LAN connectivity to the MP (`-g` and `-h` options). This method is more complex, but keeps partition configuration network traffic off the general use LAN when the `-g` option is used, while still permitting the remote management PC to be used for other purposes.

A similar option is to connect the two LANs with an intelligent router or access server that can restrict access to the management LAN to a particular set of PC systems or users authorized to connect to it. This method restricts the network visibility of the MP to specific systems or users, and allows the remote management PC to be used for other purposes as well, but does put the encrypted passwords and other data on the general use LAN.



Accessing the management station PC remotely

As previously noted, it is desirable to have the client that is running the par commands near the complex it is managing, to minimize the probability of UDP datagrams being lost in the WAN environment.

Given that a company's main support center may be geographically dispersed from its datacenter, this would mean the par commands should be deployed near the datacenter where network latency is minimal and network reliability is best. The Administrator could then use a desktop remote control package, which will incorporate an underlying network protocol more suitable for dispersed WAN links, to access the management station PC.

The options available are based on the Windows Operating System where the par commands are installed. The next few paragraphs describe the available options.

Third Party Remote Control Software (Suitable for Windows 2000 Professional)

Windows 2000 Professional did not ship with a method for remote control of the desktop. The only option is to add another vendor's remote control software such as Symantec's PCAnywhere® or an Open Source product such as Win VNC (from www.realvnc.com).

The implementation details of Third Party products are beyond the scope of this document, but each one has supporting documentation on how to make the client running the par commands available for remote desktop control.

Terminal Services (Suitable for Windows 2000 Server and Windows® Server 2003)

The server editions of Windows 2000 and Windows 2003 come with a service known as Terminal Services. Terminal Services has the ability to create another log on session that is different to the console, and leaves the console still available for other administration work.

Terminal Services is configurable in two modes – "Application mode" and "Administration Mode" which have major differences in licensing terms, and predominantly subtle differences in Application Compatibility. The ParCLI application is supported on Terminal Services in both "Application mode" and "Administration mode".

For normal use, an administrator will only enable Terminal Services for "Administration mode". This particular mode does not require any further licensing, and does not need License Activation, but due to this has two major restrictions. Firstly only two connections can be made concurrently in "Administration Mode", and the users logging in must be members of the Administrator's group. When installing Terminal Services, this is the default mode that is configured unless otherwise specified.

There is a slight difference in installing Terminal Services between Windows 2000 and Windows 2003. In Windows 2000 Server, Terminal Services must be installed by clicking its checkbox in Add/Remove Windows Components. In Windows 2003 it is installed by default, although the "Terminal Services" checkbox is not clicked. The checkbox in Windows 2003 is purely reserved to install Terminal Services in "Application Mode". Lastly, with Windows 2003 to enable connection to the Terminal Service you must enable remote connection via the System Properties "Remote" tab for the computer. This will allow you to connect.

Once installed, a client access portion of Terminal Services is required for the PC (or PC's) that will connect to the client running ParCLI. This is generally called "Remote Desktop Connection" and is available as installable image that is included with the Operating Systems, or is downloadable separately on the Microsoft website.

Windows XP and Windows 2000 Server already have the Remote Desktop Client installed by default, which can be used to connect to a Windows 2000 Server's Terminal Service. It is available at **Start → All Programs → Accessories → Communications → Remote Desktop Connection** on most systems. On Windows Server 2003 it can be found at **Start → Administrative → Tools → Remote Desktops.**

Windows 2000 Professional and some Server revisions do not come with a Terminal Services client by default. You can download the client for free from Microsoft. Go to http://www.microsoft.com/downloads and search for "Terminal Services Client".

More information on Terminal Services can be found at the Microsoft Windows 2003 Technology Center located at

http://www.microsoft.com/windowsserver2003/technologies/terminalservices/default.mspx

Remote Desktop Services (Suitable for Windows® Server 2003 and Windows XP)

Windows Server 2003 and Windows XP also have the ability to remote the desktop similar to Third Party applications such as PC Anywhere.

By default neither Operating System allows this to occur. You must enable it by the System Properties “Remote” tab for the computer. This will allow the Remote Desktop Connection program to connect directly to the client’s console. Please note an additional step is required to connect to a Windows 2003 console, whereby the /console switch must be used with the Remote Desktop Connection application. This is only present on the newest application downloadable from Microsoft and also available as an install image with Windows 2003 (it is a 32 bit program that is available on both the 32bit and 64 bit Windows® Server 2003 operating systems).

Windows XP/2003 Server Remote Desktop clients can connect to Windows Server 2003 and Windows XP with Remote Desktop Services enabled. In addition, a Windows 2000 server with Terminal Services enabled can also be accessed with the same Remote Desktop client. It is available at **Start** > **All Programs** > **Accessories** > **Communications** > **Remote Desktop Connection**. On Windows XP. On Windows Server 2003 it can be found at **Start** > **Administrative** > **Tools** > **Remote Desktops.**

Telnet

Since the par commands are executed from a command prompt, it is also possible to use a telnet application (either the telnet command delivered with Microsoft Windows, or a third party application such as Reflection® 1) to open a command prompt on the remote management PC. The remote management PC must have the Telnet service installed and started. There may be limitations on the number of telnet connections permitted into the remote management PC by the host operating system. Simply invoke the telnet application on the PC, giving it the hostname or IP address of the remote management PC as the target. Log in to the telnet server with a valid username and password. From there, execute par commands as if running in a command prompt on the remote management PC. However, only commands may be used in this mode. No GUI application may be run.

OS Service Pack Upgrade Issues

Until the required patches and hotfixes are incorporated into Windows service packs, it is possible that upgrading the service pack level of the OS after installing nPartition components could affect operation.

1. Windows 2000 Professional or Server. Upgrading from Service Pack 3 to Service Pack 4 after installing the nPartition components causes no issues.
2. Windows XP Professional. Upgrading from Windows XP to Windows XP Service Pack 1 can overwrite a file replaced by the Q332207 hotfix with an older version. Reinstalling the hotfix will correct the problem.

References

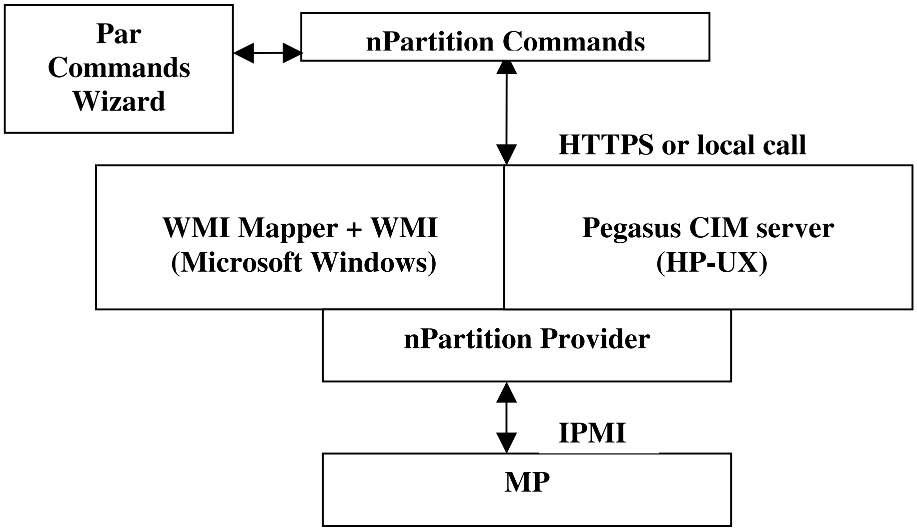
The latest versions of the following documents are available at http://docs.hp.com.

1. HP System Partitions Guide
2. HP Integrity Server User Guide
3. HP Integrity rx8620 User Service Guide

The nPartition Management Software Stack

The software configuration required for nPartition management varies depending on the operating system on which the software is executed.

The first version of the par commands was delivered on HP-UX 11i version 1. The commands made configuration queries and changes through a proprietary system firmware interface specific to PA-RISC. HP-UX 11i version 1 commands do not support remote management.



The second version of the nPartition commands was delivered first on HP-UX 11i version 2, and subsequently on selected versions of Microsoft Windows. These commands support remote management in two ways. First, they use the WBEM protocol (WMI on Windows operating system versions), which permits a client-server access model. The command acts as a WBEM or WMI client, which makes requests of a provider. That provider may be accessed on a remote system through secure HTTP, or accessed on a local system through system calls. Because the commands and provider for nPartition configuration were first developed on HP-UX, they use the Open Group's open-source WBEM client interfaces and server software, Pegasus. Pegasus uses an XML-based communication protocol and data formats over secure HTTP, which is different than that used by Microsoft's WMI implementation.

Therefore, on Microsoft Windows there must be a software layer to translate between the Pegasus protocol and data format and the WMI protocol and format. The WMI Mapper component provides this translation, allowing client applications and providers developed for Pegasus to be easily ported to Microsoft Windows. The figure above shows a typical data path. A Pegasus client, such as the *parstatus* command, sends a Pegasus-formatted request to the WBEM server on a known network port. That request is translated to WMI format by the WMI Mapper, is forwarded to the WMI server, which in turn sends it to the appropriate provider, in this case the nPartition provider. The provider uses API services provided by the WMI Mapper to translate the request back to Pegasus format, queries the management processor for necessary information, and sends a response back to the client application through the server.

Communication between the par command and the WMI Mapper is through a local system call or, when the provider is located on a remote system, by secure HTTP. The provider communicates with the partitionable complex Management Processor (MP) through the IPMI protocol. When sent over the LAN, the IPMI messages are encrypted.

This strategy permits a number of methods to configure a partitionable complex, depending on where the client command and the nPartition provider execute.

Appendix A: Installation and Configuration Details

Configuring the SSL Trusted Certificate Store on Windows.

1. Locate the SSL Trusted Certificate Store on the target nPartition.
   a. Locate the configuration file for the HP-UX CIM server on the remote HP-UX 11i version 2 nPartition through which the complex will be managed. This is normally in file $PEGASUS_HOME/cimserver_current.conf.
   b. Open the configuration file. Search for the entry: sslCertificateFilePath=<path/filename>. If there is no sslCertificateFilePath entry in the file, the default value is $PEGASUS_HOME\server.pem
   c. The file named in the entry is the SSL Trusted Certificate Store file, by default $PEGASUS_HOME\server.pem.
2. Open the certificate file, and copy everything from the text "-----BEGIN CERTIFICATE-----" to "-----END CERTIFICATE-----", inclusive, into a separate file.
3. Locate the SSL Trusted Certificate Store on the PC where the commands will be run. If the PC has been configured with the HP Shared Certificate Store, the file will be located at %HP_SSL_SHARE%\client.pem. Otherwise, the default location is %PEGASUS_HOME%\client.pem.
4. Append the certificate data copied in step 2 above to the end of the client.pem file identified in step 3.

Required Patches

The required patches are available on the Smart Setup media on which the commands themselves are delivered. Note that patches need only be installed once. When reinstalling or upgrading the other components of the nPartition management software stack, the patches need not be reinstalled.

1. On Windows 2000 Server or Professional with Service Pack 3 or later, install the WMI extension in file "wmirdist.msi". Then install hotfix Q332207 for Windows 2000.
2. On Windows XP with Service Pack 1 or later, install only hotfix Q332207 for Windows XP.
3. On Windows 2003, no patches or hotfixes are required.

Appendix B: Error messages

Par commands messages

The following messages are written to standard output by the commands. Note that this list does not include messages concerning syntax errors or errors caused by attempting a configuration change that is not valid for the current configuration, e.g. removing a cell from a partition that is not assigned to that partition. Those messages are generally self-explanatory, but additional information about the operation of the commands can be obtained from the *HP System Partitions Guide* (Reference 1).

Message	Cause	Action
Cannot connect	a. The nPar Provider you are attempting to use is not running. If using the –h option, check your local management system's nPar provider. If your are using the –u option, verify the nPar provider on the remote target nPartition. b. MP is not available on the network . c. MP settings are incorrect.	a. Make sure the nPar Provider component is installed. On Windows, verify the nPar provider service is running using **Start** -> **Control Panel** -> **Administrative Tools** -> **Services.** b. verify you have network connectivity by telnetting to the MP and successfully logging in. c. Telnet to the MP. Enter Commands Menu and enable IPMI LAN access with the SA command, and set an IPMI password with the SO command. See the *HP System Partitions Guide* (Reference 1) for more information.
Unsupported Platform	a. Command was run on the local system, which is not a partitionable server. b. With –u and –h options, target host is not a partitionable server.	A. Use the –g and –h options or the –u and –h options to specify a partitionable complex as the target of the operation. b. Specify the hostname or IP address of an nPartition.
The nPartition Configuration Privilege of the target complex is restricted.	The MP is set to disallow changes to the configuration of any nPartition except the one from which the request is made.	This can only occur when using the –u option. In that case, specify the nPartition that will be altered as the target in the –h option. See the *HP System Partitions Guide* for more information.
Cannot determine the state of the nPartition Configuration Privilege.	The command cannot retrieve this data from the provider. In most cases, this is caused by excessive lost packets during data retrieval.	Retry the command, or use a management PC with more reliable network communications to the MP.

Cannot determine if the platform is partitionable.	a. See “Error: unsupported Platform” above. b. The command cannot retrieve this data from the provider. In most cases, this is caused by excessive lost packets during data retrieval	b. Retry the command, or use a management PC with more reliable network communications to the MP
t write the Stable Complex uration Data. Cannot write the Partition Configuration Data Unable to update the Stable Complex Configuration Data.	The referenced data is inaccessible or was left in a locked state. See the AEL entry for more information.	If the data was left locked, use the command “parunlock” to unlock it. See the on-line help for the parunlock command, and the *HP System Partitions Guide* for more information.
Cannot lock Stable Complex Configuration Data. Unable to read lock for partition. Cannot lock Partition Configuration Data. Cannot lock cell data for cell <n>	The referenced data was locked when the command attempted to access it.	First retry the command. The data is normally locked only for short periods. If the data remains locked, use the command “parunlock” to unlock it. See the on-line help for the “parunlock” command and the *System Partitions Guide* for more information.
Cannot read <info> Unable to read <info> Unable to get <info> No information available for <component> <Component> information unavailable.	In most cases, these messages are caused by lost datagrams over an unreliable network connection. See the AEL entry for more information. <info> will be a identification of the specific data not available. <component> will be an identification of the specific component for which data was unavailable.	Retry the command, or use a management PC with a more reliable network connection to the target MP or nPartition. **NOTE:** This error may occur if **–w** and **–g** options are used in the same command. This condition should be reported by the parstatus as a syntax error because there is never a local partition when using the **–g** and **–h** option combination.
LED operation on <component> failed.	Attempted to turn on or off an LED that does not exist on the target complex. Only Superdome servers support all LEDs. Midrange partitionable servers, e.g. rx8620, do not have cabinet or I/O chassis LEDs. See the AEL entry to confirm this was the case.	Do not specify a non-existent LED.

Provider messages

The following messages will be found in Application Event Log entries. In most cases, additional amplifying information will follow the general message.

Message	Cause	Action
Operation failed.	Request could not be completed.	See additional information in AEL.
Firmware error.	System firmware failed to perform the requested operation.	
Service processor error.	MP firmware failed to perform requested operation.	
The power-on request could not be satisfied because an N- power condition would result.	There is insufficient system power to service a cell that was specified to be powered on.	Add additional power supplies or replace a defective power supply.
The power-on request could not be satisfied because an insufficient cooling condition would result.	There is insufficient system cooling to service a cell that was specified to be powered on	Add additional fan or blower units or replace a defective fan or blower.
Timed out waiting for a response.	Datagram was lost.	Retry command or use a management PC with a more reliable connection to the target MP or nPartition.
Insufficient privilege to perform the operation.	Requesting user does not have permission to perform the requested operation	Run the command as Administrator or “root”.
Invalid user name	Username specified in the request was not valid on the target nPartition.	Use a valid username.
Operation is only supported by the local operating system.	The requested operation can only be performed by a provider running on the nPartition. It cannot be performed through the MP.	Use the –u option with the command.
Operation is not supported by the firmware.	The system firmware does not support the requested operation.	Cannot perform the request on this target system. May require updating the system firmware on the target system.
Operation is not supported by either operating system or firmware.	Neither the local OS nor system firmware supports the requested operation.	Cannot perform the request on this target system. May require updating the OS or system firmware on the target system.
Operation is not supported by the provider.	The provider does not support the requested operation.	Update the provider to the most current revision.
Invalid parameter	Invalid data passed with the request, for example, an invalid cell id.	
The specified item does not exist.	The specified component does not exist, e.g. a cell that is not installed in the complex.	

The system interface version does not match that expected by the provider.	The version of IPMI on the target MP is unexpected. This is normally caused when the target platform has an MP that supports IPMI, but is not partitionable.	Specify a partitionable complex MP as the target of the operation.
The service processor does not support I/O expansion cabinets.	A request for data about an I/O expansion cabinet was requested on a platform that does not support them, e.g. rx7620.	Cannot perform the requested operation on this platform.
Operation is not supported by the platform.	A request was made that is supported by the platform. Generally, this would be caused by running a command intended for a later model of a system on an earlier model that does not support the feature.	Cannot perform the requested operation.
Locking or unlocking the target failed.	The target of the lock was already locked, or the lock was held by a different process.	Retry the command. If necessary, use the parunlock command to unlock the data.
Command processing resources are temporarily unavailable.	The MP is busy with another request.	Retry the command.
IPMI session error	Error in the IPMI communication between the provider and the MP.	Retry the command
No changes can be made because the profile is already in the process of being changed.	Another user has initiated a complex reconfiguration. Until the MP has completed, this configuration, no other can be performed.	Retry the command at a later time.
Locking or unlocking the target failed because the MP has target locked.	The MP has locked the requested data for internal use.	Retry the command at a later time.
The platform is not supported.	The target is not a partitionable complex.	
The system is not using a compatible version of IPMI.	The target of the operation is not a partitionable complex.	

Appendix C: Use of *wmiop* to locate problems

Wmiop.exe is installed in the %PEGASUS_HOME%\bin directory. Since this directory is added to the PATH during installation, wmiop can be executed from any directory. If not, that is the first indication that something is wrong, most likely that the PATH environment variable has not been correctly modified.

The syntax of the *wmiop* utility is as follows (an abbreviated usage message can be viewed from the command line by running "*wmiop*" with no options):

```
Usage:
 wmiop <cimoperation> [arg, ...]

Implemented operations (not case sensitive) are:
 getClass|gc <class>
 enumerateClassNames|ecn [ <class> ]
 getInstance|gi <class> [ list ]
 enumerateInstances|ei <class>
 enumerateInstanceNames|ein <class>
 getProperty|gp <class> { ask | list } [ <propnam> ]
 setProperty|sp <class> { ask | list } [ <propnam> [ <value> ] ]
 deleteClass|dc <class>
 createInstance|ci <class>
 modifyInstance|mi <class> [ list ]
 deleteInstance|di <class> [ list ]

Examples:
 wmiop ecn
 wmiop enumerateinstancenames Win32_OperatingSystem
 wmiop gi Win32_Process list
 wmiop ei Win32_ComputerSystem

Environment variables:
 CIM_NAMESPACE -- if not defined use root/cimv2
 CIM_HOST -- local connect if not defined
 CIM_PORT -- port number (default determined by CIM_NOSSL)
 CIM_NOSSL -- if defined, connect unencrypted to 5988, else 5989
 CIM_USER -- user
 CIM_PASSWORD – password

Notes:
```

```
- by setting CIM_NAMESPACE appropriately, instances of __Namespace
can
 be enumerated, created, and deleted.
- The CIM_NAMESPACE variable must be set to the correct and
desired
 namespace before running the WMIOP application.
- When an invalid classname is provided, the application will
abort its
 operation.
- It is not recommended redirect the WMIOP output to a file. Some
 operations require user input after the command line call and
these
 inputs may be omitted.
```

Test the WMI Mapper Installation

The following tests that the WMI Mapper files are installed correctly, and are accessible via the current system PATH.

Open a Command Prompt window and run the following command:

```
wmiop ei Win32_ComputerSystem
```

This command requests that WMI enumerate the instances of all known objects of type Win32_ComputerSystem. If the WMI Mapper is installed and operating correctly, then output similar to the following should result. The specific values will be different for each machine. If an error occurs, uninstall, then reinstall the WMI Mapper.

```
Instances of [Win32_ComputerSystem] (1 instances):


Instance of Win32_ComputerSystem:
{
 AdminPasswordStatus = 3
 AutomaticResetBootOption = TRUE
 AutomaticResetCapability = TRUE
 BootROMSupported = TRUE
 BootupState = "Normal"
 Caption = "FCTMARTIN"
 ChassisBootupState = 3
 CreationClassName = "Win32_ComputerSystem"
 CurrentTimeZone = -420
 DaylightInEffect = FALSE
 Description = "AT/AT COMPATIBLE"
 Domain = "DOMAIN-NAME"
 DomainRole = 3
 FrontPanelResetStatus = 3
 InfraredSupported = FALSE
 KeyboardPasswordStatus = 3
 Manufacturer = "Hewlett-Packard"
 Model = "HP Kayak PC"
 Name = "HOSTNAME"
 NetworkServerModeEnabled = TRUE
 NumberOfProcessors = 1
 OEMStringArray[•] = "SMBIOS 2.3 BIOS with HP DMI extensions "
 PauseAfterReset = -1
 PowerOnPasswordStatus = 3
 PowerState = 0
 PowerSupplyState = 3
 PrimaryOwnerName = "Joe Owner"
 ResetCapability = 1
 ResetCount = -1
 ResetLimit = -1
 Roles[•] = "LM_Workstation LM_Server NT Server_NT Backup_Browser
"
 Status = "OK"
 SystemStartupDelay = 30
 SystemStartupOptions[•] = ""Microsoft Windows 2000 Server"
/fastdetect "
 SystemStartupSetting = 0
 SystemType = "X86-based PC"
 ThermalState = 3
 TotalPhysicalMemory = 1341636608
 UserName = "DOMAIN-NAME\jowner"
 WakeUpType = 6
}
```

Test the WMI Mapper Service with HTTP Connections

The following will test that the WMI Mapper service is running and properly responding to client requests. Note that running the nPar commands with the –g option (to connect remotely to the Management Processor on the partitionable system) does *not* go through the WMI Mapper service, so this test does not apply for those cases.

The following test uses a basic HTTP connection to the service, which eliminates any possible SSL/certificate problems. By default, the WMI Mapper service is configured for HTTPS/SSL connections ONLY, therefore this test will not work without first reconfiguring the service for HTTP connections. See the installed file %PEGASUS_HOME%\ConfigREADME.txt for instructions on how to configure the service. To test the default configuration (HTTPS connections), skip to the next test, below.

Open a Command Prompt window and run the following commands:

```
set CIM_HOST=localhost
set CIM_USER=<domain\username>
set CIM_PASSWORD=<password for user, above>
set CIM_NOSSL=1
wmiop ei Win32_ComputerSystem
```

The output should be the same as the previous test. If an error occurs, ensure that the WMI Mapper service is started. If not start it and repeat the test. If it is running, uninstall, then reinstall the WMI Mapper.

If you see the following error:

Cannot connect to localhost:5988. Connection failed

The most likely cause is that the server is not configured for HTTP connections. As noted above, the default configuration is for HTTPS connections only. To configure the service for HTTP connections, open the %PEGASUS_HOME%\cimserver_planned.conf file and add/edit the following entry:

enableHttpConnection=true

Then Restart (or Stop then Start) the Pegasus WMI Mapper service from the Services control panel for the change to take effect.

Test the WMI Mapper Service with HTTPS Connections

The following will test that the WMI Mapper service is running and properly responding to client requests by secure HTTP. Note that running the nPar commands with the –g option (to connect remotely to the Management Processor on the partitionable system) does NOT go through the WMI Mapper service, so this test is N/A for those cases.

The following test uses HTTPS/SSL connections to the service, which assumes the default WMI Mapper configuration for HTTPS/SSL connections (see the installed file %PEGASUS_HOME%\ConfigREADME.txt for instructions on how to configure the service).

Open a Command Prompt window and run the following commands:

```
set CIM_HOST=localhost
set CIM_USER=<domain\username>
set CIM_PASSWORD=<password for user, above>
```

The current directory must be where the client.pem file resides (either the PEGASUS_HOME or the HP_SSL_SHARE directories):

```
cd %PEGASUS_HOME%
```

Finally, run the wmiop command:

```
wmiop ei Win32_ComputerSystem
```

The output should be the same as the previous test. If an error occurs, uninstall, then reinstall the WMI Mapper. If an SSL certificate problem is suspected, try deleting the entire %PEGASUS_HOME% and %HP_SSL_SHARE% directories after un-installing and before reinstalling. This will delete all installed certificates, causing the certificates to be re-generated during installation. Then follow the instructions for configuring SSL Shared Certificates from Appendix A.

Test Registration of the WMI nPar Provider

The following test ensures that the nPar Provider has been properly registered in WMI:

Open a Command Prompt window and run the following commands:

```
set CIM_NAMESPACE=root/cimv2/npar
wmiop ecn
```

The output should be as follows, indicating the nPar Provider is properly registered in WMI:

```
Classes in namespace [root/cimv2/npar]:
__SystemClass
 __NAMESPACE
 __Provider
  __Win32Provider
   HP_DecoupledProvider
 __ProviderRegistration
  __ObjectProviderRegistration
   __InstanceProviderRegistration
   __ClassProviderRegistration
  __PropertyProviderRegistration
  __MethodProviderRegistration
  __EventProviderRegistration
  __EventConsumerProviderRegistration
 __CIMOMIdentification
 __IndicationRelated
  __Event
   __ExtrinsicEvent
    __SystemEvent
     __EventDroppedEvent
```

```
      __EventQueueOverflowEvent
      __ConsumerFailureEvent
   __NamespaceOperationEvent
    __NamespaceCreationEvent
    __NamespaceDeletionEvent
    __NamespaceModificationEvent
   __ClassOperationEvent
    __ClassCreationEvent
    __ClassDeletionEvent
    __ClassModificationEvent
   __InstanceOperationEvent
    __InstanceCreationEvent
    __InstanceDeletionEvent
    __InstanceModificationEvent
   __TimerEvent
  __AggregateEvent
  __EventConsumer
  __EventFilter
  __FilterToConsumerBinding
  __EventGenerator
   __TimerInstruction
    __AbsoluteTimerInstruction
    __IntervalTimerInstruction
  __TimerNextFiring
__NotifyStatus
 __ExtendedStatus
__SecurityRelatedClass
 __NTLMUser9X
__PARAMETERS
__SystemSecurity
CIM_ManagedElement
 CIM_ManagedSystemElement
  CIM_LogicalElement
   HP_NParSlot
    HP_NParCellSlot
    HP_NParIOChassisSlot
   HP_NParCabinet
   HP_NParPowerCoolingDomain
   HP_NParPotentialErrorObject
```

```
        HP_NParComponent
         HP_NParCell
         HP_NParIOChassis
        HP_NParProfile
         HP_NParComplex
         HP_NParPartition
         HP_NParDynamicProfile
    HP_NParCellConnectedToIOChassis
    HP_NParComponentInSlot
     HP_NParIOChassisInSlot
     HP_NParCellInSlot
    HP_NParSlotInCabinet
     HP_NParCellSlotInCabinet
     HP_NParIOChassisSlotInCabinet
    HP_NParCellSlotInPartition
    HP_NParDomainInCabinet
    HP_NParLocalPartition
    HP_NParRemoteComplex
```

If an error occurs, or the output looks significantly different from the above, uninstall, then reinstall the nPar Provider, which will re-register the provider with WMI.

Test Operation of the WMI nPar Provider

This test ensures that the WMI nPar Provider is running and properly responding to client requests:

Open a Command Prompt window and run the following commands:

```
set CIM_NAMESPACE=root/cimv2/npar
wmiop ci HP_NParRemoteComplex
```

When prompted, enter the following information:

```
[ key ] string Address? <Management Processor hostname or IP>
string Password? <MP Admin password>
```

If successful, you should see the following message:

```
Instance [root/cimv2/npar:HP_NParRemoteComplex.Address="<mp
address>"] successfully created!
```

Otherwise, if you see the following error:

```
Error: [6] CIM_ERR_NOT_FOUND: The requested object could not be
found
```

This indicates that the nPar Provider is either not running, or not handling requests appropriately. Verify that the WMI nPar Provider service is started. If not, start it from the Services control panel, or reboot and repeat the test. If the service is started, uninstall, then reinstall the provider.