



System p  
Operations Guide for the  
Hardware Management Console  
and Managed Systems  
Version 7 Release 3.1.0

SA76-0085-00







System p

Operations Guide for the  
Hardware Management Console  
and Managed Systems  
Version 7 Release 3.1.0

SA76-0085-00

**Note**

Before using this information and the product it supports, read the information in “Notices” on page 319 and the *IBM Systems Safety Information* manual, G229-9054.

**First Edition (June 2007)**

This edition applies to IBM System p servers that contain the POWER6 processor and to all associated models.

© Copyright International Business Machines Corporation 2007. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

# Contents

<b>Figures</b> . . . . .	<b>xiii</b>
<b>Tables</b> . . . . .	<b>xv</b>
<b>Safety and environmental notices</b> . . . . .	<b>xvii</b>
<b>About this publication</b> . . . . .	<b>xxi</b>
How to send your comments . . . . .	xxi
<b>Chapter 1. Introduction to the Hardware Management Console</b> . . . . .	<b>1</b>
User interface style for the HMC . . . . .	1
Predefined user IDs and passwords. . . . .	2
Tasks and roles . . . . .	2
Starting the HMC. . . . .	3
What's new in HMC Version 7.3.1 . . . . .	4
Interface features . . . . .	4
POWER6 specific functions . . . . .	5
HMC Version 6 to HMC Version 7.3.1 task mappings. . . . .	6
Server and partition management . . . . .	6
Manage on demand activations . . . . .	9
Frame management. . . . .	11
Utilization data management . . . . .	11
System plans . . . . .	12
Licensed internal code maintenance . . . . .	12
HMC management . . . . .	13
Service applications. . . . .	14
DLPAR changes . . . . .	16
<b>Chapter 2. Using the Web-based user interface</b> . . . . .	<b>19</b>
Task bar . . . . .	20
Navigation pane. . . . .	21
Welcome . . . . .	21
Systems Management . . . . .	21
Servers . . . . .	21
Selecting a server . . . . .	22
Displaying server details . . . . .	24
Launching tasks for managed objects. . . . .	24
Partitions . . . . .	27
Displaying partition details . . . . .	29
Frames . . . . .	29
Custom Groups . . . . .	29
User-defined groups . . . . .	30
System Plans . . . . .	30
HMC Management . . . . .	31
Service Management . . . . .	33
Updates . . . . .	33
Work pane. . . . .	34
Working with Tables . . . . .	35
Selecting Rows . . . . .	35
Filtering . . . . .	35
Sorting . . . . .	35
Column configuration . . . . .	36
Views menu . . . . .	36
Status bar . . . . .	38

Status: Unacceptable . . . . .	38
Status: Attention LEDs. . . . .	39
Status: Serviceable Events . . . . .	39
Status Overview . . . . .	39
<b>Chapter 3. Systems Management - Servers . . . . .</b>	<b>41</b>
Properties . . . . .	41
Update Password . . . . .	42
Operations . . . . .	42
Power On . . . . .	43
Power Off . . . . .	43
LED Status . . . . .	43
Schedule Operations . . . . .	44
Advanced System Management (ASM) . . . . .	46
Utilization Data . . . . .	46
Rebuild. . . . .	46
Change Password . . . . .	47
Configuration . . . . .	47
Create Logical Partition . . . . .	47
System Plans . . . . .	48
Manage Custom Groups . . . . .	48
View Workload Management Groups. . . . .	48
Partition Availability Priority . . . . .	48
Manage System Profiles . . . . .	49
Manage Partition Data. . . . .	49
Connections . . . . .	51
Correcting a Connection Problem . . . . .	51
Correcting a No connection state for a managed system . . . . .	51
Correcting an Incomplete state for a managed system . . . . .	52
Correcting a Recovery state for a managed system . . . . .	53
Correcting an Error state for a managed system . . . . .	53
Correcting a Failed Authentication state for a managed system . . . . .	53
Correcting a new connection problem between the HMC and a managed system . . . . .	54
Hardware (Information) . . . . .	54
Adapters . . . . .	55
Host Ethernet Adapter (HEA) . . . . .	55
Host Channel Adapter (HCA) . . . . .	55
Virtual IO Adapters . . . . .	55
View RIO Topology. . . . .	56
Updates . . . . .	56
Serviceability . . . . .	56
Manage Serviceable Events . . . . .	57
Create Serviceable Event . . . . .	57
Reference Code History . . . . .	58
Control Panel Functions . . . . .	58
Hardware . . . . .	58
Add FRU . . . . .	58
Add Enclosure . . . . .	59
Exchange FRU . . . . .	59
Exchange Enclosure . . . . .	59
Remove FRU . . . . .	59
Remove Enclosure . . . . .	60
Power On/Off IO Unit . . . . .	60
Manage Dumps . . . . .	60
Collect VPD . . . . .	60
Edit MTMS . . . . .	61
FSP Failover . . . . .	61
Capacity on Demand . . . . .	61
Capacity Upgrade on Demand . . . . .	62
On/Off Capacity on Demand . . . . .	63
Trial Capacity on Demand . . . . .	63

Utility Capacity on Demand . . . . .	64
Reserve Capacity on Demand . . . . .	64
Advanced POWER Virtualization . . . . .	65
Enterprise Enablement. . . . .	66
Other Advanced Functions . . . . .	67
<b>Chapter 4. Systems Management - Partitions . . . . .</b>	<b>69</b>
Properties . . . . .	69
Change Default Profile . . . . .	69
Operations . . . . .	69
Activate . . . . .	70
Restart . . . . .	70
Shut Down . . . . .	70
Manage Attention LED . . . . .	71
Schedule Operations . . . . .	71
Delete . . . . .	72
Configuration . . . . .	73
Manage Profiles . . . . .	73
Manage Custom Groups . . . . .	73
Save Current Configuration . . . . .	73
Hardware (Information) . . . . .	74
Adapters . . . . .	74
Host Ethernet Adapter (HEA) . . . . .	74
Host Channel Adapter (HCA) . . . . .	74
Switch Network Interface. . . . .	74
Dynamic Logical Partitioning . . . . .	75
Processor . . . . .	75
Memory . . . . .	75
Physical Adapters . . . . .	75
Virtual Adapter . . . . .	76
Host Ethernet. . . . .	76
Console Window . . . . .	77
Serviceability . . . . .	77
Manage Serviceable Events . . . . .	78
Reference Code History . . . . .	78
Control Panel Functions . . . . .	78
<b>Chapter 5. Systems Management - Frames . . . . .</b>	<b>81</b>
Properties . . . . .	81
Update Password . . . . .	81
Operations . . . . .	82
Initialize . . . . .	82
Rebuild. . . . .	82
Change Password . . . . .	82
Power On/Off IO Unit . . . . .	82
Configuration . . . . .	83
Manage Custom Groups . . . . .	83
Connections . . . . .	83
Bulk Power Assembly (BPA) Status . . . . .	83
Reset . . . . .	84
Hardware (Information) . . . . .	84
View RIO Topology. . . . .	84
Serviceability . . . . .	85
Manage Serviceable Events . . . . .	85
Hardware . . . . .	85
Add FRU . . . . .	86
Add Enclosure . . . . .	86
Exchange FRU . . . . .	86
Exchange Enclosure . . . . .	86
Remove FRU . . . . .	87

Remove Enclosure . . . . .	87
----------------------------	----

## **Chapter 6. System Plans . . . . . 89**

View System Plan . . . . .	89
Create System Plan . . . . .	90
Deploy System Plan . . . . .	90
Export System Plan . . . . .	91
Import System Plan . . . . .	91
Remove System Plan . . . . .	91

## **Chapter 7. HMC Management tasks . . . . . 93**

Back up HMC Data. . . . .	93
Change Date and Time . . . . .	93
Change Language and Locale . . . . .	94
Change Network Settings. . . . .	94
Change User Interface Settings . . . . .	95
Change User Password . . . . .	96
Create Welcome Text . . . . .	96
Format Media . . . . .	96
Launch Guided Setup Wizard . . . . .	97
Launch Remote Hardware Management Console . . . . .	97
Lock HMC Screen . . . . .	97
Logoff or Disconnect . . . . .	98
Manage Certificates. . . . .	98
Manage Data Replication . . . . .	99
Manage Task and Resource Roles . . . . .	99
Manage User Profiles and Access. . . . .	100
Manage Users and Tasks . . . . .	101
Open 5250 Console . . . . .	101
Open Restricted Shell Terminal . . . . .	102
Remote Command Execution . . . . .	102
Remote Operation . . . . .	102
Remote Virtual Terminal. . . . .	102
Restore HMC Data . . . . .	102
Save Upgrade Data . . . . .	103
Schedule Operations . . . . .	103
Shut Down or Restart . . . . .	104
Test Network Connectivity . . . . .	104
Tip of the Day . . . . .	105
View HMC Events. . . . .	105
View Licenses . . . . .	105
View Network Topology. . . . .	106

## **Chapter 8. Service Management tasks. . . . . 107**

Create Serviceable Event . . . . .	107
Format Media . . . . .	107
Load Serviceable Events. . . . .	108
Manage Connection Monitoring . . . . .	108
Manage Customer Information . . . . .	108
Manage Dumps . . . . .	109
Manage eService Registration . . . . .	109
Manage Inbound Connectivity. . . . .	110
Manage Outbound Connectivity . . . . .	110
Manage POWER4 Service Agent . . . . .	111
Manage Remote Connections . . . . .	111
Manage Remote Support Requests . . . . .	111
Manage Serviceable Event Notification . . . . .	112
Manage Serviceable Events . . . . .	112
Manage Systems Call-Home . . . . .	112
Transmit Service Information . . . . .	113



<b>Chapter 9. Updates</b>	<b>115</b>
Update HMC	115
Managed System Updates	116
Change Licensed Internal Code for the current release.	117
Example: Change Licensed Internal Code for the Current Release	118
Upgrade Licensed Internal Code to a new release	121
Example: Upgrade Licensed Internal Code to a New Release	121
Flash Side Selection	124
Check system readiness	124
View system information	124
<b>Appendix A. HMC tasks and user roles/IDs</b>	<b>127</b>
<b>Appendix B. Remote operations</b>	<b>133</b>
Using a remote HMC.	134
Using a Web browser.	134
Using the HMC remote command line	135
Setting up secure script execution between SSH clients and the HMC	135
Enabling and disabling HMC remote commands	136
Web browser requirements	137
Preparing to use the Web browser	137
Logging on the HMC from a LAN connected Web browser	137
<b>Appendix C. Customizable data replication</b>	<b>139</b>
Peer-to-Peer replication	139
Master-to-Slave replication	141
Data replication	143
<b>Appendix D. HMC commands</b>	<b>145</b>
asmmenu.	145
bkconsdata	145
bkprofdata	146
chaccfg	147
chcod	148
chhmc.	149
chhmcusr.	151
chhwres	152
chkmedia.	159
chled	159
chlparutil.	160
chsacfg	161
chsvcevent	163
chsyscfg	164
chsyspwd	170
chsysstate	171
chusrtca	175
chvet	175
cpdump	176
cpsysplan	177
defsysplanres	178
deploysysplan	179
dump	180
getdump	181
getupgfiles	182
hmcshutdown	183
hmcwin	183
installios	183
logssh	185
lpar_netboot.	185
lpcfgop	186

lsaccfg . . . . .	187
lscod . . . . .	188
lsdump . . . . .	189
lshmc . . . . .	191
lshmcusr . . . . .	192
lshwinfo . . . . .	193
lshwres . . . . .	194
lsled . . . . .	198
lslic . . . . .	199
lslock . . . . .	201
lsparutil . . . . .	201
lsmediadev . . . . .	207
lsrefcode . . . . .	207
lssacfg . . . . .	209
lssvcevents . . . . .	209
lssyscfg . . . . .	211
lssysconn . . . . .	212
lssysplan . . . . .	213
lssysplanres . . . . .	214
lsvet . . . . .	214
migrcfg . . . . .	215
mkaccfg . . . . .	215
mkhmcusr . . . . .	216
mksyscfg . . . . .	217
mksysconn . . . . .	223
mksysplan . . . . .	224
mkvterm . . . . .	225
monhmc . . . . .	225
pedbg . . . . .	226
pesh . . . . .	227
rmaccfg . . . . .	227
rmhmcusr . . . . .	228
rmlock . . . . .	228
rmlparutil . . . . .	228
rmprofdata . . . . .	229
rmsyscfg . . . . .	229
rmsysconn . . . . .	230
rmsysplan . . . . .	232
rmsysplanres . . . . .	232
rmvterm . . . . .	232
rsthwres . . . . .	233
rstprofdata . . . . .	234
rstupgdata . . . . .	235
saveupgdata . . . . .	235
sendfile . . . . .	236
startdump . . . . .	237
updhmc . . . . .	238
updlc . . . . .	238
viosvrcmd . . . . .	242

## **Appendix E. Advanced Systems Management Interface (ASMI) . . . . . 243**

Connecting to a terminal . . . . .	243
Controlling the system power . . . . .	243
Controlling the system power using the ASMI . . . . .	243
Powering the system on and off . . . . .	243
Setting auto-power restart . . . . .	244
Performing an immediate power off . . . . .	245
Performing a system reboot . . . . .	245
Managing the Advanced System Management Interface (ASMI) . . . . .	246
ASMI requirements . . . . .	246
ASMI Authority Levels . . . . .	246

ASMI login restrictions . . . . .	247
Accessing the ASMI . . . . .	247
Accessing the ASMI using a Web browser . . . . .	247
Setting the IP address on your PC or mobile computer . . . . .	249
Accessing the ASMI using an ASCII terminal . . . . .	250
Setting up an ASMI login profile . . . . .	251
Changing ASMI passwords . . . . .	251
Retrieving ASMI login audits . . . . .	252
Changing the default language for the ASMI . . . . .	252
Updating installed languages . . . . .	252
Viewing system information . . . . .	253
Viewing vital product data . . . . .	253
Viewing persistent storage . . . . .	253
Viewing file systems . . . . .	254
Viewing system power control network trace . . . . .	254
Viewing progress indicator from previous boot . . . . .	254
Viewing progress indicator history . . . . .	255
Viewing real-time progress indicator . . . . .	255
Changing system configuration . . . . .	255
Changing system name . . . . .	255
Configuring I/O enclosures . . . . .	256
Changing the time of day . . . . .	256
Changing firmware update policy . . . . .	257
Updating firmware on IBM System p servers . . . . .	257
Enabling PCI error injection policy . . . . .	257
Configuring monitoring . . . . .	257
Removing HMC connection data . . . . .	258
Changing the interposer plug count . . . . .	258
Enabling I/O adapter memory allocation . . . . .	259
Deconfiguring hardware . . . . .	259
Setting deconfiguration policies . . . . .	259
Changing processor configuration . . . . .	259
Changing memory configuration . . . . .	260
Viewing deconfigured resources . . . . .	261
Clearing all deconfiguration errors . . . . .	261
Configuring virtual Ethernet environment settings . . . . .	261
Managing virtual I/O connectivity . . . . .	262
Setting the maximum number of virtual Ethernet switches . . . . .	262
Accepting firmware license agreement . . . . .	263
Running the floating point unit computation test . . . . .	263
Programming vital product data . . . . .	263
Setting the system brand . . . . .	263
Setting the system identifiers . . . . .	264
Setting the system enclosure type . . . . .	265
Changing service indicators . . . . .	265
Turning off system attention indicator . . . . .	265
Enabling enclosure indicators . . . . .	266
Changing indicators by location code . . . . .	266
Performing an LED test on the control panel . . . . .	267
Setting performance options . . . . .	267
Changing the logical memory block size . . . . .	267
Increasing the system memory page size . . . . .	268
Configuring network services . . . . .	268
Configuring network interfaces . . . . .	268
Configuring network access . . . . .	269
Debugging the virtual TTY . . . . .	269
Troubleshooting . . . . .	270
Troubleshooting problems in accessing the ASMI . . . . .	270
Troubleshooting the server using service aids . . . . .	271
Displaying error and event logs . . . . .	271
Enabling serial port snoop . . . . .	272

Initiating a system dump . . . . .	273
Initiating a service processor dump . . . . .	274
Initiating a partition dump . . . . .	275
Configuring a system port for call options. . . . .	275
Configuring your modem . . . . .	276
Configuring the call-home and call-in policy . . . . .	276
Testing the call-home policy . . . . .	278
Rebooting the service processor . . . . .	278
Restoring your server to factory settings . . . . .	278
Entering service processor commands . . . . .	279
Managing the control panel functions . . . . .	280
Physical control panel . . . . .	280
Accessing the control panel functions using the physical control panel . . . . .	281
Putting the physical control panel in manual operating mode . . . . .	281
Control panel function codes . . . . .	281
Primary control panel functions . . . . .	283
Function 01: Display selected IPL type, system operating mode, and IPL speed . . . . .	283
Function 02: Select IPL type, IPL speed override, system operating mode, and firmware mode . . . . .	283
Function 03: Restart IPL . . . . .	285
Function 04: Lamp test . . . . .	285
Function 05 to 06: Reserved . . . . .	286
Function 07: SPCN functions . . . . .	286
Function 08: Fast power off. . . . .	287
Functions 09 to 10: Reserved . . . . .	288
Function 11: SRC display (ASCII string) . . . . .	288
Function 12: SRC display (hex words 2-5) . . . . .	288
Function 13: SRC display (hex words 6-9) . . . . .	288
Functions 14 to 19: SRC display (callouts) . . . . .	289
Function 20: System type, model, feature code, and IPL type . . . . .	290
Customer-extended panel functions . . . . .	290
Function 21: Service tool initiation . . . . .	290
Function 22: Partition dump . . . . .	290
Functions 23 to 24: Reserved . . . . .	291
Functions 25 and 26: Service switches 1 and 2 . . . . .	291
Functions 27 to 29: Reserved . . . . .	291
Function 30: Service processor IP address and port location . . . . .	291
Functions 31 to 33: Reserved . . . . .	291
Function 34: Retry partition dump . . . . .	291
Functions 35 to 41: Reserved . . . . .	291
Function 42: Platform dump . . . . .	291
Function 43: Service processor dump . . . . .	292
Functions 44 to 54: Reserved . . . . .	292
Function 55: View and change platform dump data . . . . .	292
Functions 56 to 62: Reserved . . . . .	294
Function 63: Display system status SRCs . . . . .	294
Function 64: Display diagnostic status SRCs . . . . .	294
Functions 65 to 70: Not applicable . . . . .	295
Functions 71 to 99: Reserved . . . . .	295
Values for IPL types, system operating modes, and speeds . . . . .	295
Managing the system management services . . . . .	296
Starting the system management services . . . . .	296
Using the system management services. . . . .	297
Power-on self-test keys . . . . .	308
Collecting reference codes and system information . . . . .	309
Using the control panel to collect reference codes and system information . . . . .	309
Using AIX tools to collect reference codes and system information . . . . .	310
Supporting diagnostics . . . . .	311
Running the online and stand-alone diagnostics . . . . .	311
Running the online diagnostics . . . . .	311
Running the online diagnostics in service mode . . . . .	311
Running the online diagnostics in maintenance mode . . . . .	312

Running the online diagnostics in concurrent mode . . . . .	312
Running stand-alone diagnostics . . . . .	313
Running stand-alone diagnostics from CD. . . . .	313
Performing a slow boot . . . . .	315
Using the control panel to perform a slow boot . . . . .	315
Using the ASMI menus to perform a slow boot . . . . .	315
Contacting IBM service and support. . . . .	316
<b>Appendix F. Accessibility features . . . . .</b>	<b>317</b>
<b>Notices . . . . .</b>	<b>319</b>
Trademarks . . . . .	320
Electronic emission notices . . . . .	321
Class A Notices. . . . .	321
Terms and conditions. . . . .	324
<b>Index . . . . .</b>	<b>325</b>



---

## Figures

1. HMC pre-login window. . . . .	3	13. Work pane table . . . . .	35
2. HMC login window . . . . .	4	14. Views menu for servers . . . . .	37
3. Web-based user interface HMC workplace window. . . . .	20	15. Views menu for user-defined custom groups	38
4. Task bar. . . . .	21	16. Status bar . . . . .	38
5. Systems Management servers window . . .	22	17. Status overview . . . . .	40
6. Capacity On Demand attributes. . . . .	24	18. Remote Operation Configuration . . . . .	133
7. Tasks pad . . . . .	25	19. Configure customizable data replication window - example 1 . . . . .	140
8. Context menu. . . . .	26	20. Configure customizable data replication window - example 2 . . . . .	142
9. Tasks menu . . . . .	27	21. Connection for model 570 . . . . .	250
10. Partitions work pane . . . . .	28	22. 570 control panel . . . . .	280
11. System Plans . . . . .	31		
12. Updates. . . . .	34		





## Tables

1. Server management tasks . . . . .	6	22. Primary and customer-extended control panel (32-character) function codes . . . . .	281
2. Partition management tasks . . . . .	7	23. Function 01 on systems without OS IPL enabled . . . . .	283
3. Manage on demand activations . . . . .	9	24. Function 02: Select IPL type, system operating mode, and firmware IPL mode on powered-on systems . . . . .	284
4. Frame management . . . . .	11	25. Function 02: Select IPL type, system operating mode, system IPL speed, and firmware IPL mode on powered-off systems . . . . .	284
5. Utilization data management. . . . .	12	26. SPCN functions in function 07 . . . . .	286
6. System plans . . . . .	12	27. Function 14: FRU callout display selection sequence . . . . .	289
7. Licensed Internal Code Maintenance . . . . .	13	28. Function 15: Procedure callout display selection sequence . . . . .	289
8. HMC management . . . . .	14	29. Function 22: Initiate a partition dump . . . . .	290
9. Service applications . . . . .	14	30. Function 30: Service processor IP address and port location . . . . .	291
10. HMC Management and Service Management tasks and default user roles . . . . .	127	31. Function 42: Initiate a platform dump . . . . .	292
11. Systems Management tasks performed on managed objects and default user roles . . . . .	131	32. Function 43: Initiate a service processor dump . . . . .	292
12. Ports used by a Remote HMC for Communications . . . . .	134	33. Function 55: View the platform dump data . . . . .	293
13. Ports used by a Web browser for communications to the HMC . . . . .	134	34. Function 55: Change the platform dump data . . . . .	293
14. PC or mobile computer network configuration information . . . . .	248	35. Function 63: Display system status SRCs . . . . .	294
15. Default user IDs and passwords for the Web interface . . . . .	248	36. Function 63: Display diagnostic status SRCs . . . . .	294
16. Fields and values for network configuration . . . . .	249	37. Operating system IPL types. . . . .	295
17. Default settings for the diagnostic programs . . . . .	251	38. System operating mode values. . . . .	295
18. Default user IDs and passwords for the Web interface . . . . .	251	39. IPL speeds . . . . .	296
19. System brand values . . . . .	264	40. Firmware IPL types . . . . .	296
20. Troubleshooting problems when trying to access the ASMI through a Web browser . . . . .	270	41. SMS menus and descriptions . . . . .	298
21. Error log types . . . . .	272		



---

## Safety and environmental notices

Safety notices may be printed throughout this guide:

- **DANGER** notices call attention to a situation that is potentially lethal or extremely hazardous to people.
- **CAUTION** notices call attention to a situation that is potentially hazardous to people because of some existing condition.
- **Attention** notices call attention to the possibility of damage to a program, device, system, or data.

### World Trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the U.S. English source. Before using a U.S. English publication to install, operate, or service this product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the U.S. English publications.

### German safety information

Das Produkt ist nicht für den Einsatz an Bildschirmarbeitsplätzen im Sinne § 2 der Bildschirmarbeitsverordnung geeignet.

### Laser safety information

IBM® System p™ servers can use I/O cards or features that are fiber-optic based and that utilize lasers or LEDs.

#### Laser compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

#### CAUTION:

This product might contain one or more of the following devices: CD-ROM drive, DVD-ROM drive, DVD-RAM drive, or laser module, which are Class 1 laser products. Note the following information:

- Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.
- Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure.

(C026)

#### CAUTION:

Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

#### CAUTION:

This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

**CAUTION:**

Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following information: laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam. (C030)

**Product recycling and disposal**

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM product recycling offerings can be found on IBM's Internet site at <http://www.ibm.com/ibm/environment/products/prp.shtml>.

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM <http://www.ibm.com/ibm/environment/products/prp.shtml>.



EU Only

**Note:** This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable throughout the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

**Battery return program**

This product may contain sealed lead acid, nickel cadmium, nickel metal hydride, lithium, or lithium ion battery. Consult your user manual or service manual for specific battery information. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to <http://www.ibm.com/ibm/environment/products/batteryrecycle.shtml> or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM Equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426-4333. Please have the IBM part number listed on the battery available prior to your call.

For Taiwan: Please recycle batteries.



For the European Union:



**Note:** This mark applies only to countries within the European Union (EU).

Batteries or packaging for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a chemical symbol for the metal concerned in the battery (Pb for lead, Hg for mercury and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to the potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

For California: Perchlorate Material - special handling may apply. See [www.dtsc.ca.gov/hazardouswaste/perchlorate](http://www.dtsc.ca.gov/hazardouswaste/perchlorate).

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5 Chapter 33. Best Management Practices for Perchlorate Materials. This product/part may include a lithium manganese dioxide battery which contains a perchlorate substance.

## **IBM Cryptographic Coprocessor Card Return Program**

The following information applies only for systems originally sold prior to July 1, 2006:

This machine may contain an optional feature, the cryptographic coprocessor card, which includes a polyurethane material that contains mercury. Please follow local ordinances or regulations for disposal of this card. IBM has established a return program for certain IBM Cryptographic Coprocessor Cards. More information can be found at <http://www.ibm.com/ibm/environment/products/prp.shtml>.



---

## About this publication

This publication helps users to understand how to use the Hardware Management Console (HMC), describes the tasks you can use on the console, and how to navigate using the web-based user interface.

This guide is available in portable document format (PDF) to view or print from **Resource Link** (<http://www.ibm.com/servers/resourcelink>). It is also available as an online document and can be viewed from the Hardware Management Console.

**Note:** The HMC user interface windows represented in this document are general samples. They may or may not represent the exact windows that are displayed for your user ID or version.

For information about the accessibility features of this product, for users who have a physical disability, see Appendix F, “Accessibility features,” on page 317.

---

## How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information. If you have any comments about this publication, send your comments using Resource Link™ at <http://www.ibm.com/servers/resourcelink>. Click **Feedback** on the navigation pane. Be sure to include the name of the book, the form number of the book, and the specific location of the text you are commenting on (for example, a page number or table number).





---

# Chapter 1. Introduction to the Hardware Management Console

This chapter briefly describes some of the concepts and functions of the Hardware Management Console (HMC) and introduces the user interface that is used for accessing those functions.

The HMC is a system that controls managed systems, logical partitions, Capacity on Demand (CoD), and updates. To provide flexibility and availability, you can implement HMCs as a local HMC or a redundant HMC.

## Local HMC

A local HMC is an HMC that is physically located close to the system it manages and is connected by either a private or public network. An HMC in a private network is a DHCP server for the service processors of the systems it manages. An HMC may also manage a system over an open network, where the managed system's service processor IP address has been assigned manually using the Advanced System Management Interface (ASMI).

## Remote HMC

A remote HMC is an HMC that is not physically located near its managed systems. This could be in another part of the same room or data center, in another building, or even on another site. Typically, a remote HMC would be attached to its managed servers via a public network, but configurations with a remote HMC attached to a private network are also possible. Prior to HMC version 7, at least one local HMC was required. With Version 7, any or all HMCs may be remote.

## Redundant HMC

A redundant HMC manages a system that is already managed by another HMC. When two HMCs manage one system, they are peers, and each can be used to control the managed system. One HMC can manage multiple managed systems, and each managed system can have two HMCs. If both HMCs are connected to the server using private networks, each HMC must be a DHCP server set up to provide IP addresses on two unique, nonroutable IP ranges.

The IBM Deskside HMC (7042-C06) and Rack-mounted HMC (7042-CR4) provide dedicated workstations designed to allow you to configure and manage POWER5, POWER5+, and POWER6 processor-based servers. One HMC can manage multiple servers, and dual HMCs can provide redundant support by managing the same system. To help ensure consistent function for all 7042 HMC models, each HMC is shipped preloaded with the Hardware Management Console Licensed Machine Code Version 7 (#0962).

The Hardware Management Console Licensed Machine Code Version 7 (#0962) may also be ordered via MES for 7310 HMCs for environments that may include POWER5, POWER5+, and POWER6 processor-based servers. Version 7 is not available for the 7315 HMCs.

---

## User interface style for the HMC

This HMC uses a Web-based user interface. This interface uses a tree style navigation model providing hierarchical views of system resources and tasks using drill-down and launch-in-context techniques to enable direct access to hardware resources and task management capabilities. It provides views of system resources and provides tasks for system administration.

See Chapter 2, "Using the Web-based user interface," on page 19 for detailed information on how to use this HMC interface.

You also have the option of using the HMC Command Line Interface (CLI). See the *Command Line Support* education module (<http://www.ibm.com/servers/resourceink/lib03030.nsf/page>) for information on how to use the command line interface and see Appendix D, "HMC commands," on page 145 for descriptions of all the commands you can use to perform the HMC and server tasks.

---

## Predefined user IDs and passwords

Predefined user IDs and passwords are included with the HMC. It is imperative to your system's security that you change the hscroot predefined password immediately.

The following predefined user IDs and passwords are included with the HMC:

User ID	Password	Purpose
hscroot	abc123	The hscroot user ID and password are used to log in to the HMC for the first time. They are case-sensitive and can only be used by a member of the super administrator role.
root	passw0rd	The root user ID and password are used by the service provider to perform maintenance procedures. They cannot be used to log in to the HMC.

---

## Tasks and roles

Each HMC user can be a member of a different role. Each of these roles allows the user to access different parts of the HMC and perform different tasks on the managed system. HMC roles are either predefined or customized.

The roles discussed in this section refer to HMC users; operating systems running on logical partitions have their own set of users and roles. When you create an HMC user, you must assign that user a task role. Each task role allows the user varying levels of access to tasks available on the HMC interface. For more information about the tasks each HMC user role can perform, see Appendix A, "HMC tasks and user roles/IDs," on page 127.

You can assign managed systems and logical partitions to individual HMC users. This allows you to create a user that has access to managed system A but not to managed system B. Each grouping of managed resource access is called a managed resource role. To learn more about managed resource roles and how to create them, see "Manage Task and Resource Roles" on page 99.

The **predefined** HMC roles, which are the default on the HMC, are as follows:

<b>hmcoperator</b>	Operator	The operator is responsible for daily system operation.
<b>hmcsuperadmin</b>	Super Administrator	The super administrator acts as the root user, or manager, of the HMC system. The super administrator has unrestricted authority to access and modify most of the HMC system.
<b>hmcpe</b>	Product Engineer	A product engineer assists in support situations, but cannot access HMC user management functions. To provide support access for your system, you must create and administer user IDs with the product engineer role.
<b>hmcservicerep</b>	Service Representative	A service representative is an employee who is at your location to install, configure, or repair the system.

You can create **customized** HMC roles by modifying predefined HMC roles. Creating customized HMC roles is useful for restricting or granting specific task privileges to a certain user. For more information about creating customized HMC roles, see “Manage Task and Resource Roles” on page 99.

---

## Starting the HMC

First, turn on the HMC by setting both the display and system unit to the *On* position. The initialization window, which includes the copyright information, is displayed.

When initialization is complete, the pre-login window is displayed as shown in Figure 1.

**Note:** The pre-login window contains the link to log in to the HMC application, the ability to view the online help information, and the summarized status information for the HMC. You will need to log in to view the status information.

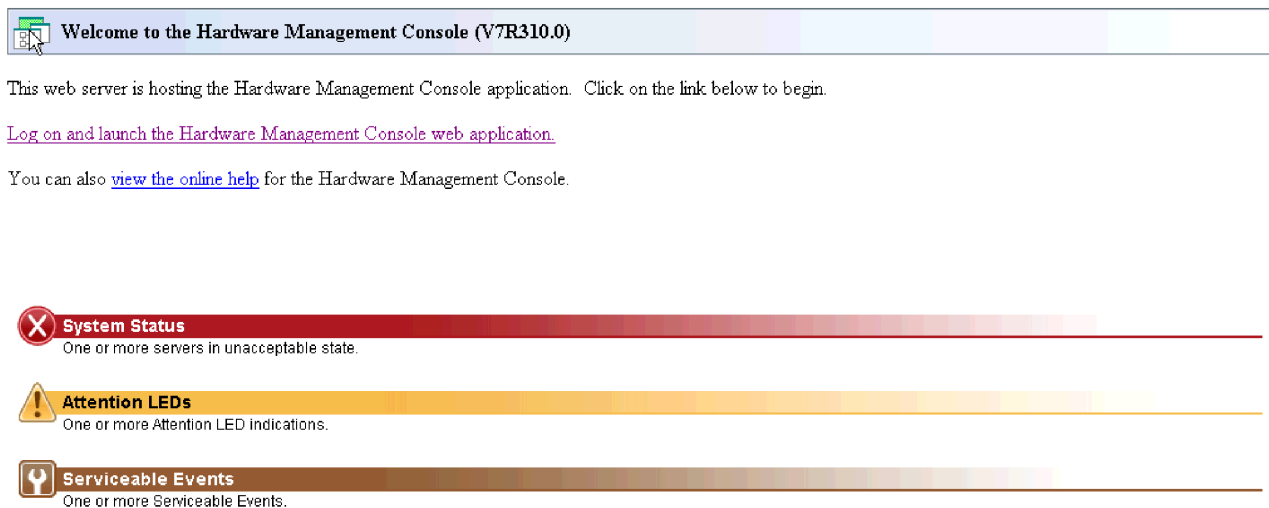



Figure 1. HMC pre-login window

To log in to the HMC, click **Log on and launch the Hardware Management Console web application.** from the pre-login window.

The Logon window is displayed as shown in Figure 2 on page 4.

---

 **Hardware Management Console (V7R310.0) Logon**

Please enter a userid and password below and click "Logon".

userid:

Password:

Figure 2. HMC login window

To log in, enter the user ID and password combination assigned to you. Then click **Logon**.

**Note:** If you previously disconnected from your session, the **Choose a Disconnected Session** window is displayed, select the session you want to reconnect to and click **Reconnect**.

After you log in, the HMC workplace window is displayed and, if enabled, the **Tip of the Day** window appears. For more information, see “Tip of the Day” on page 105.

The HMC workplace window allows you to work with tasks for your console and managed systems. Not all tasks are available for each user ID. The user role assigned to your user ID determines what tasks you are able to perform. For example, if you are assigned a user ID with the operator role, you will have access to all the tasks that have *operator* access. See Appendix A, “HMC tasks and user roles/IDs,” on page 127 for a listing of all tasks and the user roles for which the tasks are available.

If at any time you do not know or remember what user ID you are currently logged in to the HMC, look at the task bar on the top of the Welcome page or you can open the **HMC Management** node in the navigation pane, then select the **Manage Users and Tasks** task from the work pane (see “Manage Users and Tasks” on page 101 for more information).

---

## What’s new in HMC Version 7.3.1

This section highlights some of the new features and functions that can be found on the Version 7.3.1. Hardware Management Console and the POWER6 platform. You can also click **HMC Readme** from the HMC workplace Welcome pane for more information.

### Interface features

The following new Interface features include:

#### Web-based user interface:

The HMC User Interface (UI) has changed from a Java Swing implementation to a standard HTML (Web browser) implementation. The primary implication is that there no longer is a requirement to download a separate WebSM client to remotely connect to the HMC. When the HMC has been enabled to accept remote connections, any supported Web browser (i.e. IE 6.0+ or Firefox 1.5.2.0+) can be pointed at the HMC and used as the remote console.

The new UI also provides greater flexibility in how data is represented for managed systems and partitions through the sorting and filtering functions. In addition, custom groups can be created to provide essentially any structure the administrator wishes to construct over the managed objects (servers, frames, and partitions). For more information, see Chapter 2, “Using the Web-based user interface,” on page 19.

### Status bar

This feature provides quick visual feedback of the overall system status, including serviceable events and System Attention indicators. For more information, see “Status bar” on page 38.

### User task management

This task displays all of the users that are currently logged on to the HMC and which tasks they are running. A user with **hmcsuperadmin** privileges can cancel the running tasks of other users and may also logoff other users on the system. For more information, see “Manage Users and Tasks” on page 101.

### Disconnect/Logoff

This feature allows a user to either logoff of the HMC or disconnect temporarily. When a user chooses the logoff option all of the currently running task for that user are terminated, however if a user chooses the disconnect option all currently running tasks for that continue to run without interruption. When that user logs back into the HMC they will have the option of returning (reconnecting) to that previously disconnected session or starting a new session. For more information, see “Logoff or Disconnect” on page 98.

### Test Network Connectivity

This task allows a user to view network diagnostic information for the HMC. The task provides an interface to ping other IP addresses or hostnames and view various network protocol settings. For example, the routing information for the HMC can be accessed using this task. For more information, see “Test Network Connectivity” on page 104.

### Manage Data Replication

This task enables or disables customized data replication. Customized data includes the following HMC configuration settings: Customer information data, user defined custom group data, modem configuration data, and outbound connectivity data. For more information, see “Manage Data Replication” on page 99.

## POWER6 specific functions

The following new POWER6 specific functions include:

### Host Ethernet Adapters:

Host Ethernet Adapters (Integrated Virtual Ethernet Adapters) are a new feature of the POWER6 platform. They provide the ability to allow multiple partitions to share a single physical Ethernet adapter. For more information, see “Host Ethernet Adapter (HEA)” on page 55.

### Partition Availability Priority

Partition availability priority is used in the case of processor failure. If a processor fails on a logical partition, and there are no unassigned or spare processors available on the managed system, the logical partition is assigned a replacement processor from a logical partition with a lower partition-availability priority. For more information, see “Partition Availability Priority” on page 48.

### Utility CoD for Processors

Utility CoD is essentially a replacement for the POWER 5 Reserve CoD function. Utility CoD tracks processor usage on a processor-minute basis. Like Reserve CoD, Utility CoD provides additional processor capacity for uncapped partitions assigned to the shared pool. Utility CoD capacity is only charged when a partition exceeds its assigned maximum capacity. For more information, see “Utility Capacity on Demand” on page 64.

### LPAR support for Barrier Synchronization Register (BSR)

The HMC will allow BSR assignment to LPAR types (such as, AIX, Linux, VIOS, i5/OS). The BSR attributes are displayed from the **Properties** task if the managed system is BSR capable. Use the **Properties** task for managed systems to set the capability. See “Properties” on page 41 for more information.

### Dump facility enhancements

These enhancements will reduce unplanned customer outages and improve platform

serviceability, by eliminating unneeded and duplicate hardware data from platform system dump, and moving all formatting of dump data to the post-collection analysis phase. This improves dump runtime performance and frees up FSP control store to allow more problem-specific hardware data to be collected. See “Manage Dumps” on page 109 for more information.

#### **Shared pool usage of dedicated capacity**

This feature provides the ability for partitions that normally run as dedicated processors partitions to contribute unused processor capacity to the shared processor pool. You can use some of the capacity this is formerly locked up in dedicated processor partitions to satisfy peak needs for the shared processor pool without restoring to using utility on-demand processors. Use the **Properties** task for partitions to set the capability. See “Properties” on page 69 for more information.

#### **Virtual Server (VS) model instrumentation**

This feature provides a common interface for server system management. It is the first phase of work for the HMC to provide the standardized VS model as the common interface for third parties to manage the server system and their hardware resources.

#### **Electronic Error Reporting**

This feature allows automatic call-home for i5/OS partitions. Use the **Properties** task for partitions to enable the option to electronically report errors that cause partition termination or required attention. See “Properties” on page 69 for more information.

#### **Partition processor compatibility mode**

This features defines the compatibility of a partition with the given processor architecture (processor mode). Use the **Properties** task for partitions to set the capability. See “Properties” on page 69 for more information.

## **HMC Version 6 to HMC Version 7.3.1 task mappings**

This information is used to aid HMC Version 6 users in locating the equivalent WebSM HMC task in the new Web-based HMC UI. Each navigation node in the WebSM UI is broken out to a table listing the location of the WebSM task on the left hand side and then indicating the new location for the task in the Web UI on the right hand side. Where possible, a non-targeted task has been moved (no object is selected to perform the task on ) to a targeted task (a objected is selected first) to help make tasks readily available. These tasks are referred to as “Targeted” tasks and are denoted with a **T[S-System, P-Partition, H-HMC, U-Updates, SP-System Plan]**, if a target is not listed then HMC is the assumed target.

**Note:** These tables are listing tasks from a WebSM perspective and mapping to the Web UI. New tasks for POWER6 machine’s functionality are not covered here.

### **Server and partition management**

The tasks for managed system and partitions have been grouped into consistent categories for each of the object types. Instead of one long list of tasks when you select an object, there is categories of tasks to choose from. The major change in the overall Server and Partition management approach is that System Profiles and Partition Profiles are now viewed and worked with in their own separate tasks. They are no longer displayed in the container underneath a system or partition, respectively. The new task used to manage System Profiles is found by selecting a server then **Configuration > Manage System Profiles** and the new task used to manage Partition Profiles is found by selecting a partition then **Configuration > Manage Profiles**. Each of those two tasks allows you to view and work with the profiles created on the system and contain the same tasks as the WebSM UI had provided when either one of those object types were selected.

*Table 1. Server management tasks*

Task Name	Task Description	New Location
<b>Properties</b>	Display and edit managed system properties	Properties



Table 1. Server management tasks (continued)

Task Name	Task Description	New Location
<b>Reset or Remove Connection</b>	Remove or reset the HMC connection to the managed system	Connections > Reset or Remove Connection
<b>Create</b>		
Logical Partition	Create a logical partition	Configuration > Create Logical Partition >
System Profile	Create a system profile	Configuration > Manage System Profiles > New
System Plan	Create a system plan	Configuration > System Plans > Create
<b>Manage On Demand Activations</b> (See “Manage on demand activations” on page 9)	See the section below	See “Manage on demand activations” on page 9
<b>Adapters</b>		
GX+	View the properties of the GX+ adapters installed	Removed for V7.3.1.0
<b>Power On</b>	Power on the managed system	Operations > Power On
<b>Power Off</b>	Power off the managed system	Operations > Power Off
<b>Disconnect Another HMC</b>	Removes another HMC’s lock on the managed system	Connections > Disconnect Another HMC
<b>Profile Data</b>		
Restore	Restore a profile data backup file	Configuration > Manage Profile Data > Restore
Initialize	Clear the LPAR and profile configuration on the managed system	Configuration > Manage Profile Data > Initialize
Backup	Backup the LPAR and profile configuration on the managed system	Configuration > Manage Profile Data > Backup
Remove	Remove a configuration backup file	Configuration > Manage Profile Data > Remove
<b>Rebuild Managed System</b>	Rebuild the HMC’s internal representation of the managed system	Operations > Rebuild
<b>Recover Partition Data</b>	Rebuild the HMC’s internal representation of the managed system	Recover Partition Data
<b>Update Managed System Password</b>	Update the HMC passwords for the managed system	Operations > Change Password
<b>Workload Management Groups</b>	View the workload management groups	Configuration > View Workload Management Groups
<b>Status</b>	FSP connection status	Connections > Service Processor Status
<b>Add Managed System</b>	Add another managed system to the HMC	Connections > Add Managed System

Table 2. Partition management tasks

Task Name	Task Description	New Location
<b>Properties</b>	View or edit the partition properties	Properties
<b>Create Profile</b>	Create a profile for the partition	Configuration > Manage Profiles > New
Add	Add physical adapters to the partition	Dynamic Logical Partitioning > Physical Adapters > Add

Table 2. Partition management tasks (continued)

Task Name	Task Description	New Location
<b>Dynamic Logical Partitioning</b>		
Physical Adapter Resources:		
Remove	Remove physical adapters from the partition	Dynamic Logical Partitioning > Physical Adapters > Move/Remove
Move	Move physical adapters to another partition	Dynamic Logical Partitioning > Physical Adapters > Move/Remove
Processor Resources:		
Add	Add processors to the partition	Dynamic Logical Partitioning > Processor > Add/Remove
Remove	Remove processors to the partition	Dynamic Logical Partitioning > Processor > Add/Remove
Move	Move processors to the partition	Dynamic Logical Partitioning > Processor > Move
Memory Resources:		
Add	Add memory to the partition	Dynamic Logical Partitioning > Memory > Add/Remove
Remove	Remove memory to the partition	Dynamic Logical Partitioning > Memory > Add/Remove
Move	Move memory to the partition	Dynamic Logical Partitioning > Memory > Move
<b>Virtual I/O</b>		
SCSI Adapters	View the virtual SCSI adapter's connections configured for the partition	Hardware (Information) > Virtual I/O Adapters > SCSI
Ethernet Adapters	View the virtual Ethernet adapter's connections configured for the partition	Hardware (Information) > Virtual I/O Adapters > Ethernet
<b>Restart Partition</b>	Restart the partition	Operations > Restart
<b>Shutdown Partition</b>	Shutdown the partition	Operations > Shut Down
<b>Save</b>	Save the current LPAR configuration to a new profile	Configuration > Save Current Configuration
<b>Activate</b>	Activate the partition	Operations > Activate
<b>Change Default Profile</b>	Change the default profile for the partition	Change Default Profile
<b>Virtual I/O Server Command</b>	Issue a command to the Virtual I/O Server partition	Operations > Perform VIOS Command
<b>Open Terminal Window</b>	Open a virtual terminal to the partition	Console Window > Open Terminal Window
<b>Open Shared 5250 Console</b>	Open a shared 5250 console to the partition	Console Window > Open Shared 5250 Console
<b>Open Dedicated 5250 Console</b>	Open a dedicated 5250 console to the partition	Console Window > Open Dedicated 5250 Console
<b>Close Terminal Window</b>	Close the virtual terminal window connection to the partition	Console Window > Close Terminal Connection
<b>Delete</b>	Delete the partition	Operations > Delete



Task Name	Task Description	New Location
<b>Profile Tasks</b>		<b>* All profile tasks are located in the Manage Profiles task which is available when a partition is selected in the main UI.</b>
Copy	Copy the profile	Configuration > Manage Profiles > Copy
Properties	View or edit the profile properties	Configuration > Manage Profiles > Edit
Delete	Delete the profile	Configuration > Manage Profiles > Delete
Activate	Activate the profile	Configuration > Manage Profiles > Activate

Task Name	Task Description	New Location
<b>System Profile Tasks</b>		<b>* All profile tasks are located in the Manage System Profiles task which is available when a managed system is selected in the main UI.</b>
Validate	Validate the system profile configuration information	Configuration > Manage System Profiles > Validate
Copy	Copy the system profile	Configuration > Manage System Profiles > Copy
Properties	View or edit the system profile properties	Configuration > Manage System Profiles > Edit
Delete	Delete the system profile	Configuration > Manage System Profiles > Delete
Activate	Activate the system profile	Configuration > Manage System Profiles > Activate

## Manage on demand activations

Manage On Demand Activations has more categorization of tasks and is located under **Capacity On Demand (CoD)**. The different CoD types are separated out from each other and placed in their own category. For instance, instead of having one task called “Capacity Settings” that contained all of the information for the different CoD types (which retrieving all of that information to view one particular type is not the most efficient approach for performance), now each type of CoD has its own Capacity Settings task. This new categorization also allows you to easily see all of the tasks that are associated with each CoD type.

*Table 3. Manage on demand activations*

Task Name	Task Description	New Location
<b>Capacity On Demand</b>		
<b>Enter CoD Code</b>	Enter a CoD code	Capacity On Demand > Enter CoD Code
<b>Processor</b>		
Capacity Settings	View overall system processor capacity settings	Capacity On Demand > Processor > View Capacity Settings
On/Off CoD	View On/Off CoD processor settings	Capacity On Demand > Processor > On/Off CoD > View Capacity Settings

Table 3. Manage on demand activations (continued)

Task Name	Task Description	New Location
Reserve CoD	View Reserve CoD processor settings	Capacity On Demand > Processor > Reserve CoD > View Capacity Settings
Trial CoD	View Trial CoD processor settings	Capacity On Demand > Processor > Trial CoD > View Capacity Settings
Manage On/Off CoD	Manage On/Off CoD processors	Capacity On Demand > Processor > On/Off CoD > Manage
Manage Reserve CoD	Manage Reserve CoD processors	Capacity On Demand > Processor > Reserve CoD > Manage
Stop Trial CoD	Stop Trial CoD processors	Capacity On Demand > Processor > Trial CoD > Stop
Shared Processor Utilization	View the shared processor utilization data for the system	Capacity On Demand > Processor > Reserve CoD > View Shared Processor Utilization
<b>Memory</b>		
Capacity Settings	View overall system memory capacity settings	Capacity On Demand > Memory > View Capacity Settings
On/Off CoD	View On/Off CoD memory settings	Capacity On Demand > Memory > On/Off CoD > View Capacity Settings
Trial CoD	View Trial CoD memory settings	Capacity On Demand > Memory > Trial CoD > View Capacity Settings
Manage On/Off CoD	Manage On/Off CoD memory	Capacity On Demand > Memory > On/Off CoD > Manage
Stop Trial CoD	Stop Trial CoD memory	Capacity On Demand > Memory > Trial CoD > Stop
Show History Log	Displays the CoD history log	Capacity On Demand > View History Log
Show Code Information	Displays the information used to generate CoD codes by CoD type	Capacity On Demand > Processor > CUoD > View Code Information  Capacity On Demand > Processor > On/Off CoD > View Code Information  Capacity On Demand > Processor > Trial CoD > View Code Information  Capacity On Demand > Processor > Reserve CoD > View Code Information  Capacity On Demand > Memory > CUoD > View Code Information  Capacity On Demand > Memory > On/Off CoD > View Code Information  Capacity On Demand > Memory > Trial CoD > View Code Information
Show Billing Information	Displays the billing information for On/Off CoD	Capacity On Demand > Processor > On/Off CoD > View Billing Information  Capacity On Demand > Memory > On/Off CoD > View Billing Information

Task Name	Task Description	New Location
<b>Virtualization Engine Technologies</b>		Capacity On Demand > Advanced POWER Virtualization
Enter Activation Code	Copy the profile	Capacity On Demand > Advanced POWER Virtualization > Enter Activation Code  Capacity On Demand > Enterprise Enablement > Enter Activation Code
Show Code Information	View or edit the profile properties	Capacity On Demand > Advanced POWER Virtualization > View Code Information  Capacity On Demand > Enterprise Enablement > View Code Information
Show History Log	Delete the profile	Capacity On Demand > Advanced POWER Virtualization > View History Log  Capacity On Demand > Enterprise Enablement > View History Log

## Frame management

Frame Management has remained unchanged. Only a couple of the task names have changed and the tasks have been categorized not unlike the managed system and partition tasks.

*Table 4. Frame management*

Task Name	Task Description	New Location
Initiate Frames	Perform genesis IPL for all of the frames attached to the HMC	Operations > Initialize Frames
Properties	View or edit the frame properties	Properties
Rebuild Managed Frame	Rebuild the HMC's internal representation of the frame	Operations > Rebuild
Reset or Remove Connection	Reset the HMC connection to the managed frame	Operations > Reset Connection
Update Managed Frame Password	Update the HMC password for the managed frame	Operations > Change Password
I/O Unit	Power off the I/O units that are not currently owned by a Service Processor	Operations > Power Off I/O Units
Status	View the frame connection status	Operations > Bulk Power Assembly (BPA) Status

## Utilization data management

The Utilization Data Management node has been completely removed and the tasks are now strictly targeted on a managed system basis. You will find the utilization data tasks located in the "Operations" category of your managed systems.

Table 5. Utilization data management

Task Name	Task Description	New Location
Change Settings for Utilization Data Collection	T[S] Enable or disable utilization data collection on the managed system	Operations > Utilization Data > Enable  Operations > Utilization Data > Disable
View Utilization Data	T[S] View the utilization data information that has been collected	Operations > Utilization Data > View

## System plans

System plan tasks have become, for the most, part targeted tasks. You can work with all of the system plans on the HMC in one view. There are also additional system plan tasks available at the server level. For example, in the server container you can select a managed system and create a system plan by selecting the **Configuration > System Plans > Create** task.

The newly implemented System Plans container replaces the **Manage System Plans** task found in the WebSM System Plans container. You can now manage all of your system plans and perform actions on them from one view.

**Note:** \*SystemTask – indicates the task is available when a managed system is selected.

Table 6. System plans

Task Name	Task Description	New Location
Import System Plan	Import system plans from media or remote site	System Plans > Import System Plan
Deploy System Plan	T[S,SP] Deploy system plan to the system	System Plans > Deploy System Plan  Servers > System Task - Configuration > System Plans > Deploy
Manage System Plans	Manage system plans (create, delete, import, export)	System Plans
Learn more about system planning	Information Center articles regarding system planning	Welcome Screen > Online Information > IBM System Support  Welcome Screen > Online Information > Education and Tutorials

## Licensed internal code maintenance

Licensed Internal Code Maintenance has been combined into one **Updates** node which not only allows you to update the HMC with one click, but also all of the systems and frames being managed are seen along with their current code levels in one view. An **Update** task category has been created for managed systems in the servers container that will also allow you to perform code update/upgrade type of tasks.

The Backup HMC Data, Save Upgrade Data, Format Media, types of tasks have been moved away from the LIC categories into the **HMC Management** node. Also, there are a number of places where you can view the entire HMC versioning information by simply pointing to **HMC Version** at the top of the Service Management, HMC Management, and Welcome work panes.

**Note:** \* System Task – indicates the task is available when a managed system is selected.

*Table 7. Licensed Internal Code Maintenance*

Task Name	Task Description	New Location
<b>HMC Code Update</b>		
Backup Critical Console Data	Backup HMC console data	HMC Management > Backup HMC Data
Save Upgrade Data	Save HMC upgrade data information	HMC Management > Save Upgrade Data
Install Corrective Service	Install corrective service fix packs/updates	Updates > HMC Code Level > * Click <b>Update HMC</b>
Format Removable Media	Format removable media sources on the HMC (USB flash, diskette, etc)	HMC Management > Format Media
Remote Restore of Critical Console Data	Restore console data from a remote site	HMC Management > Restore HMC Data
Display HMC Version	Display complete HMC Version information such as serial number, bios level	Welcome Screen > point to <b>HMC Version</b>  HMC Management > pint to <b>HMC Version</b>  Updates > HMC Code Level
<b>Licensed Internal Code Updates</b>		
Change Licensed Internal Code for the current release	T[S,U]Update the firmware code level on the managed system/frame	Updates > System Code Levels - Change Licensed Internal Code for the current release  Servers > System Task – Updates > Change Licensed Internal Code for the current release
Flash Side Selection	T[S,U]Select flash side for update	Updates > System Code Levels > Flash Side Selection  Servers > System Task – Updates > Flash Side Selection
Upgrade Licensed Internal Code to a new release	T[S,U]Upgrade to a new firmware code level	Updates > System Code Levels > Upgrade Licensed Internal Code to a new release  Servers > System Task - Updates > Upgrade Licensed Internal Code to a new release
Check system readiness	T[S,U]Check the system readiness for code update/upgrade	Updates > System Code Levels > Check system readiness  Servers > System Task – Updates > Check system readiness

## HMC management

The HMC Management container, much like the Service Applications container, has been flattened out and all of the task are available with one click. One major change here is that the “Schedule Operations” task has been altered to become a targeted task so that you can simply select a managed system or partition in the work area and start working with scheduled operations for that object.

**Note:** \* System Task – indicates the task is available when a managed system is selected. \* Partition Task – indicates the task is available when a partition is selected.

*Table 8. HMC management*

Task Name	Task Description	New Location
<b>HMC Users</b>		
Manage HMC Users and Access	Manage user and access	HMC Management > Manage User Profiles and Access
Manage Access Task Roles and Managed Resource Roles	Manage user roles	HMC Management > Manage Task and Resource Roles
Change User Password	Change password	HMC Management > Change User Password
<b>HMC Configuration</b>		
Customize HMC Date and Time	Set date, time, and time zone	HMC Management > Change Date and Time
View HMC Events	View console events	HMC Management > View HMC Events
Customize Network Settings	Configure network, firewall, DNS, and routes	HMC Management > Change Network Settings
Test Network Connectivity	Ping utility	HMC Management > Test Network Connectivity
Schedule Operations	<b>T[S,P,H]</b> Configure scheduled operations	HMC Management > Schedule Operations  * System Task – Operations > Schedule Operations  *Partition Task – Operations > Schedule Operations
Enable or Disable Remote Command Execution	Allow SSH	HMC Management > Remote Command Execution
Enable or Disable Remote Virtual Terminal	Allow virtual terminal	HMC Management > Remote Virtual Terminal
Change Current Language and Locale	Change language and locale	HMC Management > Change Language and Locale

## Service applications

The Service Applications container has been renamed to **Service Management** and contains the majority of tasks that were found under the Service Applications nodes. The majority of tasks that are located in the Service Focal Point > Service Utilities dialogs have been moved to be targeted tasks located within the **Serviceability** task category for managed systems and partitions. You can select a managed system or partition, then select **Manage Serviceable Events** or select a system and perform a **Add FRU** task.

**Note:** \* System Task – indicates the task is available when a managed system is selected. \* Partition Task – indicates the task is available when a partition is selected.

*Table 9. Service applications*

Task Name	Task Description	New Location
<b>Service Agent</b>		
eService Registration	Registers system for use on the eService web site	Service Management > Manage eService Registration

Table 9. Service applications (continued)

Task Name	Task Description	New Location
Customer Notification	How the customer will be notified	Service Management > Manage Serviceable Event Notification
Transmit Service Information	Transmit HMC service information	Service Management > Transmit Service Information
Service Agent Connection Manager	Configure a connection manager for legacy SA clients	Service Management > Manage POWER4 Service Agent
<b>Remote Support</b>		
Customize Customer Information	Configure customer information	Service Management > Manage Customer Information
Customize Outbound Connectivity	Configure call-home settings	Service Management > Manage Outbound Connectivity
Customize Inbound Connectivity	Configure remote serve settings	Service Management > Manage Inbound Connectivity
Manage Remote Support Requests	View active RSF requests	Service Management > Manage Remote Support Requests
Manage Remote Connections	View active RCS requests	Service Management > Manage Remote Connections
Customer Service Settings	Configure service settings	Service Management > Manage Systems Call-Home
<b>Service Focal Point</b>		
Repair Serviceable Event	<b>T[S,H,P]</b> Repairs a problem.  ** Manage and Repair have been combined into one task that is accessible from the System, Partition, and HMC level	Service Management > Manage Serviceable Events  * Partition Task - Serviceability > Manage Serviceable Events  * System Task - Serviceability > Manage Serviceable Events
Manage Serviceable Events	See Repair Service Event	
<b>Install/Add/Remove Hardware</b>		
Add Enclosure	<b>T[S]</b> Add Enclosure.	System Task - Serviceability > Hardware
Add FRU	<b>T[S]</b> Add FRU	System Task - Serviceability > Hardware
Remove Enclosure	<b>T[S]</b> Remove Enclosure.	System Task - Serviceability > Hardware
Remove FRU	<b>T[S]</b> Remove FRU	System Task - Serviceability > Hardware
<b>Exchange Parts</b>		
Replace Enclosure	<b>T[S]</b> Exchange Enclosure	System Task - Serviceability > Hardware
Replace FRU	<b>T[S]</b> Exchange FRU	System Task - Serviceability > Hardware
<b>Service Utilities</b>		
Create Serviceable Event	Creates a problem for the HMC	Service Management > Create Serviceable Event

Table 9. Service applications (continued)

Task Name	Task Description	New Location
Connection Monitoring	Configures connection errors to be sent to service agent	Service Management > Manage Connection Monitoring
Load Problems From XML	Load problems from a local XML file	Service Management > Load Serviceable Events
View Network Topology	Ping broadcasting to discover managed system, HMCs, etc.	HMC Management > View Network Topology
Create Serviceable Event	T[IS] Creates a problem for targeted system	System Task – Serviceability > Create Serviceable Event
Launch ASM Menu	T[IS] Launch browser to connect to ASM	System Task – Operations > Advanced System Management ( ASM )
Manage Dumps	T[IS] Manage system dumps	System Task – Serviceability > Manage Dumps
Edit MTMS	T[IS] Modify MTMS	System Task – Serviceability > Edit MTMS
System Attention LED	T[IS] Turn System Attention LED on/off	System Task – Operations > LED Status
Identify LED processing	T[IS] Turn Identify LED on/off	System Task – Operations > LED Status
Lamp Test	T[IS] Blinks all LEDs on system	System Task – Operations > LED Status
Operator Panel Service Functions	T[IS] Mimics Op Panel functionality	System Task – Serviceability > Control Panel Functions
Power On/Off Unit	T[IS] Power system off/on	System Task – Serviceability > Hardware
View RIO Topology	T[IS] View the RIO cable connections	System Task – Hardware > View Topology
Service Processor Failover	T[IS] Configure FSP failover	System Task – Serviceability > FSP Failover
Collect VPD Information	T[IS] Collect VPD Information	System Task – Serviceability > Collect VPD

## DLPAR changes

The following dynamic LPAR changes include:

### Memory and Processors

The DLPAR operations have changed slightly in the V7.3.1.0 HMC. An overall change is that the Add and Remove operations for memory and processor resources have been combined into one task. For example, when you want to change the amount of memory that is assigned to the partition you simply launch the **Add/Remove memory** task and enter in the amount of memory you would like to have assigned to the LPAR. When you want to move resources from one partition to the other there is a separate task to facilitate that function which is very similar to the WebSM move operation.

### Physical I/O

For Physical I/O resources we have combined the move and remove operation into one task so that you can optionally move the I/O resource that you are trying to remove to another partition. The **Add** operation for I/O resources has basically stayed the same.



### **RMC-less DLPAR for AIX/Linux Partitions**

POWER5 WebSM HMC supported DLPAR operations between two AIX or Linux partitions that do not have RMC connections. This function has been removed from the UI because these types of operations require multiple steps for the user in order to be successful. You can still remove or add resources to a partition that does not have an RMC connection, however you will not be able to move resources between two AIX or Linux partitions that do not have active RMC connections.

Another change that has been implemented for DLPAR operations is that the task will display an indicator within the dialog for AIX and Linux partitions that alerts you that an RMC connection is missing. This is to let you know you are about to perform an RMC-less DLPAR operation before you start entering data into the fields in the dialog. If you would still like to move resources between two AIX or Linux partitions that do not have RMC connections the command line **chhwres** command can still be used to facilitate the move operation.



---

## Chapter 2. Using the Web-based user interface

This chapter explains how to use the web-based user interface to perform tasks on the Hardware Management Console (HMC) or on your managed resources. This user interface comprises several major components as shown in Figure 3 on page 20: the banner, the task bar, the navigation pane, the work pane, and the status bar.

The *banner*, across the top of the workplace window, identifies the product and logo. It is optionally displayed. Use the **Change User Interface Settings** task to change the setting.

The *task bar*, located below the banner, displays the names of any tasks that are running, the user ID you are logged in as, online help information, and the ability to logoff or disconnect from the console.

The *navigation pane*, in the left portion of the window, contains the primary navigation links for managing your system resources and the HMC. The items are referred to as nodes.

The *work pane*, in the right portion of the window, displays information based on the current selection from the navigation pane. For example, when **Welcome** is selected in the navigation pane, the Welcome window content is displayed in the work pane, as shown in Figure 3 on page 20.

The *status bar*, in the bottom left portion of the window, provides visual indicators of current overall system status. It also contains a status overview icon which may be selected to display more detailed status information in the work pane.

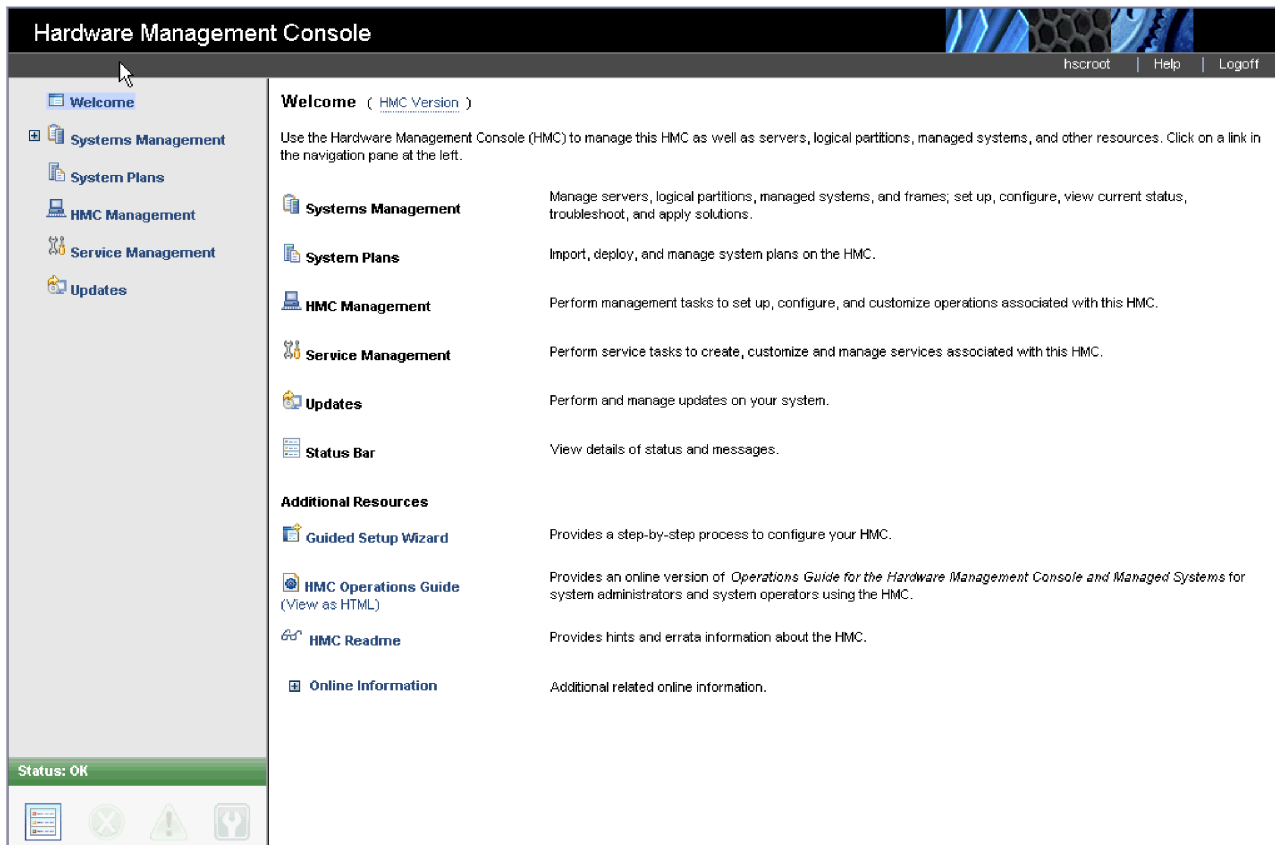


Figure 3. Web-based user interface HMC workplace window

You can resize the panes of the HMC workplace by moving the mouse pointer over the border that separates the navigation pane from the work pane until the mouse pointer changes to a double-pointed arrow. When the pointer changes shape, press and hold the left mouse button while dragging the mouse pointer to the left or right. Release the button and your navigation pane or work pane is now larger or smaller in size. You can also do this within the work pane border that separates the resources table from the tasks pad.

## Task bar

The task bar provides the capability of an active task switcher. The task bar can be used as a navigation aid to move between tasks that were launched and have not yet been closed. The task switcher does not pause or resume existing tasks. Clicking on a task in the task bar brings that task's window forward and gives it focus.

**Note:** Tasks that open separate native windows, such as AIX terminal windows, 5250 console windows, or restricted shell windows will not appear in the tasks bar when active.

The right end of the task bar also contains the following information as shown in Figure 4 on page 21:

- **user ID** that you are logged in as. By clicking the user ID, you open the **Change User Interface Settings** task.
- **Help** displays information about all the tasks on the HMC and how to use the Web-based user interface on the HMC.
- **Logoff** opens the **Logoff or Disconnect** task.

Figure 4. Task bar

## Navigation pane

The navigation pane, as shown in Figure 3 on page 20, contains the primary navigation links for managing your system resources and the HMC. These include:

- “Welcome”
- “Systems Management”
- “System Plans” on page 30
- “HMC Management” on page 31
- “Service Management” on page 33
- “Updates” on page 33

## Welcome



**Welcome** is the initial window that is displayed when you log on to the HMC. The Welcome work pane lists the nodes of the navigation pane and their descriptions. It also includes the following **Additional Resources**:

- **Guided Setup Wizard** - provides a step-by-step process to configure your HMC.
- **HMC Operations Guide** - provides an online version of the *Operations Guide for the Hardware Management Console and Managed Systems* for system administrators and system operators using the HMC.

If you are accessing the HMC remotely, you can view the publication in PDF format or in HTML format (click **View as HTML**). If you are accessing the HMC locally, you can view the publication in HTML format.

- **HMC Readme** - provides hints and errata information about the HMC.
- **Online Information**

**Note:** This information is only available when you are accessing the HMC remotely.

- **IBM System Support** - supplies support and technical information for IBM Systems
- **HMC Support** - supplies support and technical information for the HMC
- **Education and Tutorials** - supplies course materials for training and updating HMC skills

To see what level of the HMC you are currently working with, point your mouse over **HMC Version** found at the top of the work pane.

## Systems Management



**Systems Management** contains a tree view of managed resources. Resources may include:

- “Servers”
- “Frames” on page 29
- “Custom Groups” on page 29

## Servers

The **Servers** node represents the servers that are managed by this HMC. To add servers you can use the **Add Managed System** task under the **Connections** category in the tasks pad.

When you click **Servers** from the navigation pane a listing of individually defined servers is displayed in table form in the work pane and under the **Servers** node in the navigation pane, as shown in Figure 5.

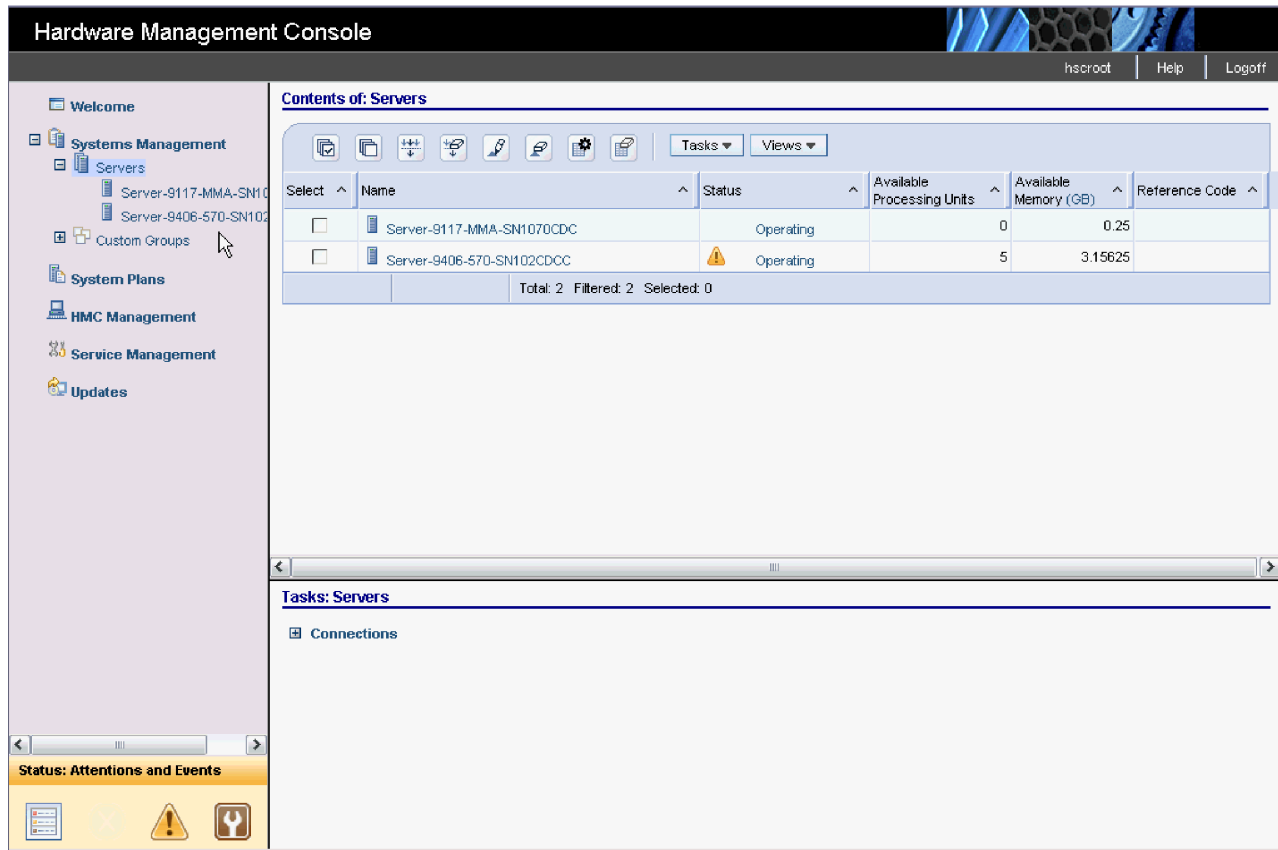


Figure 5. Systems Management servers window

**Selecting a server:** To work with a server, you can perform one of the following actions:

- Select a server under the **Servers** node from the navigation pane.
- Click on a server name from the work pane table.
- Click in the **Select** column next to the server name in the work pane table.

The Servers work pane table displays the following attributes by default.

**Name** Specifies the user-defined name of the managed system.

**Status** Displays the current status of the managed system (for example, Operating, Power off, Initializing) and, in addition, displays icons representing an unacceptable state or an active Attention LED. See “Status: Unacceptable” on page 38 or “Status: Attention LEDs” on page 39 for more information.

#### Available Processing Units

Displays the number of processing units that are available for assignment to logical partitions on the managed system. This is the total number of processing units that are activated on the managed system minus the number of processing units that are assigned to the logical partitions, including the logical partitions that are shut down, on the managed system. This number does not include any processing units that have not yet been activated with Capacity on Demand (CoD).

#### Available Memory

Displays the amount of memory that is available for assignment to logical partitions on the

managed system. This is the total amount of memory that is activated on the managed system minus the amount of memory needed by managed system firmware minus the amount of memory that is assigned to the logical partitions, including the logical partitions that are shut down, on the managed system. This number does not include any memory that has not yet been activated with Capacity on Demand (CoD). The available memory amount can be shown in MB or GB. Click **MB** or **GB** in the Available Memory column title.

**Reference Code**

Displays the system reference codes for the server. Click the reference code in the table for a detailed description.

The Servers work pane table can also display the following optional attributes in the table.

**Configurable Processing Units**

Displays the configured processing units. Configured - Licensed and usable (not guarded) processing units.

**Configurable Memory**

Displays the configured memory. Configured - Licensed and usable (not guarded) memory.

**Serial Number**

Displays the serial number of the managed system.

**Type-Model**

Displays the type and model number of the managed system (for example, 9117-MMA).

**CoD Processor Capable**

Displays whether the managed system supports Capacity on Demand (CoD) for processors.

**CoD Memory Capable**

Displays whether the managed system supports CoD for memory.

**Permanent Processors**

Specifies the number of permanent licensed processors.

**On/Off CoD Processors State**

Displays the On/Off CoD processor state.

**Trial CoD Processor State**

Displays the Trial CoD processor state.

**Reserved CoD Processor State**

Displays the Reserved CoD processor state.

**Utility CoD Processor State**

Displays the Utility CoD processor state.

**Permanent Memory (GB)**

Displays the amount of permanent activated memory.

**On/Off CoD Memory State**

Displays the On/Off CoD memory state.

**Trial CoD Memory State**

Displays the Trial CoD memory state.

Optional attributes can be displayed when you select the **Column configuration** icon on the table toolbar. This function allows you to select additional attributes that you want displayed as columns in the table. It also allows you to reorder the columns, see “Column configuration” on page 36 for more information.

You can also use **Views** from the table toolbar to display the **Default** server attributes in the table or to display the **Capacity On Demand** server attributes in the table. See Figure 6 on page 24 for a sample of

using the Capacity On Demand view and “Views menu” on page 36 for more information.

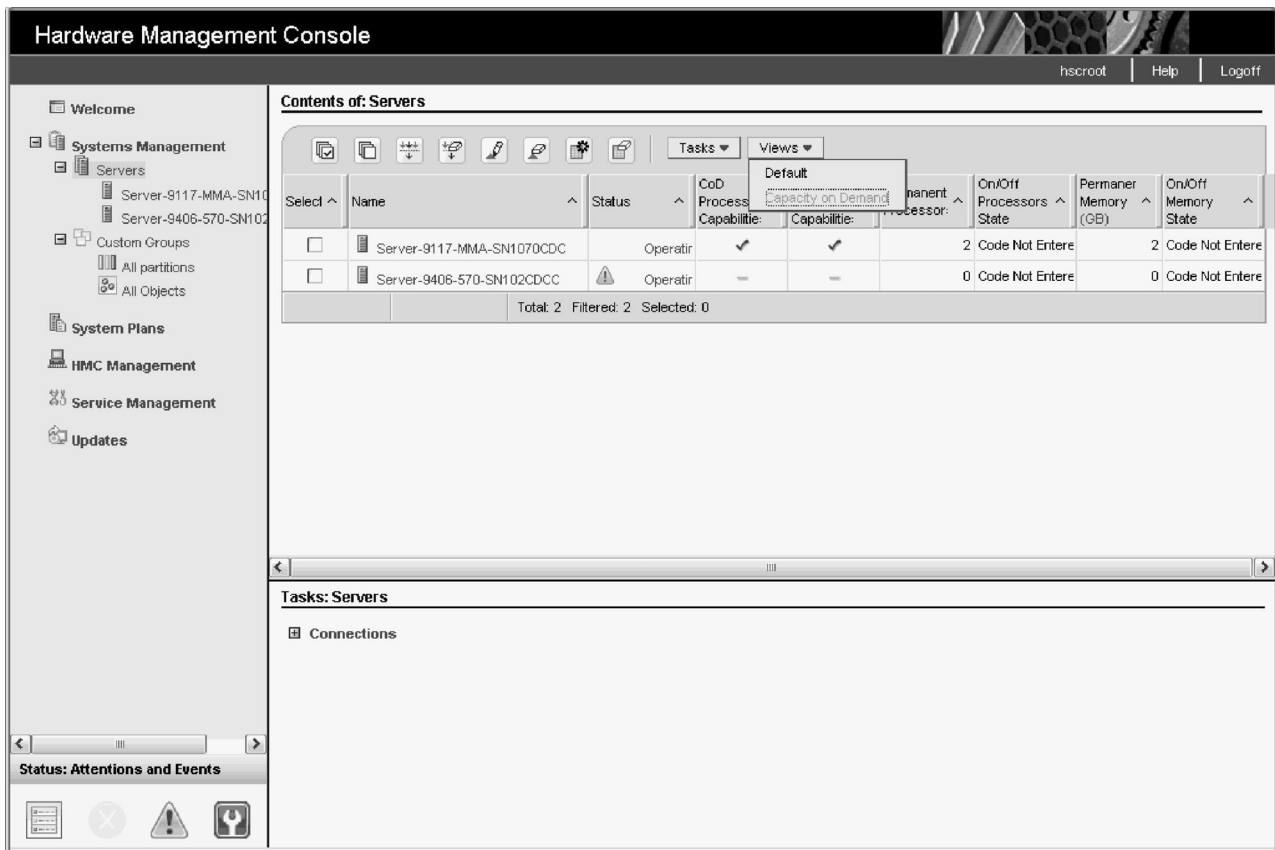


Figure 6. Capacity On Demand attributes

**Displaying server details:** To display details (properties) about a server you can select the server by clicking in the **Select** column in the work pane table. Then you can either, click **Properties** from the tasks pad or click on the double-arrow icon next to the server name and click **Properties** from the context menu. In both cases the **Properties** window is displayed.

**Launching tasks for managed objects:** After you have chosen the objects to work with you are ready to perform the appropriate tasks on them. The tasks the objects can perform include the following task groups. Task groups are simple “categorization nodes” and are not tasks themselves.

- “Operations” on page 42
- “Configuration” on page 47
- “Connections” on page 51
- “Hardware (Information)” on page 54
- “Dynamic Logical Partitioning” on page 75
- “Updates” on page 56
- “Serviceability” on page 56
- “Capacity on Demand” on page 61

You can select a task from these task groups in a variety of ways. Some of these categories may also include sub categories before you get to the actual task you want to perform, see Figure 7 on page 25. Appropriate tasks for a selected object are listed in the tasks pad, in context menus, and in the **Tasks** menu.

**Note:** If a particular task cannot be performed on an object, the task will not display.

*Tasks pad:*



The **tasks pad** appears below the work pane when you have selected an object you want to work with (see Figure 7). This view contains available tasks for selected managed objects.

**Note:**

1. Resize the tasks pad by moving the mouse pointer over the border that separates the work pane from the tasks pad.
2. Optionally display the tasks pad by using the **Change User Interface Settings** task, see “Change User Interface Settings” on page 95.
3. Expand or collapse all the task categories in the tasks pad by selecting **Expand All** or **Collapse All** from the tasks pad heading.

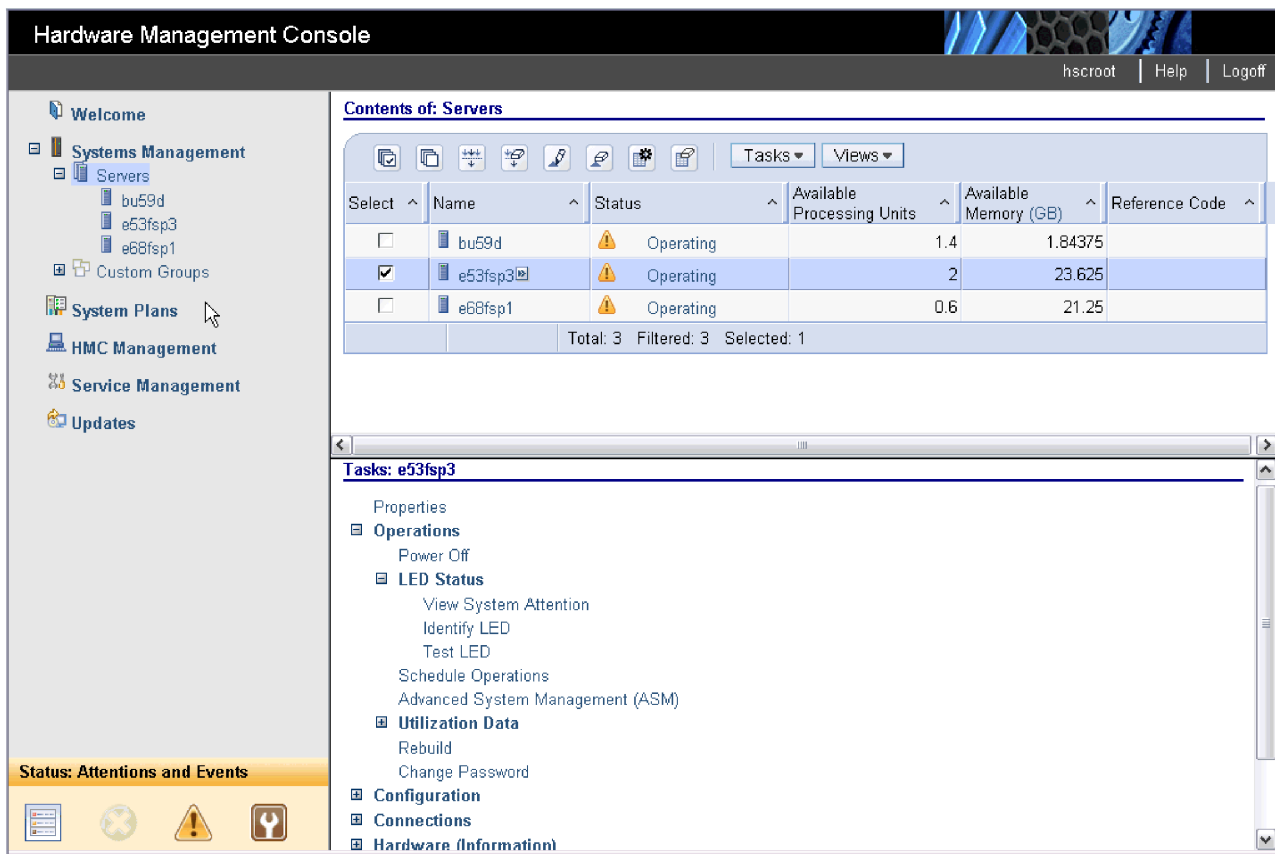


Figure 7. Tasks pad

The tasks contained in this view meet the following characteristics:

- Tasks are available for the currently selected target objects in the navigation pane or the work pane table view. If multiple objects are selected in the work pane table, the intersection of the selected objects' tasks is displayed. If there are no selections in the table, tasks are displayed for the object selected in the navigation pane.
- Tasks available are limited by the role of the user who is currently logged in.

An example of using the *tasks pad* method:

1. Select a server in the work pane table (click the **Select** column).
2. Select a task group from the tasks pad (click the expand button or click the group name).

**Note:** After you have expanded the task groups those groups remain open so that you can repeatedly open other tasks without having to reopen the task groups again.

3. Select a task that is displayed under the task group that you want to perform on that server.
4. The task window is displayed.

#### Context Menu:

The **Context menu** is a pop-up menu that lists the task groups appropriate for the selected object. Context menus are only available for table selections. For example, in the **Select** column of the Servers Work pane table, select the object you want to work with (a check mark appears). The Context menu button (double right arrows) appears next to the object name you have selected. Click the button and the task groups menu appears for that particular object, as shown in Figure 8. Then select a task to launch for the object. If more than one object is selected, the tasks that appear in the Context menu(s) apply to all selections.

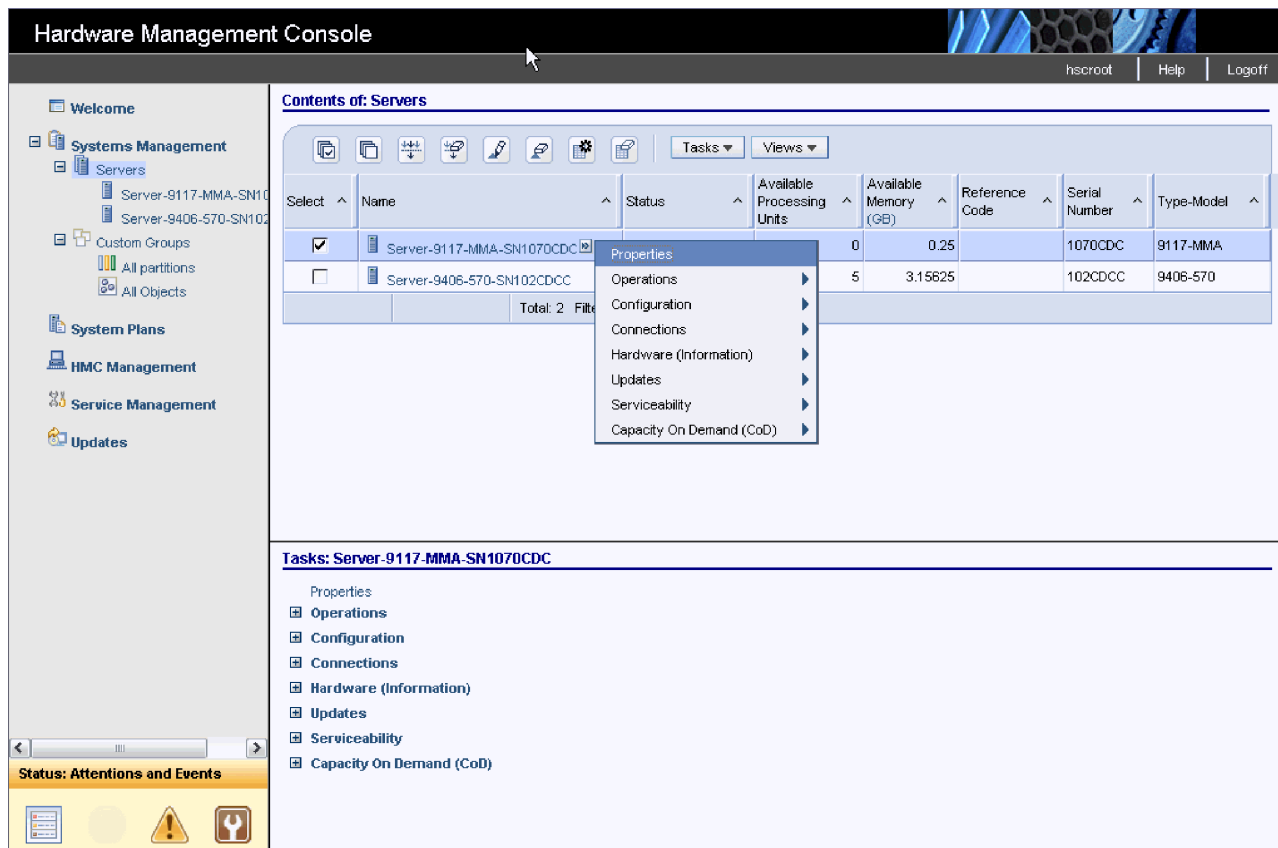


Figure 8. Context menu

#### Tasks menu:

The **tasks menu** is displayed on the table toolbar, as shown in Figure 9 on page 27. The tasks menu is only available for table selections. For example, in the **Select** column of the Servers work pane table, select the object you want to work with. Click **Tasks** for the list of the applicable task groups for the selected objects in the table. Select a task group, then select a task to open for the object. If more than one object is selected, the tasks that are displayed in the tasks menu apply to all selections.

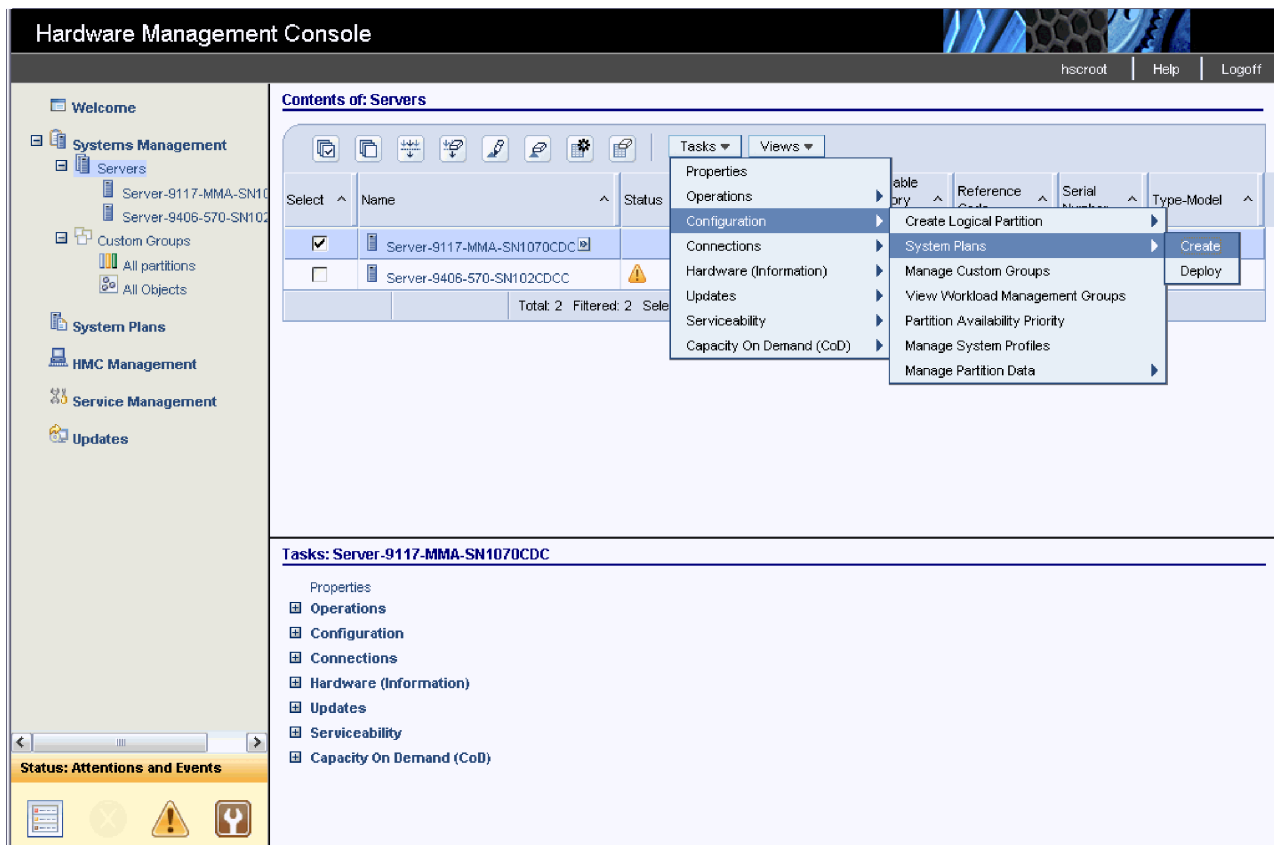


Figure 9. Tasks menu

**Partitions:** When you select a managed server in the navigation pane, the work pane displays the list of partitions defined on the server as shown in Figure 10 on page 28.

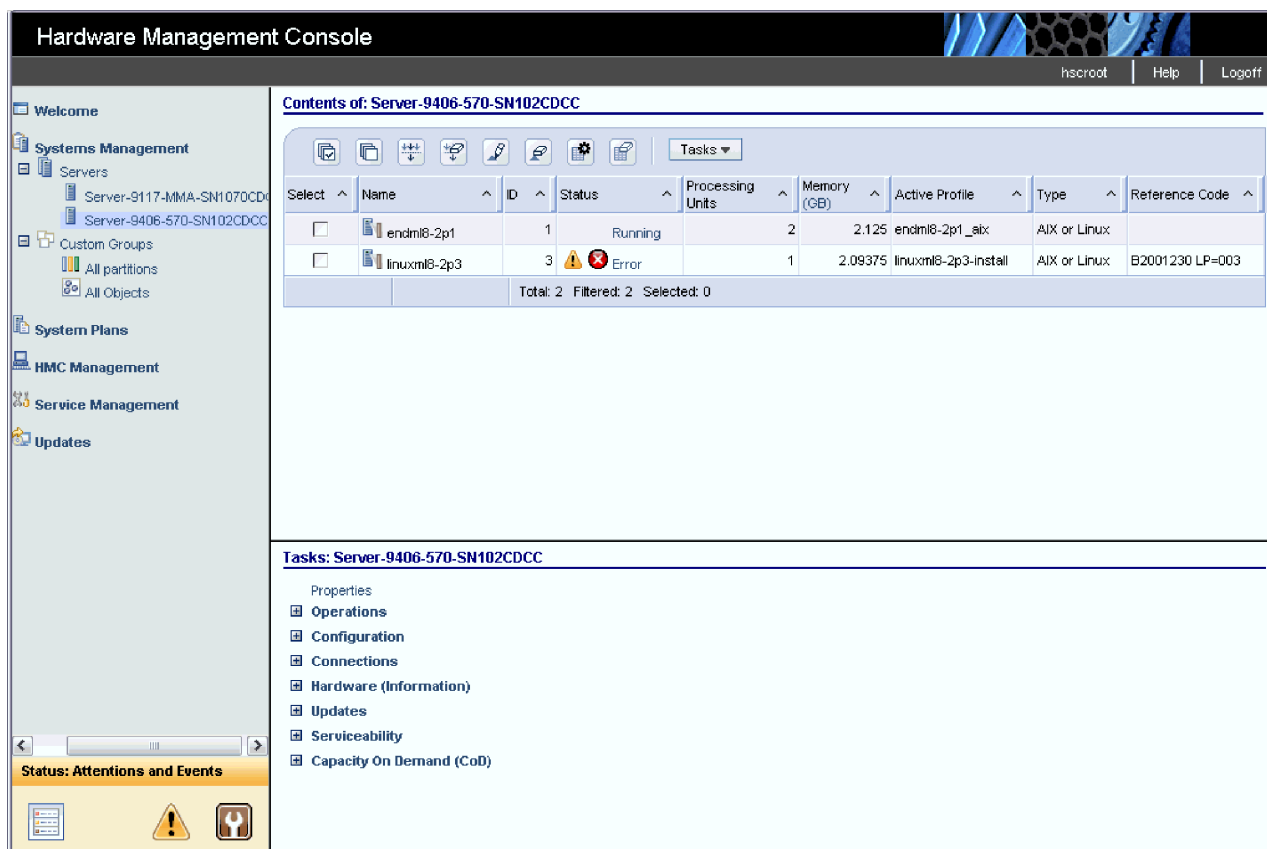


Figure 10. Partitions work pane

The Partitions work pane table displays the following attributes by default.

**Name** Specifies the user-defined name of the logical partition.

**ID** Specifies the ID of the partition

**Status** Displays the current status of the partition (for example, running, not activated) and, in addition, displays icons representing an unacceptable state or active Attention LED. See “Status: Unacceptable” on page 38 or “Status: Attention LEDs” on page 39 for more information.

#### Processing Units

Displays the unit of measure for shared processing power across one or more virtual processors. Processing power can be specified in fractions of a processor.

#### Memory

Specifies the amount of memory allocated to the partition currently. The memory amount can be shown in MB or GB. Click **MB** or **GB** in the Memory column title.

#### Active Profile

Specifies the profile that was used to activate the partition last.

#### Environment

Specifies the type of object, logical partition, server, frame (for example, i5/OS, AIX/Linux, Virtual I/O Server).

#### Reference Code

Displays the system reference codes for the partition. For POWER6 systems, click the reference code in the table for a detailed description.

The Partitions work pane table can also display the following optional attributes in the table.

### Processor

If the partition is using dedicated processors, this value indicates the number of processors currently allocated to the partition. If the partition is using shared processors, this value represents the virtual processors currently allocated to the partition.

### Service Partition

Specifies whether the partition has service authority.

### Configured

Specifies whether a partition is configured with all the required resources to power on.

### Default Profile

Specifies the profile that is configured as the default profile. When users perform the **Activate** task from the partition, this profile is selected by default.

Optional attributes can be displayed when you select the **Column configuration** icon on the table toolbar. This function allows you to select additional attributes that you want displayed as columns in the table. It also allows you to reorder the columns, see “Column configuration” on page 36 for more information.

**Displaying partition details:** To display details (properties) about a partition you can select the partition by clicking in the **Select** column in the work pane table. Then you can either, click **Properties** from the tasks pad or click on the double-arrow icon next to the partition name and click **Properties** from the context menu. You can also click on the partition name. In all cases the **Properties** window is displayed.

## Frames

The **Frames** node identifies the frames managed by this HMC.

**Note:** Frames typically have dual Bulk Power Controllers (BPCs), however only one BPC is displayed as both BPCs share the same machine type, model, and serial number and function as redundant peers.

The Frames work pane table includes the following attributes.

**Name** Displays the defined name of the Frame.

**Status** Displays the status of the frame object. A frame is in an unacceptable state when it is in **No Connection** or **Incomplete** state. When either of these conditions occurs, a red X is displayed in the status cells next to the status text which identifies the state. Clicking on either the X or the status text opens information describing the unacceptable state and potential remedies.

### Frame Number

Displays the number of the managed frame. You can modify the number.

### Connection Status

Displays connection status of the frame (side A and B).

## Custom Groups

The **Custom Groups** node provides a mechanism for you to group system resources together in a single view. In addition, groups may be nested to create custom “topologies” of system resources.

Custom groups include the predefined groups **All Partitions** and **All Objects** and any user-defined groups that you created using the **Manage Custom Groups** task under the **Configuration** category in the tasks pad. The **All Partitions** group includes all the partitions defined to all servers managed by the HMC. The **All Objects** group is a collection of all the managed servers, partitions, and frames.

These system-defined groups (All Partitions and All Objects) cannot be deleted. However, if you do not want **All Partitions** or **All Objects** displayed under **Custom Groups**, do the following:

1. Open the **Change User Interface Settings** task from the HMC Management work pane.
2. Deselect **All Partitions node** and **All Objects node** in the **User Interface Settings** window.

3. Click **OK** to save the changes and close the window. Those groups are no longer displayed under **Custom Groups** in the navigation pane.

You can use the **Views** menu on the table toolbar to display your preferred table column configuration, see “Views menu” on page 36 for more information.

#### User-defined groups:

You can use the **Manage Custom Groups** task under the Configuration category from the tasks pad to create your own group that you want to work with. This task allows you to create new groups and manage existing ones. To create a group:

1. Select one or more resources (for example: servers, partitions, frames) that you want to include in the group you want to work with.
2. Open the **Manage Custom Groups** task.
3. From the **Manage Groups** window, select **Create a new group**, specify a group name and description, click **OK** to complete. The new user-defined group is displayed in the navigation pane under the **Custom Groups** node.

You can also create a group by using the pattern match method:

1. Without selecting an object you can open the **Manage Custom Groups** task from the Custom Groups or Systems Management tasks pad.
2. From the **Create Pattern Match Group** window, select one or more group types that you want to create, specify a group name, description, and the pattern used to determine if an object should be part of the group, click **OK** to complete. The new user-defined group is displayed in the navigation pane under the **Custom Groups** node.

**Note:** Patterns specified in the **Managed Resource Pattern** input field are regular expressions. For example, if you specified **abc.\***, all the resources that begin with **abc** will be included in that group.

See “Manage Custom Groups” on page 48 for more information.

## System Plans



**System Plans** displays the plans and the tasks to deploy system plans to managed systems. A *system plan* contains a specification of the logical partition configuration of a single managed system. You can also use this node to import, export, and manage the files containing these system plans.

To display the plans and tasks:

1. Select the **System Plans** node in the navigation pane.
2. From the work pane, select a plan you want to work with by clicking in the **Select** column.
3. From the tasks pad, click one of the following tasks:
  - Create System Plan
  - Deploy System Plan
  - Export System Plan
  - Import System Plan
  - Remove System Plan
  - View System Plan

These tasks are described in further detail in “System Plans” on page 48. The table in the work pane displays the system plans that the HMC manages and attributes related to the system plans.

The following attributes are set as the defaults. However, you can select or deselect the attributes that you want displayed in the table by clicking the **Column configuration** icon on the table toolbar. You can also reorder the columns, see “Column configuration” on page 36 for more information.

**Name** Displays the system plan file name.

**Description**

Specifies a description of the system plan.

**Source**

Displays how the system plan was created.

**Version**

Displays version information about the system plan.

**Last Modified Date**

Specifies the date when the system plan was last modified.

The create and deploy System Plans tasks are also displayed for a server under the **Configuration** task group.

If there are no system plans available when you select the **System Plans** node, you can create or import a plan from the tasks listed in the tasks pad as shown in Figure 11.

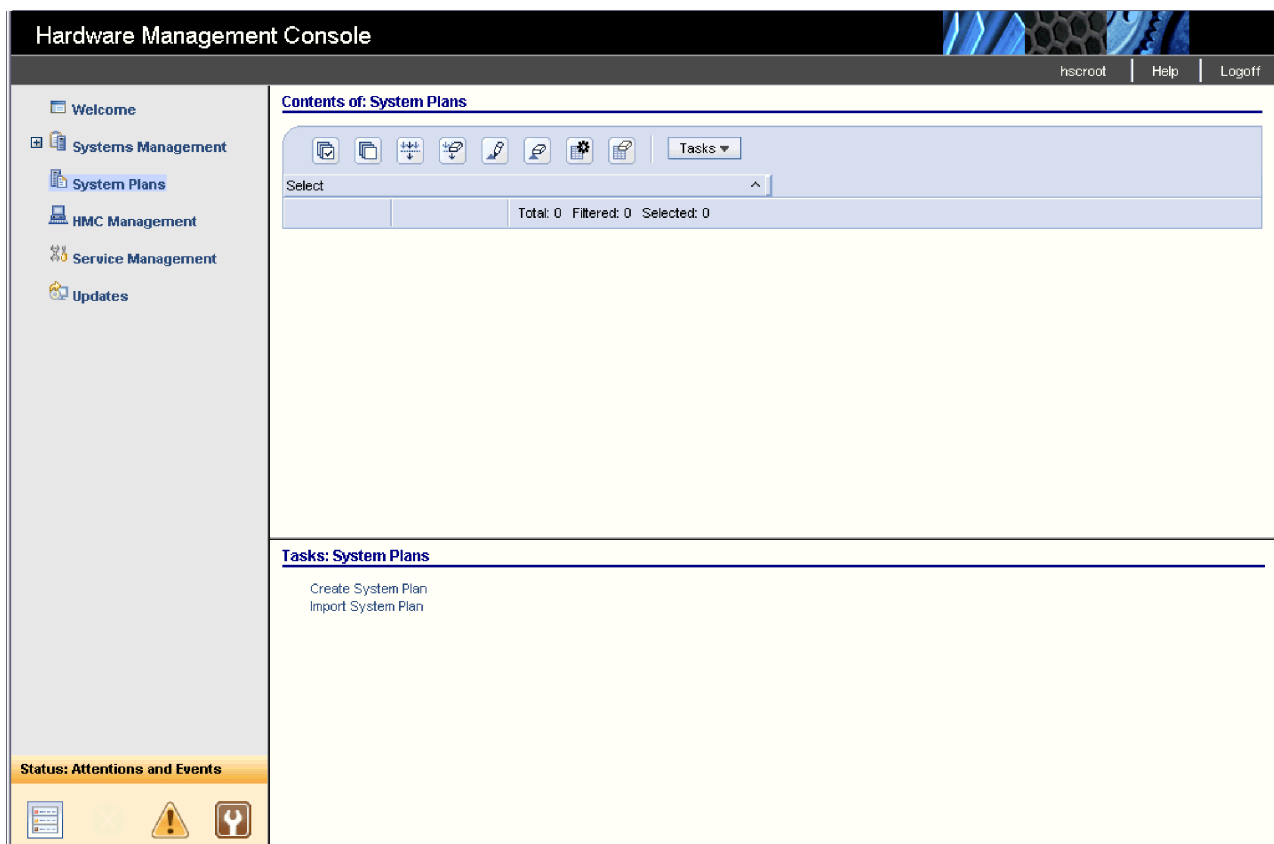


Figure 11. System Plans

## HMC Management



**HMC Management** contains a categorized or alphabetic view of HMC management tasks and their descriptions. These tasks are used for setting up the HMC, maintaining its internal code, and securing the HMC.

To display the tasks in the work pane:

1. Select the **HMC Management** node in the navigation pane.
2. From the work pane, click on the task you want to perform.
3. By default, a categorized listing of the tasks appear. The categories include:
  - Operations
  - Administration

To see what level of the HMC you are currently working with, point your mouse over **HMC Version** found at the top of the work pane.

If you want an alphabetic listing of the tasks, click **Alphabetical List** in the upper right corner of the work pane. Click **Categorized List** to go back to the task categories.

**Note:** If you are accessing the HMC remotely, some tasks do not display.

The following alphabetic list of HMC Management tasks are displayed in the work pane depending on the task roles defined to your user ID. They are described in further detail in Chapter 7, “HMC Management tasks,” on page 93 and a listing of the tasks and the default user roles that can use them are shown in Table 10 on page 127.

- “Back up HMC Data” on page 93
- “Change Date and Time” on page 93
- “Change Language and Locale” on page 94
- “Change Network Settings” on page 94
- “Change User Interface Settings” on page 95
- “Change User Password” on page 96
- “Create Welcome Text” on page 96
- “Format Media” on page 96
- “Launch Guided Setup Wizard” on page 97
- “Launch Remote Hardware Management Console” on page 97
- “Lock HMC Screen” on page 97
- “Manage Certificates” on page 98
- “Manage Data Replication” on page 99
- “Manage Task and Resource Roles” on page 99
- “Manage User Profiles and Access” on page 100
- “Manage Users and Tasks” on page 101
- “Open 5250 Console” on page 101
- “Open Restricted Shell Terminal” on page 102
- “Remote Command Execution” on page 102
- “Remote Operation” on page 102
- “Remote Virtual Terminal” on page 102
- “Restore HMC Data” on page 102
- “Save Upgrade Data” on page 103
- “Schedule Operations” on page 103
- “Shut Down or Restart” on page 104
- “Test Network Connectivity” on page 104
- “Tip of the Day” on page 105
- “View HMC Events” on page 105
- “View Licenses” on page 105
- “View Network Topology” on page 106



## Service Management



**Service Management** contains a categorized or alphabetic view of tasks and their descriptions used to service the HMC.

To display the tasks in the work pane:

1. Select the **Service Management** node in the navigation pane.
2. From the work pane, click on the task you want to perform.
3. By default, a categorized listing of the tasks appear. The category is Connectivity.

To see what level of the HMC you are currently working with, point your mouse over **HMC Version** found at the top of the work pane.

If you want an alphabetical listing of the tasks, click **Alphabetical List** in the upper right corner of the work pane. Click **Categorized List** to go back to the task categories.

The following alphabetic list of Service Management tasks are represented in the work pane depending on the task roles defined to your user ID. They are described in further detail in Chapter 8, “Service Management tasks,” on page 107 and a listing of the tasks and the default user roles that can use them are shown in Table 10 on page 127.

- “Create Serviceable Event” on page 107
- “Format Media” on page 96
- “Load Serviceable Events” on page 108
- “Manage Connection Monitoring” on page 108
- “Manage Customer Information” on page 108
- “Manage Dumps” on page 109
- “Manage eService Registration” on page 109
- “Manage Inbound Connectivity” on page 110
- “Manage Outbound Connectivity” on page 110
- “Manage POWER4 Service Agent” on page 111
- “Manage Remote Connections” on page 111
- “Manage Remote Support Requests” on page 111
- “Manage Serviceable Event Notification” on page 112
- “Manage Serviceable Events” on page 112
- “Manage Systems Call-Home” on page 112
- “Transmit Service Information” on page 113

## Updates



**Updates** provides a way for you to access information on both HMC and system firmware code levels at the same time without running a task. The Updates work pane displays the HMC code level, system code levels, and the ability to install corrective service by clicking **Update HMC**. **Note:** Before performing HMC updates, see “Update HMC” on page 115.

To display the tasks:

1. Select the **Updates** node in the navigation pane.
2. Select a managed object to apply updates on.
3. From the tasks pad, click on the task you want to perform.
4. The tasks pad provides the following tasks required to install corrective service:
  - “Change Licensed Internal Code for the current release” on page 117
  - “Upgrade Licensed Internal Code to a new release” on page 121
  - “Flash Side Selection” on page 124
  - “Check system readiness” on page 124

- “View system information” on page 124

See Figure 12 for an example of the Updates work pane and tasks pad. The Updates tasks can also be displayed under the **Updates** task group when you are working with managed objects from the **Systems Management** node of the navigation pane.

**Hardware Management Console**

hscroot | Help | Logout

**Updates**

**HMC Code Level**

Version: 7      Build Level: 20070403.1      Serial Number: KCWA6BNH  
 Release: 3.1.0      Base Version: V7R3.1.0      Model Type: 7310C04  
 Service Pack: 0      BIOS: 2BKT39AUS

[Update HMC](#)

**System Code Levels**

Select	Name	Status	Platform IPL Level	Activated Level	EC Number	Deferred Level
<input checked="" type="checkbox"/>	e36fsp8	Operating	26	26	01EM310	None

Total: 1    Filtered: 1    Selected: 1

**Tasks: e36fsp8**

- Change Licensed Internal Code for the current release
- Upgrade Licensed Internal Code to a new release
- Flash Side Selection
- Check system readiness
- View system information

**Status: Attentions and Events**

Icons: [System Health] [Error] [Warning] [Maintenance]

Figure 12. Updates

## Work pane

The work pane displays a table of information based on the current selection in the navigation pane or status bar. Selecting an object displays a configurable table in the work pane as shown in Figure 13 on page 35. The following figure also identifies some of the areas of the work pane table.

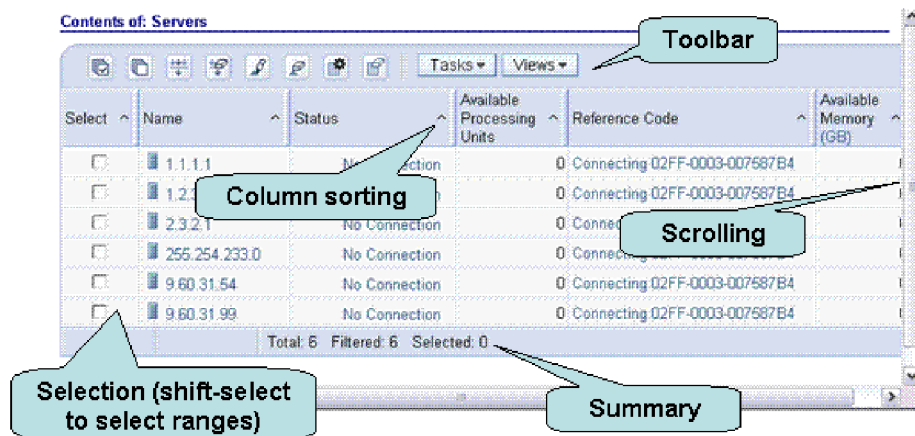


Figure 13. Work pane table

## Working with Tables

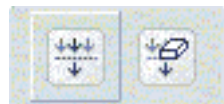
The tool bar at the top of the table contains buttons used to select, filter, sort, and arrange the entries in the table. Hovering over the toolbar buttons displays their functions. The toolbar also includes menus that are used with the information displayed in the tables. See "Tasks menu" on page 26 and "Views menu" on page 36 for more information.

### Selecting Rows



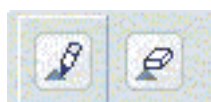
You can select more than one table row at any given time. Rows can be individually selected or a block of rows can be selected at once by first left-clicking the selection box of the first row in the desired block and then shift-clicking the selection box of the last row in the desired block. The **Select All** or **Deselect All** buttons can be used to select or deselect all objects in the table. The table summary at the bottom of the table includes the total number of items that are selected.

### Filtering



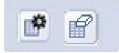
If you select the **Filter Row** button a row appears under the title row of the table. Select **Filter** under a column to define a filter for that column to limit the entries in a table. Tables can be filtered to show only those entries most important to you. The filtered view can be toggled on and off by selecting the check box next to the desired filter in the filter row. Select the **Clear All Filters** button to return to the complete listing. The table summary includes the total number of items that pass the filter criteria in addition to the total number of items.

### Sorting



The **Edit Sort** and **Clear All Sorts** buttons are used to perform multi-column sorts of objects in the table in ascending or descending order. Click **Edit Sort** to define sorts for columns in a table. Alternatively, single column sorting can be performed by selecting the ^ in the column header to change from ascending to descending order. Click **Clear All Sorts** to return to the default ordering.

## Column configuration



The column configuration buttons give you the ability to select which columns to display for folders in the Systems Management tree view. Click the **Configure Columns** button to arrange the columns in the table in a desired order or hide columns from view. All available columns are listed in the Columns list box by their column name. You select the columns you want displayed or hidden by checking or unchecking the box next to the column names. The column order is manipulated by clicking on a column name from the list box and using the arrow buttons to the right of the list to change the order of the selected column. When you have completed the configuration of the columns, click **OK**. The columns appear in the table as you specified. If you want to go back to the original layout of the table, click the **Reset Column Order, Visibility, and Widths** button from the table toolbar. Select one or more of the properties to be reset back to their original layout, click **OK** to save.

## Views menu

The **views menu** is displayed on the toolbar and is only available for table selections when working with servers, custom groups, exceptions view, or attention LEDs view. This table option allows you to display different sets of attributes (columns) in the table. Figure 14 on page 37 displays an example of the **Views** options when you are working with servers. Figure 15 on page 38 displays an example of the **Views** options when you are working with user-defined custom groups.

You can also change the attributes for each view. For example, if you choose **Default** from the views menu and you do not want Available Processing Units appearing in the table, use the **Configure columns** table toolbar button and deselect **Available Processing Units**, then click **OK**. Now, when you choose the **Default** view the view displays the table without the Available Processing Units column. To go back to the original default view for any of the views use the **Reset Column Order, Visibility, and Widths** table toolbar button (see “Column configuration”).

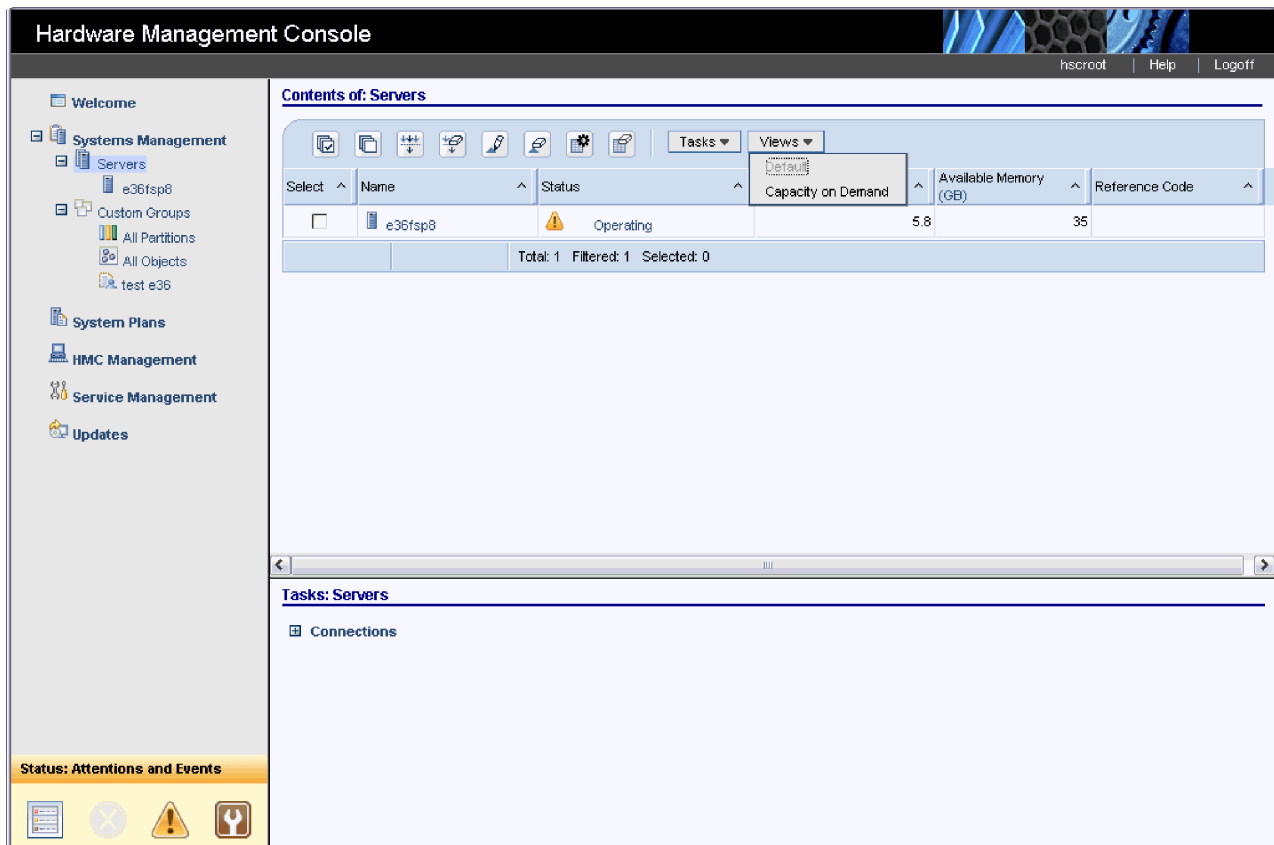


Figure 14. Views menu for servers

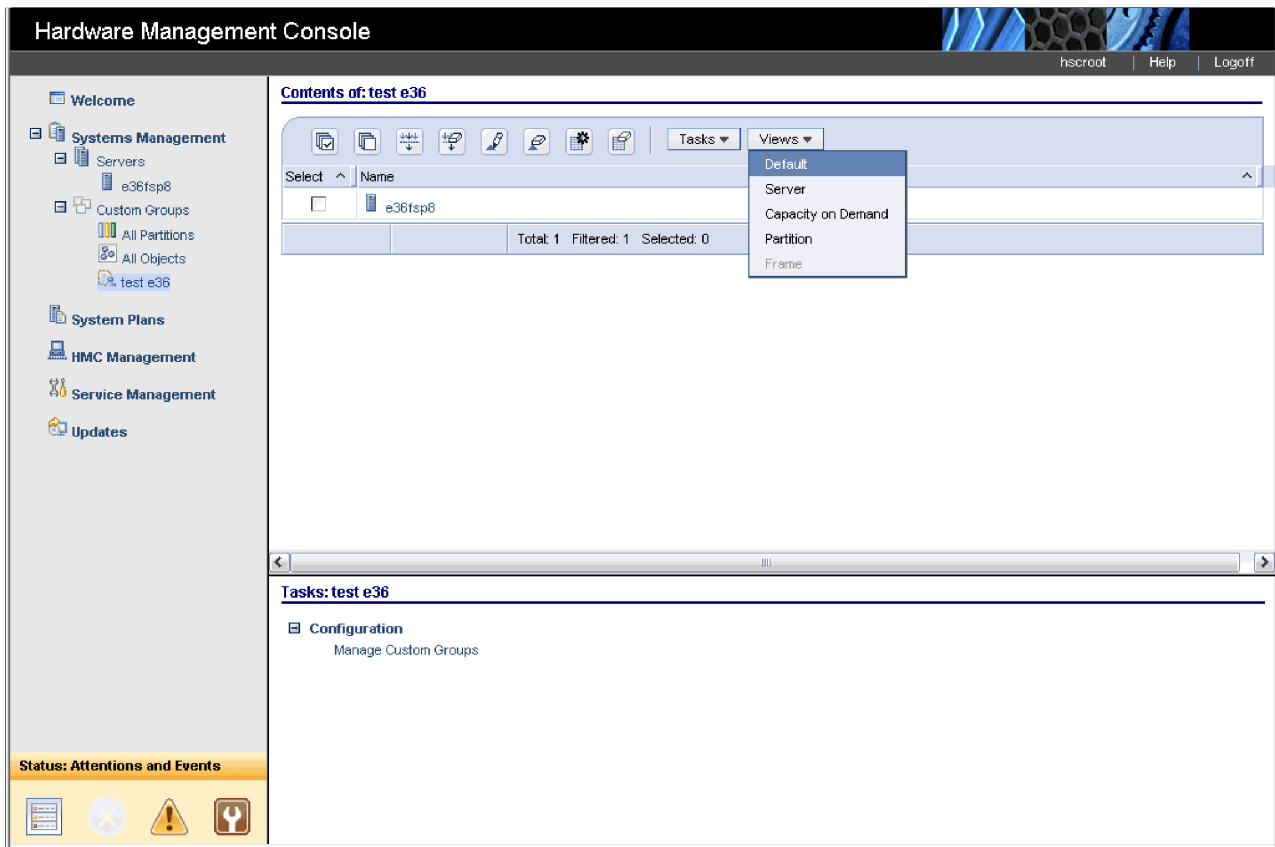


Figure 15. Views menu for user-defined custom groups

## Status bar

The status bar in the bottom left pane, as shown in Figure 16, provides a view of overall system status, including managed system resources and the HMC. A status-sensitive title, background color, and indicator icons are part of the status bar. The status indicators (icons) appear in color when one or more objects go into unacceptable status, have attention LEDs, or have open serviceable events. Otherwise, the status icon is not available.



Figure 16. Status bar

Click any of the individual icons in the status bar to view a listing of resources with specific status. For example, select the Unacceptable icon to view all resources in an unacceptable state. The results are displayed in a table in the work pane.

## Status: Unacceptable



If any managed object is in unacceptable state, the Unacceptable indicator (icon) is activated on the status bar. When you select the **Unacceptable** indicator (icon) it displays a table in the work pane of only the

objects in an unacceptable state. By clicking on the icon, help information is opened describing unacceptable status (Error state) of the server or partition. You can also use the **Views** menu to display your preferred table column configuration for these objects, see “Views menu” on page 36.

## Status: Attention LEDs



If any managed object’s Attention LED is activated, the Attention LED (icon) is activated in the status bar. When you select the **Attention LED** indicator (icon) it displays a table in the work pane of only the objects in Attention LED. By clicking on the icon, help information is opened guiding you in problem determination. You can also use the **Views** menu to display your preferred table column configuration for these objects, see “Views menu” on page 36 for more information.

## Status: Serviceable Events



If at least one serviceable event for the HMC or a managed object is in open state, the serviceable event icon, is activated in the status bar. By clicking on the icon the **Manage Serviceable Events** task is accessed with the filter set to view all open events.

## Status Overview



When you select the **Status Overview** icon, it displays a highly visible and detailed summary of system status in the work pane, as shown in Figure 17 on page 40. It displays details about any errors (objects with unacceptable state), attention LEDs active, or open serviceable events found for the HMC or managed objects. It also summarizes the total number of errors, attention LEDs, and open serviceable events by object type. Object types include the server, partition, frames, and the HMC. When any of these conditions are present, links are available to drill down and display all objects with the particular state in the work pane.

**Note:** Drilling down in the Status Overview work pane is the same as using the status bar indicators.

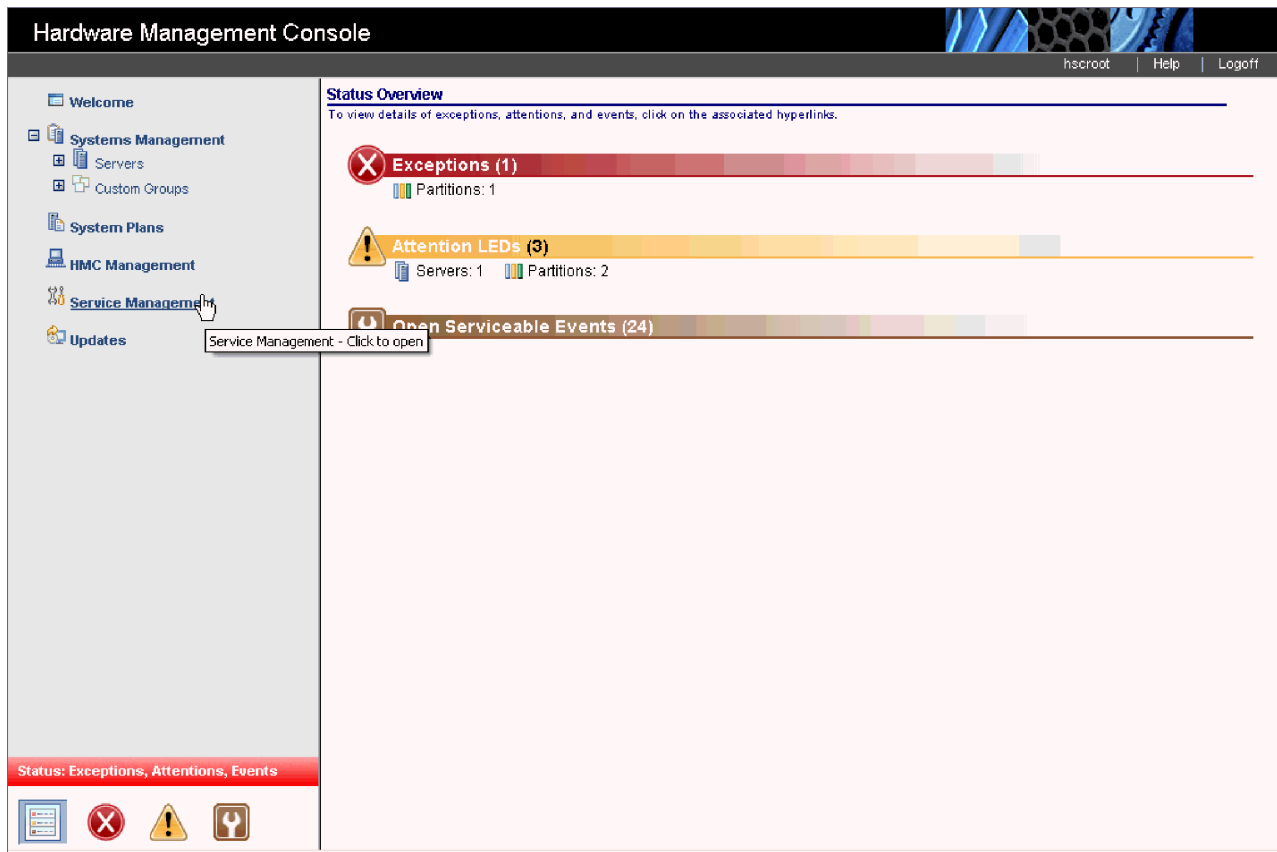


Figure 17. Status overview



---

## Chapter 3. Systems Management - Servers

**Systems Management** displays tasks to manage servers, logical partitions, and frames. Use these tasks to set up, configure, view current status, troubleshoot, and apply solutions.



This chapter describes the tasks used when a server is selected.

To launch these tasks, see “Launching tasks for managed objects” on page 24. The following sets of tasks are represented in the tasks pad, tasks menu,

- “Operations” on page 42
- “Configuration” on page 47
- “Connections” on page 51
- “Hardware (Information)” on page 54
- “Dynamic Logical Partitioning” on page 75
- “Updates” on page 56
- “Serviceability” on page 56
- “Capacity on Demand” on page 61

or context menu. The tasks listed in the tasks pad change as selections are made in the work area. The context is always listed at the top of the tasks pad in the format Task: Object. These tasks are listed when a managed system is selected and the context is Tasks: Server-9117-MMA-SN1234ABC.

---

### Properties

The **Properties** task displays the selected managed system’s properties. This information is useful in system and partition planning and resource allocation. These properties include:

#### General

The **General** tab displays the system’s name, serial number, model and type, state, attention led state, service processor version, maximum number of partitions, assigned service partition (if designated), and power off policy information.

#### Processor

The **Processor** tab displays information about the managed system’s processors including maximum number of processors per partition, installed processing units, deconfigured processing units, available processing units, configurable processing units, minimum number of processing units per virtual processor and maximum number of shared processor pools. A table displays partition processor usage.

#### Memory

The **Memory** tab displays information about the managed system’s memory including installed memory, deconfigured memory, available memory, configurable memory, memory region size, current memory available for partition usage, and system firmware current memory. A table displays partition memory usage.

#### I/O

The **I/O** tab displays the physical I/O resources for the managed system. The assignment of I/O slots and partition and adaptor-type information are displayed, grouped by units. Select the link in the **Slot** column to display the physical I/O properties of each resource. Select **I/O Pools** to display all of the I/O pools found in the system and the partitions that are participating in the pools.

## Power-On Parameters

The **Power-On Parameters** tab displays both the default manufacturing settings and the current managed system settings for boot mode. Changing these setting in the **Next** column will take effect on the next restart of the managed system.

## Capabilities

The **Capabilities** tab displays the runtime capabilities of this server, such as Capacity On Demand, Micro-Partitioning, Huge Page memory, etc. Select **Help** for more information on the capabilities listed.

## Advanced

The **Advanced** tab displays huge page memory capabilities on the managed system, including available huge page memory, configurable huge page memory, current page size, and current maximum huge page memory. To change memory allocation on systems with huge page table support, set the Requested huge page memory (in pages) field to the desired memory. To change the requested value for huge page memory, the system must be powered off.

Related HMC CLI commands:

- “chhwres” on page 152
- “chsyscfg” on page 164
- “lshwres” on page 194
- “lsled” on page 198
- “lssyscfg” on page 211

---

## Update Password

Use the **Update Password** task to update HMC access and Advanced System Management Interface (ASMI) passwords on the managed system.

The first time you access a managed system using an HMC, the system prompts you to enter passwords for each of the following:

- Hardware Management Console: HMC access
- Advanced System Management Interface: General
- Advanced System Management Interface: Admin

If you are using an HMC to access the managed system before all required passwords have been set, enter the appropriate password for each password that is presented in the Update Password task.

If another HMC subsequently needs access to this managed system, upon attempting to access this HMC the user is presented with the *Update Password Failed Authentication* window, which will prompt for the HMC access password you entered.

In the event that the HMC access password changes while you are logged in to the managed system, your HMC will discover that it can no longer authenticate after it attempts to reconnect to that managed system. This will result in a state of *Failed Authentication* for that managed system. You will be required to enter the new password before any actions can be performed.

---

## Operations

**Operations** contains the tasks for operating servers. The following are represented in the **Operations** tasks.

- “Restart” on page 70
- “Shut Down” on page 70
- “Power Off” on page 43
- “LED Status” on page 43
- “Schedule Operations” on page 44
- “Advanced System Management (ASM)” on page 46

- “Utilization Data” on page 46
- “Rebuild” on page 46
- “Change Password” on page 47

## Power On

Use the **Power On** task to start a managed system.

Choose from three different options to start your managed system:

- **Partition standby:** When the Partition standby power-on is completed, the system will be in standby mode. Partition standby mode allows you to create and activate logical partitions.
- **System profile:** Powers on the system according to a predefined set of system profiles. Select the system profile that you want to use from the list.
- **Partition auto start :** Powers on the managed system to partition standby mode and then activates all partitions that are marked as auto start or those partitions that were running when the system shut down. For example, if you create a partition with four processors, dynamically remove one processor from the logical partition, and then shut down the system, the partition auto start option activates this partition with three processors because the three-processor configuration was the last configuration used. The Hardware Management Console (HMC) ignores whatever is specified in the profile for the partition. You can create and activate logical partitions in partition auto start mode.

## Power Off

This task shuts down the managed system. Powering off the managed system will make all partitions unavailable until the system is again powered on.

Before you power off the managed system, ensure that all logical partitions have been shut down and that their states have changed from Running to Ready. For more information on shutting down a logical partition, see “Shut Down” on page 70

If you do not shut down all logical partitions on the managed system before you power off the managed system, the managed system shuts down each logical partition before the managed system itself powers off. This can cause a substantial delay in powering off the managed system, particularly if the logical partitions are not responsive. Further, the logical partitions might shut down abnormally, which could result in data loss and further delays when you activate the logical partitions once more.

Choose from the following options:

### Normal power off

The Normal power off mode shuts down the system’s operations in a controlled manner. During the shutdown, programs running active jobs are allowed to perform cleanup (end-of-job processing).

### Fast power off

The Fast power off mode shuts down the system by stopping all active jobs immediately. The programs running those jobs are not allowed to perform any cleanup. Use this option when you need to shut down the system because of an urgent or critical situation.

Related HMC CLI commands:

- “chsysstate” on page 171

## LED Status

This task contains the tasks for viewing system attention LED information, lighting specific LEDs to identify a system component, and testing all LEDs on a managed system.

The system provides several LEDs that help identify various components, such as enclosures or field replaceable units (FRUs), in the system. For this reason, they are called *Identify* LEDs. Individual LEDs are

located on or near the components. The LEDs are located either on the component itself or on the carrier of the component (for example, memory card, fan, memory module, or processor). LEDs are either green or amber. Green LEDs indicate either of the following:

- Electrical power is present.
- Activity is occurring on a link. (The system could be sending or receiving information.)

Amber LEDs indicate a fault or identify condition. If your system or one of the components on your system has an amber LED turned on or blinking, identify the problem and take the appropriate action to restore the system to normal. For more information on troubleshooting an amber LED indicating a fault, see *System p Problem Analysis*, SA76-0111.

You can activate or deactivate the following types of identify LEDs:

#### **Identify LED for an enclosure**

If you want to add an adapter to a specific drawer (enclosure), you need to know the machine type, model, and serial number (MTMS) of the drawer. To determine whether you have the correct MTMS for the drawer that needs the new adapter, you can activate the LED for a drawer and verify that the MTMS corresponds to the drawer that requires the new adapter.

#### **Identify LED for a FRU associated with a specified enclosure**

If you want to hook up a cable to a specific I/O adapter, you can activate the LED for the adapter which is a field replaceable unit (FRU), and then physically check to see where to hook up the cable. This can be especially useful when you have several adapters with open ports.

You can deactivate a system attention LED or a logical partition LED. For example, you might determine that a problem is not a high priority and decide to repair the problem at a later time. However, you want to be alerted if another problem occurs, so you must deactivate the system attention LED so that it can be activated again if another problem occurs.

Choose from the following options:

#### **View System Attention LED**

Displays the current system attention LED and corresponding partition LED states for the selected system. From this task, you can activate or deactivate system attention LEDs.

#### **Identify LED**

Displays the current Identify LED states for all the location codes contained in the selected enclosure. From this task, you can select a single location code or multiple location codes to operate against and activate or deactivate the LED(s) by selecting the corresponding button.

#### **Test LED**

Initiates an LED Lamp Test against the selected system. All LEDs will activate for several minutes.

Related HMC CLI commands:

- “chled” on page 159
- “lsled” on page 198

## **Schedule Operations**

Use this task to create a schedule for certain operations to be performed on the managed system without operator assistance.

Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation. A schedule can be set for one operation or repeated many times.

For example, you could schedule power on or off operations for a managed system.

The **Scheduled Operations** task displays the following information for each operation:

- The processor that is the object of the operation.
- The scheduled date
- The scheduled time
- The operation
- The number of remaining repetitions

From the **Scheduled Operations** window you can:

- Schedule an operation to run at a later time
- Define operations to repeat at regular intervals
- Delete a previously scheduled operation
- View details for a currently scheduled operation
- View scheduled operations within a specified time range
- Sort scheduled operations by date, operation, or managed system

An operation can be scheduled to occur one time or it can be scheduled to be repeated. You will be required to provide the time and date that you want the operation to occur. If the operation is scheduled to be repeated, you will be asked to select:

- The day or days of the week that you want the operation to occur. (optional)
- The interval, or time between each occurrence. (required)
- The total number of repetitions. (required)

The operations that can be scheduled for the managed system are:

#### **Activate on a System Profile**

Schedules an operation on a selected system for scheduling activation of a selected system profile.

#### **Backup Profile Data**

Schedules an operation to back up profile data for a managed system

#### **Power Off Managed System**

Schedules an operation for a system power off at regular intervals for one or more managed systems.

#### **Power On Managed System**

Schedules an operation for a system power on at regular intervals for one or more managed systems.

To schedule operations on the managed system:

1. Open **Systems Management** from the navigation pane.
2. Select one or more managed systems to work with from the work pane.
3. In the tasks pad, select the **Operations** task category, then open **Schedule Operations**. The **Schedule Operations** window is displayed.
4. From the **Schedule Operations** window, click **Options** from the menu bar to display the next level of options:
  - To add a scheduled operation, point to **Options** and then click **New...**
  - To delete a scheduled operation, select the operation you want to delete, point to **Options** and then click **Delete**.
  - To update the list of scheduled operations with the current schedules for the selected objects, point to **Options** and then click **Refresh**.
  - To view a scheduled operation, select the operation you want to view, point to **View** and then click **Schedule Details...**
  - To change the time of a scheduled operation, select the operation you want to view, point to **View** and then click **New Time Range...**

- To sort the scheduled operations, point to **Sort** and then click one of the sort categories that appears.
5. To return to the HMC workplace, point to **Options** and then click **Exit**.

Use the online Help to get additional information for scheduling an operation.

## Advanced System Management (ASM)

If configured to do so, the HMC connects directly to the Advanced System Management (ASM) interface for a selected system from this task.

ASM is an interface to the service processor that allows you to set flags that affect the operation of the server, such as auto power restart, and to view information about the server, such as the error log and vital product data.

To connect to the Advanced System Management interface:

1. From the **System Management** tasks list, select **Operations**.
2. From the **Operations** task list, select **Advanced System Management (ASM)**.

For more information on the Advanced System Management interface, see Appendix E, “Advanced Systems Management Interface (ASMI),” on page 243.

Related HMC CLI commands:

- “asmmenu” on page 145

## Utilization Data

Use this task to set the HMC to collect resource utilization data for a specific managed system or for all systems the HMC manages. The HMC collects utilization data for memory and processor resources. You can use this data to analyze trends and make resource adjustments. The data is collected into records called events. Events are created at the following times:

- At periodic intervals (hourly, daily, and monthly)
- When you make system-level and partition-level state and configuration changes that affect resource utilization
- When you start up, shut down, and change the local time on the HMC

You must set the HMC to collect utilization data for a managed system before utilization data can display for the managed system.

- Use the **Enable** task to enable the collection of utilization data on a selected managed system.
- Use the **Disable** task to disable the collection of utilization data on a selected managed system.
- Use the **View** task and specify the time span desired to view the collected data for a selected managed system. Restrict the amount of data returned by specifying a maximum number of events.

Related HMC CLI commands:

- “chlpoutil” on page 160
- “lslpoutil” on page 201
- “rmlpoutil” on page 228

## Rebuild

Use the **Rebuild** task to extract the configuration information from the managed system and rebuild the information on the Hardware Management Console. The **Rebuild** operation does not disrupt the operation of the running server.

Rebuilding the managed system updates, or refreshes, the information on the HMC about the managed system. Rebuilding the managed system is useful when the state of the managed system is Incomplete. The Incomplete state means that the HMC cannot gather complete information from the managed system about logical partitions, profiles, or resources.

Rebuilding the managed system is different from simply refreshing the HMC window. When the managed system is rebuilt, the HMC extracts the information from the managed system. You cannot start other tasks while the HMC rebuilds the managed system. This process can take several minutes.

Related HMC CLI commands:

- “chsysstate” on page 171

## Change Password

Use the **Change Password** task to change the HMC access password on the selected managed system. After the password is changed, you must update the HMC access password for all other HMCs from which you want to access this managed system.

Enter the current password. Then enter a new password and verify it by entering it again.

Related HMC CLI commands:

- “chsyspwd” on page 170

---

## Configuration

**Configuration** contains the tasks for configuring your managed system and partitions. The following are represented in the **Configuration** tasks:

- “Create Logical Partition”
- “System Plans” on page 48
- “Manage Custom Groups” on page 48
- “View Workload Management Groups” on page 48
- “Partition Availability Priority” on page 48
- “Manage System Profiles” on page 49
- “Manage Partition Data” on page 49

## Create Logical Partition

Use this task to create a new AIX or Linux logical partition (LPAR) on your managed system. The Create LPAR Wizard helps you create a new logical partition and a default profile for the partition.

Ensure you have logical partition planning information before you use this wizard. Logical partition planning information can be found at the System Planning Tool (SPT) website at <http://www.ibm.com/systems/support/tools/systemplanningtool/>. The SPT is available to assist you in system planning, design, validation and to provide a system validation report that reflects your system requirements while not exceeding system recommendations.

You might also find it helpful to be familiar with logical partition concepts. Logical partitioning information can be found in the Logical Partitioning Guide, SA76-0098.

Use the online Help for additional information on logical partition creation.

Related HMC CLI commands:

- “mksyscfg” on page 217



## System Plans

These tasks record or import specifications for logical partitions, partition profiles, or hardware specifications on a chosen system.

A *system plan* is a specification of the logical partition configuration of a single managed system. A system plan is stored in a file that is called a *system-plan* file and has a file suffix of *.sysplan*. A system-plan file can contain more than one system plan, although multiple plans in a single file are not common.

The **System Plans** tasks creates a record of the hardware and partition configuration of a managed system at a given time. It records specifications for the logical partitions and partition profiles on the selected system. It can also record hardware specifications that the HMC is able to detect.

To maximize the information that the HMC can obtain from the managed system, power on the managed system and activate the logical partitions on the managed system before creating the new system plan.

The **System Plans** tasks are the same tasks that are available from the **System Plans** node from the navigation pane and are documented here: Chapter 6, “System Plans,” on page 89.

## Manage Custom Groups

Groups are comprised of logical collections of objects. You can report status on a group basis, allowing you to monitor your system in a way that you prefer.

You can also nest groups (a group contained within a group) to provide hierarchical or topology views.

One or more user-defined groups might already be defined on your HMC. Default groups are listed under the **Custom Groups** node under **Server Management**. The default groups are **All Partitions** and **All Objects**. You can create others, delete the ones that were created, add to created groups, create groups using the pattern match method, or delete from created groups by using the **Manage Custom Groups** task.

Use the online Help if you need additional information for working with groups.

## View Workload Management Groups

This task displays a detailed view of the workload management groups you have specified for this managed system. Each group displays the total number of processors, processing units for partitions using shared mode processing, and the total amount of memory allocated to the partitions in the group.

Related HMC CLI commands:

- “lshwres” on page 194
- “lssyscfg” on page 211

## Partition Availability Priority

Use this task to specify the partition-availability priority of each logical partition on this managed system.

The managed system uses partition-availability priorities in the case of processor failure. If a processor fails on a logical partition, and there are no unassigned processors available on the managed system, the logical partition can acquire a replacement processor from logical partitions with a lower partition-availability priority. This allows the logical partition with the higher partition-availability priority to continue running after a processor failure.

You can change the partition availability priority for a partition by selecting a partition and choosing an availability priority from those listed.

Use the online Help if you need additional information about prioritizing partitions.



Related HMC CLI commands:

- “chsyscfg” on page 164
- “lssyscfg” on page 211
- “mksyscfg” on page 217

## Manage System Profiles

A system profile is an ordered list of partition profiles that is used by the HMC to start the logical partitions on a managed system in a specific configuration.

When you activate the system profile, the managed system attempts to activate each partition profile in the system profile in the order specified. A system profile helps you activate or change the managed system from one complete set of logical partition configurations to another.

It is possible for you to create a system profile that has a partition profile that has overcommitted resources. You can use the HMC to validate the system profile against the currently available system resources and against the total system resources. Validating your system profile ensures that your I/O devices and processing resources are not overcommitted, and it increases the likelihood that the system profile can be activated. The validation process estimates the amount of memory needed to activate all of the partition profiles in the system profile. It is possible that a system profile can pass validation and yet not have enough memory to be activated.

Use this task to:

- **Create** new system profiles.
- Create a **Copy** of a system profile.
- **Validate** the resources specified in the system profile against the resources available on the managed system. The validation process indicates whether any of the logical partitions in the system profile are already active and whether the uncommitted resources on the managed system can meet the minimum resources specified in the partition profile.
- View the **Properties** of a system profile. From this task, you can view or change an existing system profile.
- **Delete** a system profile.
- **Activate** a system profile. When you activate a system profile, the managed system will attempt to activate the partition profiles in the order specified in the system profile.

Use the online Help if you need additional information about managing system profiles.

Related HMC CLI commands:

- “chsyscfg” on page 164
- “chsysstate” on page 171
- “lssyscfg” on page 211
- “mksyscfg” on page 217
- “rmsyscfg” on page 229

## Manage Partition Data

A partition profile is a record on the HMC that specifies a possible configuration for a logical partition. When you activate a partition profile, the managed system attempts to start the logical partition using the configuration information in the partition profile.

A partition profile specifies the desired system resources for the logical partition and the minimum and maximum amounts of system resources that the logical partition can have. The system resources specified within a partition profile includes processors, memory, and I/O resources. The partition profile can also

specify certain operating settings for the logical partition. For example, you can set a partition profile so that, when the partition profile is activated, the logical partition is set to start automatically the next time that you power on the managed system.

Each logical partition on a managed system that is managed by an HMC has at least one partition profile. You can create additional partition profiles with different resource specifications for your logical partition. If you create multiple partition profiles, you can designate any partition profile on the logical partition to be the default partition profile. The HMC activates the default profile if you do not select a specific partition profile to be activated. Only one partition profile can be active at one time. To activate another partition profile for a logical partition, you must shut down the logical partition before you activate the other partition profile.

A partition profile is identified by partition ID and profile name. Partition IDs are whole numbers used to identify each logical partition that you create on a managed system, and profile names identify the partition profiles that you create for each logical partition. Each partition profile on a logical partition must have a unique profile name, but you can use a profile name for different logical partitions on a single managed system. For example, logical partition 1 cannot have more than one partition profile with a profile name of normal, but you can create a profile named normal for each logical partition on the managed system.

When you create a partition profile, the HMC shows you all of the resources available on your system. The HMC does not verify if another partition profile is currently using a portion of these resources. Therefore, it is possible for you to overcommit resources. When you activate a profile, the system attempts to allocate the resources that you assigned to the profile. If you have overcommitted resources, the partition profile will not be activated.

For example, you have four processors on your managed system. Partition 1 profile A has three processors, and partition 2 profile B has two processors. If you attempt to activate both of these partition profiles at the same time, partition 2 profile B will fail to activate because you have overcommitted processor resources.

When you shut down a logical partition and reactivate the logical partition using a partition profile, the partition profile overlays the resource specifications of the logical partition with the resource specifications in the partition profile. Any resource changes that you made to the logical partition using dynamic logical partitioning are lost when you reactivate the logical partition using a partition profile. This is desirable when you want to undo dynamic logical partitioning changes to the logical partition. However, this is not desirable if you want to reactivate the logical partition using the resource specifications that the logical partition had when you shut down the managed system. Therefore, keep your partition profiles up to date with the latest resource specifications. You can save the current configuration of the logical partition as a partition profile. This allows you to avoid having to change partition profiles manually.

If you shut down a logical partition whose partition profiles are not up to date, and the logical partition is set to start automatically when the managed system starts, you can preserve the resource specifications on that logical partition by restarting the entire managed system using the partition autostart power-on mode. When the logical partitions start automatically, the logical partitions have the resource specifications that the logical partitions had when you shut down the managed system.

Use the Manage Partition Data tasks to:

- **Restore** partition data. If you lose partition profile data, use the **Restore** task in one of three ways:
  - Restore partition data from a backup file. Profile modifications performed after the selected backup file was created will be lost.
  - Restore merged data from your backup file and recent profile activity. The data in the backup file takes priority over recent profile activity if the information conflicts.

- Restore merged data from recent profile activity and your backup file. The data from recent profile activity takes priority over your backup file if the information conflicts.
- **Initialize** a partition profile. Initializing the partition data for a managed system will delete all of the currently defined system profiles, partitions, and partition profiles.
- **Backup** a partition profile to a file.
- **Delete** a backup of partition data.

Use the online Help if you need additional information about managing partition data.

Related HMC CLI commands:

- “bkprofdata” on page 146
- “rmprofdata” on page 229
- “rstprofdata” on page 234

---

## Connections

**Connections** tasks allow you to view the HMC connection status to service processors or frames, reset those connections, connect another HMC to the selected managed system, or connect another managed system to the HMC.

If you have selected a managed system in the work area, the following tasks pertain to that managed system. If you have selected a frame, the tasks pertain to that frame. For managed systems, the tasks are:

- **Service Processor Status** displays the HMC connection status to the service processor of a selected managed system. If you have selected a frame, **Service Processor Status** displays the state of the connection from the HMC to side A and side B of the bulk power assembly.

Related HMC CLI commands:

- “lssyscfg” on page 211
- “lssysconn” on page 212

- Use the **Reset or Remove Connections** task to remove or reset a managed system from the Contents area of the HMC.

Related HMC CLI commands:

- “rmsysconn” on page 230

- **Disconnect another HMC** drops the connection between the selected HMC and the selected managed system. The disconnected HMC will try to reconnect. If the disconnected HMC has a lock on the managed server, this task forces the selected HMC to release its lock.
- The **Add Managed System** task guides you through adding systems in the network to systems managed by this HMC.

Related HMC CLI commands:

- “mksysconn” on page 223

## Correcting a Connection Problem

To correct a connection problem between the HMC and the managed system or to correct the state of a managed system in *No Connection*, *Incomplete*, *Recovery*, *Error*, or *Failed Authentication* state, follow the procedures below.

### Correcting a No connection state for a managed system

The **No connection** state can occur when the HMC is not connected, or the handshake with the managed system failed.

Use this procedure for a system that was previously connected to the same HMC and is now in No connection state. If you have a new system, a new HMC, or have moved your system to a different HMC, refer to Correcting a connection problem between the HMC and a managed system.

1. From the **Systems Management - Servers** work pane, select the managed system.

2. Select **Connections - Service Processor Status**. Record the IP address of the service processor.
3. From the **HMC Management** work pane, select **Test Network Connectivity**.
4. Enter the IP address of the service processor and select **Ping**.
5. Choose from the following options:
  - If the ping is successful, go to step 6.
  - If the ping is not successful, go to step 7.
6. If the ping test is successful, perform the following steps:
  - a. In the **Systems Management - Servers** work pane, ensure that there are no reference codes displayed in the **Reference Code** column for the server in Incomplete state. **Note:** A steady reference code could indicate a hardware problem. If the reference code is a clickable link, click the reference code to display possible procedures to correct the problem. If the reference code is not a link or a solution is not presented, contact your next level of support or your hardware service provider.
  - b. Restart the HMC. For more information on restarting the HMC, see “Shut Down or Restart” on page 104.
  - c. If restarting the HMC does not resolve the problem, contact your next level of support or your hardware service provider.
7. If the ping test is not successful, perform the following steps:
  - a. In the **Systems Management - Servers** work pane, ensure that there are no reference codes displayed in the **Reference Code** column for the server in Incomplete state. **Note:** A steady reference code could indicate a hardware problem. If the reference code is a clickable link, click the reference code to display possible procedures to correct the problem. If the reference code is not a link or a solution is not presented, contact your next level of support or your hardware service provider.
  - b. If your system has a control panel, check to see if the power light is on. Choose from the following options:
    - If there is power to the managed system, go to step 8.
    - If there is no power to the managed system, “Power On” on page 43 the managed system. After the power is restored, wait 5 minutes for the service processor to re-IPL and the HMC to re-establish contact. If the system is equipped with redundant service processors, allow up to 20 minutes for this step.
8. Verify physical network connectivity:
  - a. Verify that the HMC and the service processor are correctly connected to your Ethernet network.
  - b. Verify that Ethernet link status is good on all network segments which exist between the HMC and the managed system.
  - c. If you think the network might be the problem, connect a cable from the HMC to the service processor and try pinging the failing system. Then choose from the following options:
    - If the ping is successful, put the cables back the way they were and correct the network problem. After the network problem is resolved, repeat this entire procedure.
    - If the ping is not successful, put the cables back the way they were and continue with step 8.d.
  - d. Reset the service processor using the following steps:
    - 1) “Power Off” on page 43 the server.
    - 2) Unplug the AC power cord and re-plug it back in.
    - 3) “Power On” on page 43 the server.
9. If the problem is not resolved by any of the above steps, contact your next level of support or your hardware service provider.

## Correcting an Incomplete state for a managed system

The **Incomplete** state can occur when the HMC failed to get all of the necessary information from the managed system.

To correct an **Incomplete** state, perform the following steps:

1. From the **Systems Management - Servers** work pane, select the managed system.
2. In the tasks pad, select **Operations - Rebuild**.
3. Select **Yes** to refresh the internal representation of the managed system on the HMC.
  - If the state remains **Incomplete**, rebuild the managed system several more times
  - If the state goes to **Recovery**, see “Correcting a Recovery state for a managed system.”
  - If the state does not remain in **Incomplete** or go to **Recovery**, continue with the next step.
4. In the tasks pad, select **Connections - Reset or Remove Connections** to reset the connection from the managed system to the HMC. If this fails, continue to the next step.
5. Restart the HMC. For more information on restarting the HMC, see “Shut Down or Restart” on page 104.
  - If the state goes to **Recovery**, see “Correcting a Recovery state for a managed system.”
  - If the state remains **Incomplete**, perform the following steps:
    - Verify that there is a redundant HMC.
    - Verify that no one is entering commands from the alternate HMC.
    - Repeat step 1 through 5. If it still fails, continue with the next step.
6. If the problem persists, contact your next level of support or your hardware service provider.

### Correcting a Recovery state for a managed system

The **Recovery** state can occur when the save area in the service processor assembly is not synchronized with the HMC.

To recover from the **Recovery** state, perform the following steps:

1. Restore partition data. For details, see the **Restore** task in “Manage Partition Data” on page 49. If this solves the problem, this ends the procedure.
2. If the problem is not resolved after restoring partition data, choose the option that describes what happened:
  - If the state remains **Recovery**, retry restoring partition data. If it fails a second time, follow the problem determination procedure for any reference codes you receive.
  - If the state changed to **Incomplete**, refer to “Correcting an Incomplete state for a managed system” on page 52.
  - If the state changed to **No Connection**, refer to “Correcting a No connection state for a managed system” on page 51.
3. If the problem persists, contact your next level of support or your hardware service provider.

### Correcting an Error state for a managed system

The **Error** state automatically generates a call to the service support center if the function is enabled.

If the automatic call support function is not enabled, contact your next level of support or your hardware service provider.

### Correcting a Failed Authentication state for a managed system

The **Failed Authentication** state can occur when the HMC access password for the managed system is not valid.

1. Do you have an HMC password?
  - **Yes:** Enter the HMC password and choose from the following options:
    - If the managed system goes to **Operating**, **Power Off**, or **Standby** state, the authentication was successful. This ends the procedure.
    - If the managed system goes to **No connection**, **Incomplete**, **Recovery**, or **Error** state, refer to Correcting the managed system operating state.

- **No:** Do you have an ASMI admin password?
    - **Yes:** Continue with step 2.
    - **No:** Contact your next level of support to request CE login. Then continue with step 2, using CE login instead of admin password for step 2.a.
2. Perform the following steps:
    - a. Login to the ASMI with admin authority. See “Advanced System Management (ASM)” on page 46.
    - b. Select **Login Profile**.
    - c. Select **Change Password**.
    - d. In the **User ID to change field**, select **HMC**.
    - e. Enter the ASMI’s admin password in the **Current password for user ID admin** field. **Note:** Do not enter the HMC user password.
    - f. Enter the ASMI’s admin password.
    - g. Enter a new HMC access password twice and click **Continue**.
    - h. From the **Systems Management - Servers** work pane, select the managed system.
    - i. Select **Update password**.
    - j. Input the new password that was set in step 2.g. This ends the procedure.

## Correcting a new connection problem between the HMC and a managed system

Use this procedure in the following situations:

- You have a new HMC
- You have a new system
- You moved your system to a different HMC

If your system was previously connected to the same HMC and is now in **No connection** state, refer to “Correcting a No connection state for a managed system” on page 51.

1. From the **Systems Management - Servers** work pane, select **Connections - Add Managed System** from the tasks pad. For more information, see “Connections” on page 51. Does the system appear in the work pane?
  - **Yes:** This ends the procedure.
  - **No:** Continue with step 2.
2. Check for network problems, cables, switches, link lights on the service processor, and so on. Was there a problem?
  - **Yes:** Correct the problem and return to step 1.
  - **No:** Continue with step 3.
3. Reset the service processor to force it to request a new IP address using the following steps:
  - a. “Power Off” on page 43 the server.
  - b. Unplug the AC power cord and re-plug it back in.
  - c. “Power On” on page 43 the server.
4. Did resetting the service processor resolve the problem?
  - **Yes:** This ends the procedure.
  - **No:** Contact your next level of support.

---

## Hardware (Information)

**Hardware (Information)** tasks are used to display information about the hardware attached to a selected managed system.

The following are represented in the **Hardware (Information)** tasks:

- “View RIO Topology” on page 56



## Adapters

Use the **Adapters** tasks to view information about the Host Ethernet Adapters (HEA) or Host Channel Adapters (HCA) for a selected managed system.

### Host Ethernet Adapter (HEA)

A Host Ethernet Adapter (HEA) allows multiple logical partitions to share a single physical Ethernet adapter.

Unlike most other types of I/O devices, you can never assign the HEA itself to a logical partition. Instead, multiple logical partitions can connect directly to the HEA and use the HEA resources. This allows these logical partitions to access external networks through the HEA without having to go through an Ethernet bridge on another logical partition.

Use the **Host Ethernet** task to display or configure the ports of the physical Host Ethernet Adapters (HEAs) on a selected managed system.

To configure a physical port on an HEA, select the port from the list and select Configure.

Use the online Help for additional information on configuring HEA ports.

Related HMC CLI commands:

- “chhwres” on page 152
- “lshwres” on page 194

### Host Channel Adapter (HCA)

Host Channel Adapters provide a managed system with port connections to other InfiniBand devices. That port can be connected to another HCA, a target device, or an InfiniBand switch that redirects the data coming in on one of its ports out to a device attached to another of its ports.

Use the **Host Channel** task to show a list of the HCAs for the managed system. You can select an HCA from the list to display the current partition usage for the HCA.

From this task you can display:

- The physical location of each HCA on the managed system.
- The number of Globally Unique Identifiers (GUIDs) that are in use on each HCA.
- The number of GUIDs on each HCA that are available to be assigned to logical partitions.
- HMC management status. HCAs that are unable to be managed by an HMC are in an error state.
- The logical partition usage for a selected HCA.

Related HMC CLI commands:

- “lshwres” on page 194

## Virtual IO Adapters

Use the **Virtual IO Adapters** commands to view the topology of currently configured virtual scsi and virtual ethernet adapters on a selected partition.

Use the **SCSI** task to view the topology of virtual SCSI adapters on a partition. Displayed are:

- Adapter name
- Backing device
- Remote partition
- Remote Adapter
- Remote Backing Device

Use the **Ethernet** task to view the current virtual ethernet configuration for the partition.

- Adapter name
- Virtual LANs
- I/O Server
- Server Virtual Adapter
- Shared Adapter

Partitions assigned to a VLAN that is bridged have access to a external network via a physical shared ethernet adapter owned by a Virtual I/O Server.

## View RIO Topology

This task displays the current RIO topology for the selected managed system and any discrepancies between the current topology and the last valid topology.

High Speed Link (HSL), also known as Remote I/O (RIO), resources provide the connection between system I/O busses and the system processor. HSL/RIO resources are normally configured in loops with the system unit having an HSL/RIO controller resource that handles routing of the data between the system processor and the system I/O busses. System I/O busses connect to the loop with HSL I/O adapter or RIO adapter resources.

Use this task to display the current RIO topology of the selected managed system. Current Topology displays the current topology. Any discrepancies between the current topology and the last valid topology are identified as errors. The following information is shown:

- The starting location of the physical RIO cable and the RIO connection (cable to port)
- The ending location of the physical RIO cable and the RIO connection (cable to port)
- Starting Node Type Displays the values of the node. Possible values are Local Bridge, Local NIC, Remote Bridge, and Remote NIC
- Link Status Displays the leading port status
- Cable Length Displays the length of the RIO cables. Errors occur when the actual cable lengths are different from the expected cable lengths
- The serial number of the power-controlling managed system
- The serial number of the function-controlling managed system

---

## Updates

**Updates** tasks perform a guided update of managed system, power, or I/O Licensed Internal Code.

These **Update** tasks are the same tasks that are available from the Updates node of the navigation pane and are documented here: “Managed System Updates” on page 116.

---

## Serviceability

Problem Analysis on the HMC automatically detects error conditions and reports to you any problem that requires service to repair it. These problems are reported to you as serviceable events. Use the **Manage Events** task to view specific events for selected systems. However, if you notice a problem occurred or you suspect a problem is affecting the system but Problem Analysis has not reported it to you, use the **Create Serviceable Event** task to report the problem to your service provider.

The following are represented in the **Serviceability** tasks:

- “Manage Serviceable Events” on page 112
- “Create Serviceable Event” on page 107
- “Reference Code History” on page 58
- “Control Panel Functions” on page 58
- “Hardware” on page 58
- “Manage Dumps” on page 60



- “Collect VPD” on page 60
- “Edit MTMS” on page 61
- “FSP Failover” on page 61

## Manage Serviceable Events

Problems on your managed system are reported to the HMC as serviceable events. The **Manage Serviceable Events** task allows you view the problem, manage problem data, call home the event to your service provider, or repair the problem.

To set the criteria for the serviceable events you to view:

1. Open the **Manage Serviceable Events** task from the tasks pad.
2. From the **Manage Serviceable Events** window provide event criteria, error criteria, and FRU criteria.
3. Click **OK** when you have specified the criteria you want for the serviceable events you want to view.
4. Select **ALL** if you do not want the results filtered.

The **Serviceable Events Overview** panel displays all of the events that match your criteria. The information displayed in the compact table view includes:

- Problem Number
- PMH Number
- Reference Code - Click on the Reference code to display a description of the problem reported and actions that may be taken to fix the problem.
- Status of the problem
- Last reported time of the problem
- Failing MTMS of the problem

The full table view includes more detailed information, including reporting MTMS, first reported time, and serviceable event text.

Select a serviceable event and use the **Selected** drop down menu to:

- **View event details:** FRUs associated with this event and their descriptions.
- **Repair the event:** Launch a guided repair procedure, if available.
- **Call home the event:** Report the event to your service provider.
- **Manage event problem data:** View, call home, or offload to media data and logs associated with this event.
- **Close the event:** After the problem is solved, add comments and close the event.

Use the online Help if you need additional information on managing serviceable events.

## Create Serviceable Event

Use this task to report a problem on your managed system to your service provider or to test problem reporting on your managed system.

Submitting a problem is dependent upon whether you have customized your HMC to use the Remote Support Facility (RSF) and if it is authorized to automatically call for service. If so, the problem information and service request is sent to the service provider automatically with a modem transmission.

To report a problem on your managed system:

1. Open the **Create Serviceable Event** task from the Service Management work pane.
2. From the **Report a Problem** window, enter a brief description of your problem in the **Problem Description** input field and then click **Request Service**.

or

To test problem reporting from the **Report a Problem** window:

1. Select **Test automatic problem reporting** and enter *This is just a test* in the **Problem Description** input field.
2. Click **Request Service**.

The problems are reported to the service provider for the managed system. Reporting a problem sends to the service provider the information you provide on the **Report a Problem** window, and machine information that identifies the console.

Use the online Help if you need additional information for reporting a problem or testing if problem reporting works.

## Reference Code History

Reference codes provide general diagnostic, troubleshooting, and debugging information.

The most recent reference codes are displayed. To view a history of reference codes, enter the number of codes to retrieve from the history and select **Go**. If detailed information is available on the managed system you are viewing, select the desired reference code to view the details of a specific reference code.

Related HMC CLI commands:

- “lsrefcode” on page 207

## Control Panel Functions

This task displays the available virtual control panel functions for the managed system selected.

**(20) Type, Model, Feature** displays the managed system’s machine type, model, and feature code. Also displayed are the CEC IPL Type and the FSP IPL Type for the managed system.

Related HMC CLI commands:

- “lssyscfg” on page 211

## Hardware

These tasks are used to add, exchange, or remove hardware from the managed system. From the hardware tasks you can display a list of installed FRUs or enclosures and their locations. Select a FRU or an enclosure and launch a step-by-step procedure to add, exchange, or remove the unit.

**Hardware** tasks include:

- “Add FRU”
- “Add Enclosure” on page 59
- “Exchange FRU” on page 59
- “Exchange Enclosure” on page 59
- “Remove FRU” on page 59
- “Remove Enclosure” on page 60
- “Power On/Off IO Unit” on page 60

### Add FRU

Use the **Add FRU** task to locate and add a Field Replaceable Unit (FRU).

To add a FRU:

1. Select an enclosure type from the drop down list.
2. Select an FRU type from the list.
3. Click **Next**.
4. Select a location code from the displayed list.
5. Click **Add** to add the selected enclosure location to **Pending Actions**.

6. Click **Launch Procedure** to begin adding the selected FRU type to the enclosure locations identified in **Pending Actions**.
7. Click **Finish** when you have completed the FRU installation process.

## Add Enclosure

Use the **Add Enclosure** task to locate and add an enclosure.

To add an enclosure:

1. Select an enclosure type, then click **Add** to add the selected enclosure type's location code to **Pending Actions**.
2. Click **Launch Procedure** to begin adding the enclosures identified in **Pending Actions** to the selected system.
3. Click **Finish** when you have completed the enclosure installation process.

## Exchange FRU

Use the **Exchange FRU** task to exchange one FRU with another.

To exchange a FRU:

1. Select an installed enclosure type from the drop down list.
2. From the displayed list of FRU types for this enclosure, select an FRU type.
3. Click **Next** to display a list of locations for the FRU type.
4. Select a location code for a specific FRU.
5. Click **Add** to add the FRU location to **Pending Actions**.
6. Select **Launch Procedure** to begin replacing the FRUs listed in **Pending Actions**.
7. Click **Finish** when you have completed the installation.

## Exchange Enclosure

Use the **Exchange Enclosure** task to exchange one enclosure for another.

To exchange an enclosure:

1. Select an installed enclosure, then click **Add** to add the selected enclosure's location code to **Pending Actions**.
2. Click **Launch Procedure** to begin replacing the enclosures identified in **Pending Actions** in the selected system.
3. Click **Finish** when you have completed the enclosure replacement process

## Remove FRU

Use the **Remove FRU** task to remove a FRU from your managed system.

To remove a FRU:

1. Select an enclosure from the drop down list to display a list FRU types currently installed in the selected enclosure.
2. From the displayed list of FRU types for this enclosure, select an FRU type.
3. Click **Next** to display a list of locations for the FRU type.
4. Select a location code for a specific FRU.
5. Click **Add** to add the FRU location to **Pending Actions**.
6. Select **Launch Procedure** to begin removing the FRUs listed in **Pending Actions**.
7. Click **Finish** when you have completed the removal procedure.

## Remove Enclosure

Use the **Remove Enclosure** task to remove an enclosure.

To remove an enclosure:

1. Select an enclosure type, then click **Add** to add the selected enclosure type's location code to **Pending Actions**.
2. Click **Launch Procedure** to begin removing the enclosures identified in **Pending Actions** from the selected system.
3. Click **Finish** when you have completed the enclosure removal process.

## Power On/Off IO Unit

Use the **Power On/Off IO Unit** task to power on or off an IO unit.

Only units or slots that reside in a power domain can be powered on or off. The corresponding power on/off buttons will be disabled for location codes that are not controllable by the HMC.

## Manage Dumps

These tasks are used to manage system, service processor, and power subsystem dumps for systems managed by the HMC.

### system dump

A collection of data from server hardware and firmware, either after a system failure or a manual request. Only perform a system dump under the direction of your next level of support or your service provider.

### service processor dump

A collection of data from a service processor either after a failure, external reset, or manual request.

### power subsystem dump

A collection of data from Bulk Power Control service processor. This is only applicable to certain models of managed systems.

Use the **Manage Dumps** task to:

- Initiate a system dump, a service processor dump, or a power subsystem dump (if applicable).
- Modify the dump capability parameters for a dump type before initiating a dump.
- Delete a dump.
- Copy a dump to media such as a DVD-RAM.
- Copy a dump to another system using FTP.
- Call home a dump by using the Call Home feature to transmit the dump back to your service provider, for example IBM Remote Support, for further analysis.
- View the offload status of a dump as it progresses.

Use the online Help if you need additional information for managing dumps.

## Collect VPD

Use this task to copy Vital Product Data (VPD) to removable media.

The managed system has VPD that is stored internally. The VPD consists of information such as how much memory is installed, and how many processors are installed. These records can provide valuable information which can be used by remote service and service representatives so that they can help you keep the firmware and software on your managed system up to date.

The information in the VPD file can be used to complete the following types of orders for your managed system:

- Install or remove a sales feature
- Upgrade or downgrade a model
- Upgrade or downgrade a feature

Using this task, this information can be sent to removable media (diskette, DVD-RAM, or memory key) for use by you or your service provider.

Use the online Help if you need additional information for collecting VPD.

## Edit MTMS

Use this task to display or edit the model, type, machine serial (MTMS) or configuration ID of an enclosure.

The MTMS value or configuration ID for an expansion unit may need to be edited during a replacement procedure.

Use the online Help if you need additional information for editing MTMS.

## FSP Failover

Use the **FSP Failover** task to enable a secondary service processor if your managed system's primary service processor fails.

**FSP Failover** capability is designed to eliminate customer outages due to service processor hardware failures. If a redundant service processor is supported for the current system configuration, use the **Setup** task to set up FSP Failover for the selected managed system. Use the **Initiate** task to initiate FSP Failover for the selected managed system.

---

## Capacity on Demand

**Capacity on Demand (CoD)** tasks activate inactive processors or memory that are installed on your managed server.

Capacity on Demand (COD) allows you to nondisruptively activate (no boot required) processors and memory. Capacity on Demand also gives you the option to temporarily activate capacity to meet intermittent performance needs, to activate additional capacity on a trial basis, and to access capacity to support operations in times of need.

The following are represented in the **Capacity on Demand** tasks:

- "Capacity Upgrade on Demand" on page 62
- "On/Off Capacity on Demand" on page 63
- "Trial Capacity on Demand" on page 63
- "Utility Capacity on Demand" on page 64
- "Reserve Capacity on Demand" on page 64
- "Advanced POWER Virtualization" on page 65
- "Enterprise Enablement" on page 66
- "Other Advanced Functions" on page 67

Use the **Enter CoD Code** task to enter any CoD codes that you have obtained for your system.

This code can be any of the following types of CoD codes:

- CUoD processor activation code
- CUoD memory activation code
- Trial CoD processor code

- Trial CoD memory code
- On/Off CoD processor enablement code
- On/Off CoD memory enablement code
- On/Off CoD capacity termination code
- Reserve CoD capacity prepaid code
- Utility CoD enablement code
- Utility CoD reporting code
- Utility CoD termination code

Use the **View History Log** task to see the CoD history log for your system. The CoD history log contains information about the CoD events that have occurred on your system. The entries are shown in chronological order, starting with the most recent entry. You can see the date and time that each event occurred and a description of each event.

Related HMC CLI commands:

- “chcod” on page 148
- “lscod” on page 188

## Capacity Upgrade on Demand

Capacity Upgrade on Demand (CUoD) is permanent capacity for nondisruptive growth.

You can permanently activate inactive processors and memory units by purchasing an activation feature and entering the provided activation code. Capacity Upgrade on Demand (CUoD) enables you to permanently activate one or more inactive processors or memory units without requiring you to restart your server or interrupt your business.

You can order activation features for a new server, a server model upgrade, or an installed server. After you place your order, you will receive a code that activates inactive processors or memory units. For a new server or a server model upgrade, your order can contain one or more activation features for processors or memory units, which results in one or more activation codes. In this case, the activation codes are entered before the server is sent to you.

When you order Capacity Upgrade on Demand (CUoD) activation features for an installed server, you must determine whether you want to permanently activate some or all of your inactive processors or memory units. You must order one or more activation features and then use the resulting one or more activation codes to activate your inactive processors or memory units.

Contact your IBM Business Partner or IBM sales representative to place your order for one or more activation features.

### Notes:

- It can take several days to process an order. You can use a one-time no-charge Trial Capacity on Demand for 30 days to satisfy workload requirements while your order for permanent activation of additional capacity is being fulfilled. For more information, see [Ordering Trial Capacity on Demand](#).
- An order for activation features will process more quickly if you do not include any miscellaneous features with the order.

Use the **View Code Information** task to view the information used to generate a CUoD processor activation code for the selected managed system. If you want to save this information to a file, select **Save**.

Related HMC CLI commands:

- “chcod” on page 148
- “lscod” on page 188

## On/Off Capacity on Demand

On/Off Capacity on Demand (On/Off CoD) is temporary capacity for fluctuating workloads.

You can activate processors or memory units for a number of days, as your business peaks demand, by using inactive resources on a temporary basis. With On/Off CoD, you can temporarily activate and deactivate processors and memory units to satisfy business peaks. After you request that a number of processors or memory units be made temporarily available for a specified number of days, those processors and memory units are available immediately. You can start and stop requests for On/Off CoD, and you can also change the number of resources or days in a running On/Off request. This offering has contract requirements.

To take advantage of On/Off Capacity on Demand (CoD), you must order an On/Off CoD enablement feature. The enablement feature provides the On/Off CoD enablement code that allows you to request temporary activation of inactive processors or memory units by entering the code on your server.

To order On/Off Capacity on Demand (CoD), contact your IBM Business Partner or IBM sales representative. Your IBM Business Partner or IBM sales representative guides you through the completion of the required On/Off CoD contracts with IBM and places a customer order for an On/Off CoD enablement feature.

Use the **Manage** task to activate or deactivate processors or memory units or to change the number or resources or days in a running On/Off CoD request.

Use the **View Capacity Settings** task to view:

- The On/Off CoD state on the selected managed system.
- The number of active On/Off CoD processors or memory and inactive processors or memory on the managed system.
- The number of processor or memory days and hours remaining in the current On/Off CoD request.
- The number of unreturned On/Off CoD processors or memory from a previous On/Off CoD request.
- The number of processor or memory days available for new On/Off CoD requests.

Use the **View Billing Information** task to view or save information used to manually report On/Off CoD processor or memory billing information.

Use the **View Code Information** task to view the information used to generate a On/Off CoD processor or memory enablement code for the selected managed system. If you want to save this information to a file, select **Save**.

Related HMC CLI commands:

- “chcod” on page 148
- “lscod” on page 188

## Trial Capacity on Demand

Trial Capacity on Demand is temporary capacity for workload testing or any one time need.

You can evaluate the use of inactive processors, memory, or both, at no charge using Trial CoD. After it is started, the trial period is available for 30 power-on days. This means the trial period advances only while the server is powered on. You can use the HMC to stop a current CoD trial for processors or memory units before the trial automatically expires. If you choose to stop the trial before it expires, you cannot restart it and you forfeit any remaining days.

You can activate your inactive processors or memory for a trial period by obtaining and entering a trial processor code or a trial memory code with Trial Capacity on Demand (CoD).



Before the trial period expires, you must either enter a Capacity Upgrade on Demand activation code to permanently activate the Trial CoD resources, or you must return the Trial CoD resources.

Use the **Stop** task to terminate Trial CoD.

Use the **View Capacity Settings** task to view the following settings for the selected managed system:

- The Trial CoD state.
- The number of activated Trial CoD processors or memory.
- The total number of power-on days and hours remaining until the current Trial CoD period expires.

Use the **View Code Information** task to view the information used to generate a Trial CoD code for the selected managed system. If you want to save this information to a file, select **Save**.

Related HMC CLI commands:

- “chcod” on page 148
- “lscod” on page 188

## Utility Capacity on Demand

Utility Capacity on Demand (Utility CoD) allows you to activate the inactive processors that are installed on your managed system to meet the variable workload demands of your business.

When you use Utility CoD, activated Utility CoD processors are placed in the shared processor pool and are used only as needed by uncapped partitions. If all non-Utility CoD processors in the shared processor pool are being used, and one or more uncapped partitions require additional resources, then the managed system allows the uncapped partitions to use one Utility CoD processor for one minute, and one Utility CoD processor minute of use is recorded. The managed system continues to use this Utility CoD processor and record processor minutes until the Utility CoD processor is no longer needed. The managed system continuously monitors the processor utilization within the shared processor pool. If additional processor resources are needed, the managed system automatically uses additional Utility CoD processors and records processor minutes for those processors. You pay only for the number of processor minutes that the Utility CoD processors are used. Optionally, you may prepay for Utility CoD usage.

Use the **Manage Utility CoD** task to:

- View the Utility CoD state
- Change the number of Utility CoD processors in the shared processor pool
- Set a processor minute usage limit

Use the **View Capacity Settings** task to see current information about Utility CoD, including usage and reporting information.

Use the **View Code Information** task to view the information used to generate a Utility CoD code for the selected managed system. If you want to save this information to a file, select **Save**.

Use the **View Shared Processor Utilization** task to view the distribution and utilization of processors in the shared processor pool.

Related HMC CLI commands:

- “chcod” on page 148
- “lscod” on page 188

## Reserve Capacity on Demand

Reserve Capacity on Demand (CoD) provides prepaid temporary capacity that is automatically used by the server to help meet the demands of business peaks.



With Reserve CoD, you can purchase a reserve capacity prepaid feature that represents a number of processor days. You can then activate the inactive processors using Reserve CoD as your business requires.

The reserve processors are put in the server shared processor pool, where they are used as needed by uncapped partitions. Whenever the capacity of the non-Reserve CoD processors in the shared processor pool reaches the maximum capacity of those processors and is no longer sufficient to support the server workload, then the Reserve CoD processors are used.

When a Reserve CoD processor is used, one processor day is subtracted from the prepaid number of processor days. You pay only for the number of processor days that the reserve processors are actually used. The processors can remain active until all of the reserve processor days that you have paid for have been used.

Because you have already paid for the reserve capacity before you use it, contracts and reporting are not necessary.

Use the **View Shared Processor Utilization** task to view the distribution and utilization of processors in the shared processor pool.

Related HMC CLI commands:

- “chcod” on page 148
- “lscod” on page 188

## Advanced POWER Virtualization

Advanced POWER Virtualization is a set of comprehensive systems technologies and services designed to enable you to aggregate and manage resources through a consolidated, logical view.

Advanced POWER enables the system for these features:

- Virtual I/O hosting
- Partition Load Manager
- Micro-Partitioning

Use the **Enter Activation Code** task to enter any Capacity on Demand advanced functions activation codes that you have obtained for your system. Specify the appropriate code in the Code field to activate any of the following on-demand functions:

- **Advanced POWER Virtualization:** Permanently activates the Advanced POWER Virtualization capabilities, which can include Virtual I/O Server and Micro-Partitioning.
- **Enterprise Enablement:** Permanently activates the Enterprise Enablement capabilities, which can include 5250 Commercial Processing Workload (5250 CPW) capacity for application processing.

Use the **View History Log** task to see the activation history log for Capacity on Demand advanced functions on your system. The history log contains information about the activations of Capacity on Demand advanced functions that have occurred on your system. Capacity on Demand advanced functions include Advanced POWER Virtualization and Enterprise Enablement.

A log entry is created each time an activation code is entered successfully, and an additional log entry is created for each capability that is enabled by the activation code. For each entry in the Capacity on Demand advanced functions activation history log, this table shows the date and time on the system when the entry was logged and a description of the log entry. The entries are shown in chronological order, starting with the most recent entry.

If the history log has wrapped, a message is shown at the bottom of the window. The history log can contain as many as eight activation code entries. (For each activation code entry, an additional log entry

is created for each capability that is enabled by the activation code.) When eight activation code entries have been logged to the history log, the next entry causes the history log to wrap (that is, the newest entry overlays the oldest entry).

Use the **View Code Information** task to view the information used to generate a CoD advanced functions activation code for the selected managed system. If you want to save this information to a file, select **Save**.

Related HMC CLI commands:

- “chcod” on page 148
- “lscod” on page 188

## Enterprise Enablement

Use the **Enterprise Enablement** tasks to enter an Enterprise Enablement activation code, view Enterprise Enablement code information, or view a history log of Enterprise Enablement activation activity.

Use the **Enter Activation Code** task to enter any Capacity on Demand advanced functions activation codes that you have obtained for your system. Specify the appropriate code in the Code field to activate any of the following on-demand functions:

- **Advanced POWER Virtualization:** Permanently activates the Advanced POWER Virtualization capabilities, which can include Virtual I/O Server and Micro-Partitioning.
- **Enterprise Enablement:** Permanently activates the Enterprise Enablement capabilities, which can include 5250 Commercial Processing Workload (5250 CPW) capacity for application processing.

Use the **Enter Activation Code** task to enter any Capacity on Demand advanced functions activation codes that you have obtained for your system. Specify the appropriate code in the Code field to activate any of the following on-demand functions:

- **Advanced POWER Virtualization:** Permanently activates the Advanced POWER Virtualization capabilities, which can include Virtual I/O Server and Micro-Partitioning.
- **Enterprise Enablement:** Permanently activates the Enterprise Enablement capabilities, which can include 5250 Commercial Processing Workload (5250 CPW) capacity for application processing.

Use the **View History Log** task to see the activation history log for Capacity on Demand advanced functions on your system. The history log contains information about the activations of Capacity on Demand advanced functions that have occurred on your system. Capacity on Demand advanced functions include Advanced POWER Virtualization and Enterprise Enablement.

A log entry is created each time an activation code is entered successfully, and an additional log entry is created for each capability that is enabled by the activation code. For each entry in the Capacity on Demand advanced functions activation history log, this table shows the date and time on the system when the entry was logged and a description of the log entry. The entries are shown in chronological order, starting with the most recent entry.

If the history log has wrapped, a message is shown at the bottom of the window. The history log can contain as many as eight activation code entries. (For each activation code entry, an additional log entry is created for each capability that is enabled by the activation code.) When eight activation code entries have been logged to the history log, the next entry causes the history log to wrap (that is, the newest entry overlays the oldest entry).

Use the **View Code Information** task to view the information used to generate a CoD advanced functions activation code for the selected managed system. If you want to save this information to a file, select **Save**.

Related HMC CLI commands:

- “chcod” on page 148
- “lscod” on page 188

## Other Advanced Functions

Use the **Other Advanced Functions** tasks to enter an advanced function activation code, view advanced function code information, or view a history log of advanced function activation activity.

Use **Enter Activation Code** to enter any Capacity on Demand advanced functions activation codes that you have obtained for your system. Specify the appropriate code in the Code field to activate any of the following on-demand functions:

- **Advanced POWER Virtualization:** Permanently activates the Advanced POWER Virtualization capabilities, which can include Virtual I/O Server and Micro-Partitioning.
- **Enterprise Enablement:** Permanently activates the Enterprise Enablement capabilities, which can include 5250 Commercial Processing Workload (5250 CPW) capacity for application processing.

Use the **View History Log** task to see the activation history log for Capacity on Demand advanced functions on your system. The history log contains information about the activations of Capacity on Demand advanced functions that have occurred on your system. Capacity on Demand advanced functions include Advanced POWER Virtualization and Enterprise Enablement.

A log entry is created each time an activation code is entered successfully, and an additional log entry is created for each capability that is enabled by the activation code. For each entry in the Capacity on Demand advanced functions activation history log, this table shows the date and time on the system when the entry was logged and a description of the log entry. The entries are shown in chronological order, starting with the most recent entry.

If the history log has wrapped, a message is shown at the bottom of the window. The history log can contain as many as eight activation code entries. (For each activation code entry, an additional log entry is created for each capability that is enabled by the activation code.) When eight activation code entries have been logged to the history log, the next entry causes the history log to wrap (that is, the newest entry overlays the oldest entry).

Use the **View Code Information** task to view the information used to generate a CoD advanced functions activation code for the selected managed system. If you want to save this information to a file, click Save.

Related HMC CLI commands:

- “chcod” on page 148
- “lscod” on page 188



---

## Chapter 4. Systems Management - Partitions

**Systems Management** displays tasks to manage servers, logical partitions, and frames. Use these tasks to set up, configure, view current status, troubleshoot, and apply solutions.



This chapter describes the tasks displayed when a partition is selected.

To launch these tasks, see “Launching tasks for managed objects” on page 24. The following sets of tasks are represented in the tasks pad, tasks menu, or context menu. The tasks listed in the tasks pad change as selections are made in the work area. The context is always listed at the top of the tasks pad in the format Task: Object. These tasks are listed when a partition is selected and the context is Tasks: *partition name*.

---

### Properties

The **Properties** task displays the selected partition’s properties. This information is useful in resource allocation and partition management. These properties include:

#### General

The **General** tab displays the partition’s name, id, environment, state, resource configuration, operating system, the current profile used when starting the partition, and the system on which the partition is located.

#### Hardware

The **Hardware** tab displays the current usage of processors, memory, and I/O on the partition.

#### Virtual Adapters

The **Virtual Adapters** tab displays the current configuration of virtual adapters. Virtual adapters allow for the sharing of resources between partitions. From this tab, you can view, create, and edit virtual adapters on the partition.

#### Settings

The **Settings** tab displays the boot mode and keylock position of the partition. Also displayed are the current service and support settings for the partition.

**Other** The **Other** tab displays the partition’s Workload Management Group (if applicable), and the partition’s Power controlling partitions.

---

### Change Default Profile

Use the **Change Default Profile** task to change the default profile for the partition.

Select a profile from the drop down list to be the new default profile.

Related HMC CLI commands:

- “chsyscfg” on page 164

---

### Operations

**Operations** contains the tasks for operating partitions. The following are represented in the **Operations** tasks.

- “Activate” on page 70
- “Restart” on page 70

- “Shut Down”
- “Manage Attention LED” on page 71
- “Schedule Operations” on page 71
- “Delete” on page 72

## Activate

Use the **Activate** task to activate a partition on your managed system in the **Not Activated** state.

A list of profiles is display that are valid to start the selected partition. Select from the list of profiles and click OK to activate the partition. Check **Open a terminal window or console** to do so.

## Restart

Use this task to restart the selected logical partition or partitions.

For i5/OS logical partitions, use this window only if you cannot restart the i5/OS logical partition from the command line of the operating system. Using this window to restart an i5/OS logical partition will result in an abnormal IPL.

Choose one of the following options (the Operating System option and the Operating System Immediate option are only enabled if Resource Monitoring and Control (RMC) is up and configured):

**Dump** The HMC shuts down the logical partition and initiates a main storage or system memory dump. For AIX and Linux logical partitions, the HMC also notifies the logical partition that it will be shut down. For i5/OS logical partitions, the processors are stopped immediately. After the shutdown is complete, the logical partition is immediately restarted. (i5/OS logical partitions are restarted multiple times so that the logical partition can store the dump information.) Use this option if a portion of the operation system appears hung and you want a dump of the logical partition for analysis.

### Operating System

The HMC shuts down the logical partition normally by issuing a shutdown -r command to the logical partition. During this operation, the logical partition performs any necessary shutdown activities. After the shutdown is complete, the logical partition is immediately restarted. This option is only available for AIX logical partitions. Immediate: The HMC shuts down the logical partition immediately. The HMC ends all active jobs immediately. The programs running in those jobs are not allowed to perform any job cleanup. This option might cause undesirable results if data has been partially updated. Use this option only after a controlled end has been unsuccessfully attempted.

### Operating System Immediate

The HMC shuts down the logical partition immediately by issuing a shutdown -Fr command to the logical partition. During this operation, the logical partition bypasses messages to other users and other shutdown activities. After the shutdown is complete, the logical partition is immediately restarted. This option is only available for AIX logical partitions.

### Dump Retry

The HMC retries a main storage or system memory dump on the logical partition. After this is complete, the logical partition is shut down and restarted. Use this option only if you have previously tried the Dump option without success. This option is only available for i5/OS logical partitions.

Related HMC CLI commands:

- “chsysstate” on page 171

## Shut Down

Use this task to shut down the selected logical partition or partitions.

For i5/OS logical partitions, use this window only if you cannot shut down the i5/OS logical partition from the command line of the operating system. Using this window to shut down an i5/OS logical partition will result in an abnormal IPL.

Choose from the following options:

#### **Delayed**

The HMC shuts down the logical partition using the delayed power-off sequence. This allows the logical partition time to end jobs and write data to disks. If the logical partition is unable to shut down within the predetermined amount of time, it will end abnormally and the next restart may be longer than normal.

#### **Immediate**

The HMC shuts down the logical partition immediately. The HMC ends all active jobs immediately. The programs running in those jobs are not allowed to perform any job cleanup. This option might cause undesirable results if data has been partially updated. Use this option only after a controlled shutdown has been unsuccessfully attempted.

#### **Operating System**

The HMC shuts down the logical partition normally by issuing a shutdown command to the logical partition. During this operation, the logical partition performs any necessary shutdown activities. This option is only available for AIX logical partitions.

#### **Operating System Immediate**

The HMC shuts down the logical partition immediately by issuing a shutdown -F command to the logical partition. During this operation, the logical partition bypasses messages to other users and other shutdown activities. This option is only available for AIX logical partitions.

Related HMC CLI commands:

- “chsysstate” on page 171

## **Manage Attention LED**

Use the **Manage Attention LED** to activate or deactivate an attention LED on your partition.

All attention LEDs for the partitions on the managed system are listed. Select an LED and choose to activate or deactivate.

## **Schedule Operations**

Use this task to create a schedule for certain operations to be performed on the logical partition without operator assistance.

Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation. A schedule can be set for one operation or repeated many times.

For example, you could schedule an operation to remove resources from a logical partition or move resources from one logical partition to another.

The **Scheduled Operations** task displays the following information for each operation:

- The processor that is the object of the operation.
- The scheduled date
- The scheduled time
- The operation
- The number of remaining repetitions

From the **Scheduled Operations** window you can:

- Schedule an operation to run at a later time
- Define operations to repeat at regular intervals
- Delete a previously scheduled operation
- View details for a currently scheduled operation
- View scheduled operations within a specified time range
- Sort scheduled operations by date, operation, or managed system

An operation can be scheduled to occur one time or it can be scheduled to be repeated. You will be required to provide the time and date that you want the operation to occur. If the operation is scheduled to be repeated, you will be asked to select:

- The day or days of the week that you want the operation to occur. (optional)
- The interval, or time between each occurrence. (required)
- The total number of repetitions. (required)

The operations that can be scheduled for a logical partition are:

#### **Activate on an LPAR**

Schedules an operation on a selected profile for activation of the selected logical partition.

#### **Dynamic Reconfiguration**

Schedules an operation for adding, removing, or moving a resource (processors or megabytes of memory).

#### **Operating System Shutdown (on a partition)**

Schedules a shutdown of the selected logical partition.

To schedule operations on the HMC:

1. Open **Systems Management** from the navigation pane.
2. Select one or more partitions to work with from the work pane.
3. In the tasks pad, select the **Operations** task category, then open **Schedule Operations**. The **Schedule Operations** window is displayed.
4. From the **Schedule Operations** window, click **Options** from the menu bar to display the next level of options:
  - To add a scheduled operation, point to **Options** and then click **New...**
  - To delete a scheduled operation, select the operation you want to delete, point to **Options** and then click **Delete**.
  - To update the list of scheduled operations with the current schedules for the selected objects, point to **Options** and then click **Refresh**.
  - To view a scheduled operation, select the operation you want to view, point to **View** and then click **Schedule Details...**
  - To change the time of a scheduled operation, select the operation you want to view, point to **View** and then click **New Time Range...**
  - To sort the scheduled operations, point to **Sort** and then click one of the sort categories that appears.
5. To return to the HMC workplace, point to **Options** and then click **Exit**.

Use the online Help to get additional information for scheduling an operation.

## **Delete**

Use the **Delete** task to delete the selected partition.

The Delete task deletes the selected partition and all of the partition profiles associated with the partition from the managed system. When you delete a partition, all hardware resources currently assigned to that partition become available to other partitions.



---

## Configuration

**Configuration** contains the tasks for configuring your partitions. The following are represented in the **Configuration** tasks:

- “Manage Profiles”
- “Manage Custom Groups”
- “Save Current Configuration”

### Manage Profiles

Use the **Manage Profiles** task to create, edit, copy, delete, or activate a profile for the selected partition.

A partition profile contains the resource configuration for the partition. You can modify the processor, memory, and adapter assignments for a profile by editing the profile.

The default partition profile for a logical partition is the partition profile that is used to activate the logical partition if no other partition profile is selected. You cannot delete the default partition profile unless you first designate another partition profile as the default partition profile. The default profile is defined in the status column.

Choose **Copy** to create an exact copy of the selected partition profile. This allows you to create multiple partition profiles that are nearly identical to one another by copying a partition profile and changing the copies as needed.

### Manage Custom Groups

Groups are comprised of logical collections of objects. You can report status on a group basis, allowing you to monitor your system in a way that you prefer.

You can also nest groups (a group contained within a group) to provide hierarchical or topology views.

One or more user-defined groups might already be defined on your HMC. Default groups are listed under the **Custom Groups** node under **Server Management**. The default groups are **All Partitions** and **All Objects**. You can create others, delete the ones that were created, add to created groups, create groups using the pattern match method, or delete from created groups by using the **Manage Custom Groups** task.

Use the online Help if you need additional information for working with groups.

### Save Current Configuration

Use this task to save the current configuration of a logical partition to a new partition profile by entering a new profile name.

This procedure is useful if you change the configuration of a logical partition using dynamic logical partitioning and you do not want to lose the changes when you restart the logical partition. You can perform this procedure at any time after you initially activate a logical partition.

Related HMC CLI commands:

- “mksyscfg” on page 217

---

## Hardware (Information)

**Hardware (Information)** tasks are used to display information about the hardware attached to a selected managed system.

The following are represented in the **Hardware (Information)** tasks:

- “View RIO Topology” on page 56

## Adapters

Use the **Adapters** tasks to view information about the Host Ethernet Adapters (HEA) or Host Channel Adapters (HCA) for a selected managed system.

### Host Ethernet Adapter (HEA)

A Host Ethernet Adapter (HEA) allows multiple logical partitions to share a single physical Ethernet adapter.

Unlike most other types of I/O devices, you can never assign the HEA itself to a logical partition. Instead, multiple logical partitions can connect directly to the HEA and use the HEA resources. This allows these logical partitions to access external networks through the HEA without having to go through an Ethernet bridge on another logical partition.

Use the **Host Ethernet** task to display or configure the ports of the physical Host Ethernet Adapters (HEAs) on a selected managed system.

To configure a physical port on an HEA, select the port from the list and select Configure.

Use the online Help for additional information on configuring HEA ports.

Related HMC CLI commands:

- “chhwres” on page 152
- “lshwres” on page 194

### Host Channel Adapter (HCA)

Host Channel Adapters provide a managed system with port connections to other InfiniBand devices. That port can be connected to another HCA, a target device, or an InfiniBand switch that redirects the data coming in on one of its ports out to a device attached to another of its ports.

Use the **Host Channel** task to show a list of the HCAs for the managed system. You can select an HCA from the list to display the current partition usage for the HCA.

From this task you can display:

- The physical location of each HCA on the managed system.
- The number of Globally Unique Identifiers (GUIDs) that are in use on each HCA.
- The number of GUIDs on each HCA that are available to be assigned to logical partitions.
- HMC management status. HCAs that are unable to be managed by an HMC are in an error state.
- The logical partition usage for a selected HCA.

Related HMC CLI commands:

- “lshwres” on page 194

### Switch Network Interface

Use the **Switch Network Interface** task to display a list of the Switch Network Interface (SNI) adapters for the selected managed system.

Displayed is the SNI adapter handle, the name of the partition to the adapter is assigned, the physical location of the adapter, and the host name or IP address of the adapter.

---

## Dynamic Logical Partitioning

**Dynamic Logical Partitioning (DLPAR)** tasks dynamically add or remove processors, memory, and adapters to and from logical partitions.

The following are represented in the **Dynamic Logical Partitioning** tasks:

- “Processor”
- “Memory”
- “Virtual Adapter” on page 76
- “Host Ethernet” on page 76

### Processor

Use DLPAR **Processor** tasks to add or remove processor resources from a logical partition or to move processor resources from one logical partition to another.

Use the **Add or Remove** task to add processor resources to or remove processor resources from the selected logical partition without restarting the logical partition.

Use the **Move** task to move processor resources from the selected logical partition to another logical partition without restarting either logical partition.

Use the online Help for more information on adding, removing, or moving processor resources.

Related HMC CLI commands:

- “chhwres” on page 152
- “lshwres” on page 194

### Memory

Use DLPAR **Memory** tasks to add or remove memory resources from a logical partition or to move memory resources from one logical partition to another.

Use the **Add or Remove** task to add memory to or remove memory from the selected logical partition without restarting the logical partition.

Use the **Move** task to move memory from the selected logical partition to another logical partition without restarting either logical partition.

Use the online Help for more information on adding, removing, or moving processor resources.

Related HMC CLI commands:

- “chhwres” on page 152
- “lshwres” on page 194

### Physical Adapters

Use the DLPAR Physical Adapters tasks to add I/O slots to a logical partition without restarting the partition or to move or remove I/O slots from a logical partition without restarting the partition.

Use the **Add** task to add I/O slots to a logical partition without restarting the partition. When you add an I/O slot to a logical partition, the I/O adapter in that I/O slot and the devices that are controlled by

the I/O adapter can be used by the logical partition. This function is typically used to share infrequently used devices among logical partitions by moving these devices from one logical partition to another.

Use the **Move or Remove** task to remove I/O slots from a logical partition or move I/O slots between logical partitions without restarting the logical partitions. When you remove an I/O slot from a logical partition, the I/O adapter in that I/O slot and the devices that are controlled by the I/O adapter are also removed from the logical partition. If you choose to move the I/O slot to another logical partition, the I/O adapter and the devices that are controlled by the I/O adapter are also moved to the other logical partition. This function is typically used to share infrequently used devices among logical partitions by moving these devices from one logical partition to another.

It is recommended that you vary off the I/O slot and all I/O adapters and devices connected to the I/O slot before you remove the I/O slot from the logical partition.

Related HMC CLI commands:

- “chhwres” on page 152
- “lshwres” on page 194

## Virtual Adapter

This task displays a list of all of the virtual adapters that currently exist for this logical partition or partition profile.

Use this task to create, change, or remove a virtual adapter on a logical partition or in a partition profile.

From this task you can:

- Display the properties of a virtual adapter.
- Edit the properties of a virtual adapter.
- Create a new virtual adapter.
- Delete a virtual adapter.

Use the online Help for more information on managing virtual adapters.

Related HMC CLI commands:

- “chhwres” on page 152
- “lshwres” on page 194

## Host Ethernet

Use **Host Ethernet** tasks to add Logical Host Ethernet Adapter (LHEA) logical ports dynamically to a running logical partition.

Use the **Add** task to add LHEA logical ports dynamically to a running logical partition. These logical ports allow the logical partition to access and use the physical port resources on a physical Host Ethernet Adapter (HEA).

Some operating system or system software versions do not allow you to add logical ports dynamically. Consult the documentation for the operating system or system software for more information.

To add logical ports dynamically to the logical partition, select the HEA whose resources you want to use, select the physical port for which you want to create a logical port, and click **Configure**. You can then configure the logical port and return to this window. If you change your mind about adding a logical port to the logical partition, select the physical port that corresponds to the logical port and click **Reset**. You can then configure a different logical port for that physical port.

When you are done adding logical ports to the running logical partition, click **OK**.

Use the **Move or Remove** task to move LHEA logical ports dynamically from the selected logical partition.

These logical ports allow the logical partition to access and use the physical port resources on a physical HEA. You can move the logical ports dynamically to another running logical partition, or you can leave the logical ports as unassigned.

Some operating system or system software versions do not allow you to move or remove logical ports dynamically. Consult the documentation for the operating system or system software for more information.

To remove logical ports dynamically from the logical partition, select the HEA whose logical ports you want to remove, select the physical port whose logical ports you want to remove and click **OK**.

To move logical ports dynamically from the logical partition to another running logical partition, select the HEA whose logical ports you want to remove, select the physical port whose logical ports you want to move, select the destination logical partition in Logical Partition, and click **OK**.

Related HMC CLI commands:

- “chhwres” on page 152
- “lshwres” on page 194

---

## Console Window

Use the **Open Terminal Window** task to open a terminal window to the operating system running on the selected partition.

Use the **Close Terminal Connection** task to close the connection.

Use the **Open Shared 5250 Console** task to open a shared console with an i5/OS partition.

Use the **Open Dedicated 5250 Console** task to open a dedicated console with an i5/OS partition.

---

## Serviceability

Problem Analysis on the HMC automatically detects error conditions and reports to you any problem that requires service to repair it. These problems are reported to you as serviceable events. Use the **Manage Events** task to view specific events for selected systems. However, if you notice a problem occurred or you suspect a problem is affecting the system but Problem Analysis has not reported it to you, use the **Create Serviceable Event** task to report the problem to your service provider.

The following are represented in the **Serviceability** tasks:

- “Manage Serviceable Events” on page 112
- “Create Serviceable Event” on page 107
- “Reference Code History” on page 58
- “Control Panel Functions” on page 58
- “Hardware” on page 58
- “Manage Dumps” on page 60
- “Collect VPD” on page 60
- “Edit MTMS” on page 61
- “FSP Failover” on page 61

## Manage Serviceable Events

Problems on your managed system are reported to the HMC as serviceable events. The **Manage Serviceable Events** task allows you view the problem, manage problem data, call home the event to your service provider, or repair the problem.

To set the criteria for the serviceable events you to view:

1. Open the **Manage Serviceable Events** task from the tasks pad.
2. From the **Manage Serviceable Events** window provide event criteria, error criteria, and FRU criteria.
3. Click **OK** when you have specified the criteria you want for the serviceable events you want to view.
4. Select **ALL** if you do not want the results filtered.

The **Serviceable Events Overview** panel displays all of the events that match your criteria. The information displayed in the compact table view includes:

- Problem Number
- PMH Number
- Reference Code - Click on the Reference code to display a description of the problem reported and actions that may be taken to fix the problem.
- Status of the problem
- Last reported time of the problem
- Failing MTMS of the problem

The full table view includes more detailed information, including reporting MTMS, first reported time, and serviceable event text.

Select a serviceable event and use the **Selected** drop down menu to:

- **View event details:** FRUs associated with this event and their descriptions.
- **Repair the event:** Launch a guided repair procedure, if available.
- **Call home the event:** Report the event to your service provider.
- **Manage event problem data:** View, call home, or offload to media data and logs associated with this event.
- **Close the event:** After the problem is solved, add comments and close the event.

Use the online Help if you need additional information on managing serviceable events.

## Reference Code History

Use the **Reference Code History** task to view reference codes that have been generated for the selected logical partition. Reference codes are diagnostic aids that help you determine the source of a hardware or operating system problem.

By default, only the most recent reference codes that the logical partition has generated are displayed. To view more reference codes, enter the number of reference codes that you want to view into **View history** and click **Go**. The window displays that number of the latest reference codes, with the date and time at which each reference code was generated. The window can display up to the maximum number of reference codes stored for the logical partition.

## Control Panel Functions

This task displays the available virtual control panel functions for the partition selected. The tasks are:

### (21) Activate Dedicated Service Tools

Starts Dedicated Service Tools (DST) on the partition.

### (65) Disable Remote Service

Deactivates remote service on the partition.

**(66) Enable Remote Service**

Activates remote service on the partition.

**(67) Disk Unit IOP Reset/Reload**

Disk unit IOP reset/reload is enabled only by specific disk unit error conditions.

**(68) Concurrent Maintenance Power Off Domain**

Concurrent maintenance power domain Power Off.

**(69) Concurrent Maintenance Power On Domain**

Concurrent maintenance power domain Power On.

**(70) IOP Control Storage Dump**

This IOP dump function is enabled by specific error conditions.





---

## Chapter 5. Systems Management - Frames

**Systems Management** displays tasks to manage servers, logical partitions, and frames. Use these tasks to set up, configure, view current status, troubleshoot, and apply solutions.



This chapter describes the tasks used when a frame is selected.

To launch these tasks, see “Launching tasks for managed objects” on page 24. The following sets of tasks are represented in the tasks pad, tasks menu, or context menu. The tasks listed in the tasks pad change as selections are made in the work area. The context is always listed at the top of the tasks pad in the format Task: Object. These tasks are listed when a managed system is selected and the context is Tasks: *Frame Name*.

---

### Properties

The **Properties** task displays the selected frame properties. These properties include:

#### General

The **General** tab displays the frame name and number, state, type, model, and serial number.

#### Managed Systems

The **Managed Systems** tab displays all of the managed systems contained in the frame and their cage numbers. A cage is a division of the enclosure that holds the managed systems, the I/O units, and the bulk power assemblies (BPAs).

#### I/O Units

The **I/O Units** tab displays all of the I/O units contained in the frame, their cage numbers, and their assigned managed systems. A cage is a division of the enclosure that holds the managed systems, the I/O units, and the bulk power assemblies (BPAs). “Not owned” in the System column indicates that the corresponding I/O unit has not been assigned to a managed system.

---

### Update Password

Use the **Update Password** task to update HMC access and Advanced System Management Interface (ASMI) passwords on the managed system.

The first time you access a managed system using an HMC, the system prompts you to enter passwords for each of the following:

- Hardware Management Console: HMC access
- Advanced System Management Interface: General
- Advanced System Management Interface: Admin

If you are using an HMC to access the managed system before all required passwords have been set, enter the appropriate password for each password that is presented in the Update Password task.

If another HMC subsequently needs access to this managed system, upon attempting to access this HMC the user is presented with the *Update Password Failed Authentication* window, which will prompt for the HMC access password you entered.

In the event that the HMC access password changes while you are logged in to the managed system, your HMC will discover that it can no longer authenticate after it attempts to reconnect to that managed

system. This will result in a state of *Failed Authentication* for that managed system. You will be required to enter the new password before any actions can be performed.

---

## Operations

**Operations** contains the tasks for operating frames. The following are represented in the **Operations** tasks.

- “Initialize”
- “Rebuild”
- “Change Password”
- “Power On/Off IO Unit”

### Initialize

Use the **Initialize** task to initialize a frame.

When you initialize a managed frame, all of the frames managed by the HMC are powered on. As each individual frame is powered on, the I/O units that are contained within the frame are powered on as well. When all the I/O units for the frame have been powered on, then the managed systems that are contained within the frame are powered on. The complete initialization process may take several minutes to complete.

**Note:** Managed systems that are already powered on will not be affected (meaning they will not be powered off and back on again).

### Rebuild

Use the **Rebuild** task to rebuild frame information on the HMC.

Updating, or rebuilding, the frame acts much like a refresh of the frame information. Rebuilding the frame is useful when the system’s state indicator in the Work pane of the HMC is shown as *Incomplete*. The *Incomplete* indicator signifies that the HMC cannot gather complete resource information from the managed system within the frame.

No other tasks can be performed on the HMC during this process, which may take several minutes.

### Change Password

Use the **Change Password** task to change the HMC access password on the selected managed frame. After the password is changed, you must update the HMC access password for all other HMCs from which you want to access this managed frame.

Enter the current password. Then enter a new password and verify it by entering it again.

Related HMC CLI commands:

- “chsyspwd” on page 170

### Power On/Off IO Unit

Use the **Power On/Off IO Unit** task to power off an IO unit.

Only units or slots that reside in a power domain can be powered off. The corresponding power on/off buttons will be disabled for location codes that are not controllable by the HMC.

---

## Configuration

**Configuration** contains the tasks for configuring your frame. The following are represented in the **Configuration** tasks:

- Manage Custom Groups

### Manage Custom Groups

Groups are comprised of logical collections of objects. You can report status on a group basis, allowing you to monitor your system in a way that you prefer.

You can also nest groups (a group contained within a group) to provide hierarchical or topology views.

One or more user-defined groups might already be defined on your HMC. Default groups are listed under the **Custom Groups** node under **Server Management**. The default groups are **All Partitions** and **All Objects**. You can create others, delete the ones that were created, add to created groups, create groups using the pattern match method, or delete from created groups by using the **Manage Custom Groups** task.

Use the online Help if you need additional information for working with groups.

---

## Connections

**Connections** tasks allow you to view the HMC connection status to frames or reset those connections.

### Bulk Power Assembly (BPA) Status

Use the **Bulk Power Assembly Status** task to view the state of the connection from the Hardware Management Console (HMC) to side A and side B of the bulk power assembly. The HMC will operate normally with a connection to either side A or side B. However, for code update operations and some concurrent maintenance operations, the HMC needs connections to both sides.

Displayed are:

- IP address
- BPA Role
- Connection Status
- Connection Error code

If the status is not Connected, the Connection status may be:

#### Starting/Unknown

One of the bulk power assemblies (BPAs) contained in the frame is in the process of starting. The state of the other BPA cannot be determined.

#### Standby/Standby

Both of the bulk power assemblies (BPAs) contained in the frame are in the standby state. A BPA in the standby state is operating normally.

#### Standby/Starting

One of the bulk power assemblies (BPAs) contained in the frame is operating normally (in standby state). The other BPA is in the process of starting.

#### Standby/Not Available

One of the bulk power assemblies (BPAs) contained in the frame is operating normally (in the standby state), but the other BPA is not operating normally.

#### Pending frame number

A change to the frame number is in progress. No operations can be performed when the frame is in this state.

**Failed Authentication**

The HMC access password for the frame is not valid. Enter a valid password for the frame.

**Pending Authentication - Password Updates Required**

The frame access passwords have not been set. You must set the required passwords for the frame, to enable secure authentication and access control from the HMC.

**No Connection**

The HMC cannot connect to the frame.

**Incomplete**

The HMC failed to get all of the necessary information from the managed frame. The frame is not responding to requests for information.

**Reset**

Use the **Reset** task to reset the connection between the HMC and the selected managed frame.

When you reset the connection with a managed frame, the connection is broken and then reconnected. Reset the connection with the managed frame if the managed frame is in a No Connection state and you have verified that the network settings are correct on both the HMC and the managed frame.

---

**Hardware (Information)**

**Hardware (Information)** tasks are used to display information about the hardware attached to a selected managed frame.

The following are represented in the **Hardware (Information)** tasks:

- “View RIO Topology”

**View RIO Topology**

This task displays the current RIO topology for the selected managed frame and any discrepancies between the current topology and the last valid topology.

High Speed Link (HSL), also known as Remote I/O (RIO), resources provide the connection between system I/O busses and the system processor. HSL/RIO resources are normally configured in loops with the system unit having an HSL/RIO controller resource that handles routing of the data between the system processor and the system I/O busses. System I/O busses connect to the loop with HSL I/O adapter or RIO adapter resources.

Use this task to display the current RIO topology of the selected managed system. Current Topology displays the current topology. Any discrepancies between the current topology and the last valid topology are identified as errors. The following information is shown:

- The starting location of the physical RIO cable and the RIO connection (cable to port)
- The ending location of the physical RIO cable and the RIO connection (cable to port)
- Starting Node Type Displays the values of the node. Possible values are Local Bridge, Local NIC, Remote Bridge, and Remote NIC
- Link Status Displays the leading port status
- Cable Length Displays the length of the RIO cables. Errors occur when the actual cable lengths are different from the expected cable lengths
- The serial number of the power-controlling managed system
- The serial number of the function-controlling managed system

---

## Serviceability

Problem Analysis on the HMC automatically detects error conditions and reports to you any problem that requires service to repair it. These problems are reported to you as serviceable events. Use the **Manage Serviceable Events** task to view specific events for selected systems. Use the **Hardware** tasks to add, remove, or exchange a Field Replaceable Unit (FRU).

The following are represented in the **Serviceability** tasks:

- “Manage Serviceable Events”
- “Hardware”

## Manage Serviceable Events

Problems on your managed frame are reported to the HMC as serviceable events. The **Manage Serviceable Events** task allows you view the problem, manage problem data, call home the event to your service provider, or repair the problem.

To set the criteria for the serviceable events you to view:

1. Open the **Manage Serviceable Events** task from the tasks pad.
2. From the **Manage Serviceable Events** window provide event criteria, error criteria, and FRU criteria.
3. Click **OK** when you have specified the criteria you want for the serviceable events you want to view.
4. Select **ALL** if you do not want the results filtered.

The **Serviceable Events Overview** panel displays all of the events that match your criteria. The information displayed in the compact table view includes:

- Problem Number
- PMH Number
- Reference Code - Click on the Reference code to display a description of the problem reported and actions that may be taken to fix the problem.
- Status of the problem
- Last reported time of the problem
- Failing MTMS of the problem

The full table view includes more detailed information, including reporting MTMS, first reported time, and serviceable event text.

Select a serviceable event and use the **Selected** drop down menu to:

- **View event details:** FRUs associated with this event and their descriptions.
- **Repair the event:** Launch a guided repair procedure, if available.
- **Call home the event:** Report the event to your service provider.
- **Manage event problem data:** View, call home, or offload to media data and logs associated with this event.
- **Close the event:** After the problem is solved, add comments and close the event.

Use the online Help if you need additional information on managing serviceable events.

## Hardware

These tasks are used to add, exchange, or remove hardware from the managed frame. From the hardware tasks you can display a list of installed FRUs or enclosures and their locations. Select a FRU or an enclosure and launch a step-by-step procedure to add, exchange, or remove the unit.

**Hardware** tasks include:

- “Add FRU” on page 86
- “Add Enclosure” on page 86
- “Exchange FRU” on page 86

- “Exchange Enclosure” on page 59
- “Remove FRU” on page 87
- “Remove Enclosure” on page 87

## Add FRU

Use the **Add FRU** task to locate and add a Field Replaceable Unit (FRU).

To add a FRU:

1. Select an enclosure type from the drop down list.
2. Select an FRU type from the list.
3. Click **Next**.
4. Select a location code from the displayed list.
5. Click **Add** to add the selected enclosure location to **Pending Actions**.
6. Click **Launch Procedure** to begin adding the selected FRU type to the enclosure locations identified in Pending Actions.
7. Click **Finish** when you have completed the FRU installation process.

## Add Enclosure

Use the **Add Enclosure** task to locate and add an enclosure.

To add an enclosure:

1. Select an enclosure type, then click **Add** to add the selected enclosure type’s location code to **Pending Actions**.
2. Click **Launch Procedure** to begin adding the enclosures identified in **Pending Actions** to the selected system.
3. Click **Finish** when you have completed the enclosure installation process.

## Exchange FRU

Use the **Exchange FRU** task to exchange one FRU with another.

To exchange a FRU:

1. Select an installed enclosure type from the drop down list.
2. From the displayed list of FRU types for this enclosure, select an FRU type.
3. Click **Next** to display a list of locations for the FRU type.
4. Select a location code for a specific FRU.
5. Click **Add** to add the FRU location to **Pending Actions**.
6. Select **Launch Procedure** to begin replacing the FRUs listed in **Pending Actions**.
7. Click **Finish** when you have completed the installation.

## Exchange Enclosure

Use the **Exchange Enclosure** task to exchange one enclosure for another.

To exchange an enclosure:

1. Select an installed enclosure, then click **Add** to add the selected enclosure’s location code to **Pending Actions**.
2. Click **Launch Procedure** to begin replacing the enclosures identified in **Pending Actions** in the selected system.
3. Click **Finish** when you have completed the enclosure replacement process

## Remove FRU

Use the **Remove FRU** task to remove a FRU from your managed system.

To remove a FRU:

1. Select an enclosure from the drop down list to display a list FRU types currently installed in the selected enclosure.
2. From the displayed list of FRU types for this enclosure, select an FRU type.
3. Click **Next** to display a list of locations for the FRU type.
4. Select a location code for a specific FRU.
5. Click **Add** to add the FRU location to **Pending Actions**.
6. Select **Launch Procedure** to begin removing the FRUs listed in **Pending Actions**.
7. Click **Finish** when you have completed the removal procedure.

## Remove Enclosure

Use the **Remove Enclosure** task to remove an enclosure.

To remove an enclosure:

1. Select an enclosure type, then click **Add** to add the selected enclosure type's location code to **Pending Actions**.
2. Click **Launch Procedure** to begin removing the enclosures identified in **Pending Actions** from the selected system.
3. Click **Finish** when you have completed the enclosure removal process.





---

## Chapter 6. System Plans

**System Plans** displays the tasks used to record or import specifications for logical partitions, partition profiles, or hardware specifications on a chosen system.

To display the tasks available for a system plan, select a system plan from the System Plan work pane table. The following tasks are available:

- “View System Plan”
- “Create System Plan” on page 90
- “Deploy System Plan” on page 90
- “Export System Plan” on page 91
- “Import System Plan” on page 91
- “Remove System Plan” on page 91

Related HMC CLI commands:

- “cpsysplan” on page 177
- “defsplanres” on page 178
- “deploysysplan” on page 179
- “lssysplan” on page 213
- “lssysplanres” on page 214
- “mksysplan” on page 224
- “rmsysplan” on page 232
- “rmsysplanres” on page 232

---

### View System Plan

This task is used to review the detailed information in the selected system plan.

The System Plan Viewer consists of four main areas:

**Title pane**

Displays basic information about the System Plan Viewer and the application from which you accessed the viewer.

**Navigation pane**

Provides a navigation tree of the system plan that you are viewing.

**Contents pane**

Provides the detailed view of the information in the system plan that you are viewing.

**Actions pane**

Contains action buttons that allow you to work with the system plan.

Use the navigation tree to determine which aspects of the system plan to view. Some levels of the tree can be expanded or collapsed to reveal more entries. Entries in the tree with a + (plus) symbol contain further entries and are expandable by clicking on the + symbol. When an entry is expanded, the + symbol changes to a - (minus) symbol. Clicking the - symbol collapses the entry and hides any further entries that it contains. Clicking on an entry in the tree displays the contents for that entry in the contents pane.

The first level of the navigation tree is the system plan name. You must select the + symbol next to the name to expand the file and view the main entries within the tree for the system plan.

Use the online Help for more information on viewing a system plan.

Related HMC CLI commands:

- “lssysplan” on page 213

- “lssysplanres” on page 214

---

## Create System Plan

This task is used to create a new system plan for a system that this HMC manages. The new system plan contains specifications for the logical partitions and partition profiles of the managed system that you used to create the plan.

The new system plan also can contain hardware information that the HMC is able to obtain from the selected managed system. However, the HMC might not be able to detect all system hardware and partition settings. For example, the HMC is not able to detect the types of disk drives installed on the managed system unless the HMC uses Resource Monitoring and Control (RMC) to monitor resources on the managed system.

To maximize the information that the HMC can obtain from the managed system, power on the managed system and activate the logical partitions on the managed system before creating the new system plan.

When you use the HMC to create a system plan for a managed system, you can capture partition configuration information and a limited amount of associated hardware configuration information. Additionally, you can set up Resource Monitoring and Control (RMC) prior to creating a system plan to capture more detailed information. Although it may cause the creation of the system plan to take several more minutes to finish processing, by using RMC you can capture disk drive and tape drive configuration information for a managed system in the system plan.

Use the online Help for more information on creating a system plan.

Related HMC CLI commands:

- “defsysplanres” on page 178
- “mksysplan” on page 224

---

## Deploy System Plan

This task is used to select the system plan that you want to deploy and the name of the managed system on which you want to deploy the plan.

This task uses the Deploy System Plan wizard to perform the following actions, depending on the contents of the system plan:

- If the system plan contains logical partition information, you can use the wizard to create the specified logical partitions on the managed system. You can choose to create all the logical partitions specified within the system plan, or you can choose which logical partitions in the system plan that you want to create.
- If the system plan contains operating environment installation information, you can use the wizard to install the operating environment for a specified partition. You can use the wizard to specify the resource location that the wizard needs for installing the operating system environment, as well as to specify or change operating environment installation settings. Currently, the wizard provides support for installing a Virtual I/O Server (VIOS) operating environment only.
- If the system plan contains VIOS provisioning information for a partition, you can use the wizard to provision the partition. The wizard can configure one or more client partitions and provision certain resources for the partitions when the system plan contains this type of provisioning information.

Use the online Help for more information on deploying a system plan.

Related HMC CLI commands:

- “deploysysplan” on page 179

---

## Export System Plan

This task is used to export a system plan to other systems or other HMCs.

You have three options for exporting the selected system-plan file:

- You can export the system file to the local system on which you are running the browser to access the HMC.
- You can export the system-plan file to removable media that is currently mounted to the HMC, such as optical discs or USB Mass Storage devices.
- You can export the system-plan file to a remote file transfer protocol (FTP) site. Exporting a system-plan file by means of FTP allows you to import the system-plan file into a different HMC. You can then deploy a system plan in the file to a system that the other HMC manages.

Use the online Help for more information on exporting a system plan.

---

## Import System Plan

This task is used to import a system plan to other systems or other HMCs.

You can save this system plan and import the plan on other systems that this HMC manages that have hardware that is identical to the hardware in the system plan. You can import the system plan on another HMC and use it to deploy the system plan to other systems the target HMC manages that have hardware that is identical to the hardware in the system plan.

You can also import a system plan created using the System Planning Tool (SPT) at <http://www.ibm.com/systems/support/tools/systemplanningtool/>. The SPT is available to assist you in system planning, design, validation and to provide a system validation report that reflects your system requirements while not exceeding system recommendations. The SPT is a PC-based browser application designed to be run in a standalone environment. The SPT emulates an LPAR configuration and validates that the planned partitions are valid. It allows you to test the placement of hardware within the system to ensure that the placement is valid. When you have prepared your partitioning plan using the SPT, you can save this plan in a system plan file. You can import this file into your HMC and deploy the system plan to a managed system that is managed by the HMC. When you deploy the system plan, the HMC creates the logical partitions from the system plan on the managed system.

You can import a system-plan file from one of three sources:

- You can import a system file from the local system on which you are running the browser to access the HMC.
- You can import a system-plan file from removable media that is currently mounted to the HMC, such as optical discs or USB Mass Storage devices.
- You can import a system-plan file from a remote file transfer protocol (FTP) site. Importing a system-plan file by means of FTP allows you to deploy a system plan from a source other than the current HMC.

Use the online Help for more information on importing a system plan.

---

## Remove System Plan

This task is used to permanently remove the specified system plan from the HMC.

**Note:** Removing the system plan from the HMC does not undo any partition or hardware configuration changes that occurred if the specified system plan was deployed on a managed system.

Use the online Help for more information on removing a system plan.

Related HMC CLI commands:

- “rmsysplan” on page 232
- “rmsysplanres” on page 232

---

## Chapter 7. HMC Management tasks

This chapter alphabetically describes the tasks that are available on the Hardware Management Console (HMC) for the **HMC Management** tasks.

To open these tasks, see “HMC Management” on page 31.

**Note:** Depending on the task roles assigned to your user ID you may not have access to all the tasks. See Table 10 on page 127 for a listing of the tasks and the user roles allowed to access them.

---

### Back up HMC Data

This task backs up (or archives) the data that is stored on your HMC hard disk that is critical to support HMC operations.

You should back up the HMC data after changes have been made to the HMC or information associated with logical partitions.

The HMC data stored on the HMC hard drive can be saved to a DVD-RAM on a local system, a remote system mounted to the HMC file system (such as NFS), or sent to a remote site using File Transfer Protocol (FTP).

Using the HMC, you can back up all important data, such as the following:

- User-preference files
- User information
- HMC platform-configuration files
- HMC log files
- HMC updates through Install Corrective Service.

**Note:** Use the archived data only in conjunction with a reinstallation of the HMC from the product CDs.

To back up the HMC critical data:

1. Open the **Back up HMC Data** task from the HMC Management work pane.
2. From the **Back up HMC Data** window, choose the archive option you want to perform.
3. Click **Next**, then follow the appropriate instructions depending on the option you chose.
4. Click **OK** to continue with the backup process.

Use the online Help if you need additional information for backing up the HMC data.

Related HMC CLI commands:

- “bkconsdata” on page 145

---

### Change Date and Time

This task enables you to change the time and date of the battery-operated HMC clock and to add or remove time servers for the Network Time Protocol (NTP) service.

Use this task:

- If the battery is replaced in the HMC.
- If your system is physically moved to a different time zone.

**Note:** The time setting will adjust automatically for daylight saving time in the time zone you select.

To change the date and time:

1. Open the **Change Date and Time** task from the HMC Management work pane.
2. Select the **Customize Console Date and Time** tab. The **Customize Console Date and Time** pane is displayed.
3. Enter the date and time information in the appropriate fields.
4. Click **OK** to apply the new information.

To change the time server information:

1. Open the **Change Date and Time** task from the HMC Management work pane.
2. Select the **NTP Configuration** tab. The **NTP Configuration** pane is displayed.
3. Provide the appropriate information for the time server.
4. Click **OK** to apply the new information.

Use the online Help if you need additional information for changing the date and time of the HMC or for adding or removing time servers for the Network Time Protocol (NTP) service.

Related HMC CLI commands:

- “chhmc” on page 149
- date
- “lshmc” on page 191

---

## Change Language and Locale

This task sets the language and location for the HMC. After you select a language, you can select a locale associated with that language.

The language and locale settings determine the language, the character set, and other settings specific to the country or region (such as formats for date, time, numbers, and monetary units). Changes made in the **Change Language and Locale** window affect only the language and locale for the HMC itself. If you access the HMC remotely, the language and locale settings on your browser determine the settings that the browser uses to display the HMC interface.

To change the language and locale on the HMC:

1. Open the **Change Language and Locale** task from the HMC Management Work pane.
2. From the **Change Language and Locale** window, choose the applicable language and locale.
3. Click **OK** to apply the change.

Use the online Help if you need additional information for changing the language and locale of the HMC.

Related HMC CLI commands:

- “chhmc” on page 149
- “lshmc” on page 191

---

## Change Network Settings

This task allows you to view the current network information for the HMC and to change network settings.

1. Open the **Change Network Settings** from the HMC Management work pane.
2. From the **Change Network Settings** window, you can work with the following tabs:

### Identification

Contains the host name and domain name of the HMC.

**Console name**

Your HMC user name, the name that identifies your console to other consoles on the network. This is the short host name, for example: hmcibm1.

**Domain name**

A name that Domain Name Services (DNS) can translate to the IP address. For example, DNS might translate the domain name www.example.com to 198.105.232.4. (The long host name consists of the console name plus a period plus the domain name, for example: hmcibm1.endicott.ibm.com.)

**Console description**

This is for your use only. An example might be: Main HMC for customer finance.

**LAN Adapters**

A summarized list of all (visible) Local Area Network (LAN) adapters. You can select any of these and click **Details...** to open a window allowing you to change addressing, routing, other LAN adapter characteristics, and firewall settings.

**Name Services**

Specify the Domain Name Services (DNS) and domain suffix values for configuring the console network settings.

**Routing**

Specify the routing information and default gateway information for configuring the console network settings.

The **Gateway address** is the route to all networks. The default gateway address (if defined) informs this HMC where to send data if the target station does not reside on the same subnet as the source. If your machine can reach all stations on the same subnet (usually a building or a sector within a building), but cannot communicate outside the area, it is usually because of an incorrectly configured default gateway.

You can assign a specific LAN to be the **Gateway device** or you can choose "any."

You can select **Enable 'routed'** to start the routed daemon, which allows it to run and allows any routing information to be exported from the HMC.

3. Click **OK** when you have completed this task.

**Note:** Depending on the type of change that you make, the network or console automatically restarts or the console automatically reboots.

Use the online Help to get additional information for customizing the network settings.

Related HMC CLI commands:

- "chhmc" on page 149
- "lshmc" on page 191

---

## Change User Interface Settings

This task enables you to customize settings that control how the HMC interface appears. You can display or hide certain user interface components and icons, display or hide specific navigation nodes, and determine whether or not to save user interface settings changes.

**Note:** User interface changes apply to the currently logged on user ID only.

To change user interface settings:

1. Open the **Change User Interface Settings** task from the HMC Management work pane. Optionally, you can also open the task by clicking on the logged on user name link displayed in the task bar below the banner. By default, all items are selected in the **Change User Interface Settings** task window.

2. You can deselect any item that you do not want displayed on your interface, then click **Apply** or **OK** for the change to take affect.
3. When Save settings as my defaults at logoff is selected, any customization to the following items are saved when the user logs off:
  - Displayed user interface components, such as the banner and tasks pad
  - Displayed navigation and work pane icons
  - Displayed nodes in the navigation pane
  - Table view customization, such as filters, sorts, column sizing, ordering, and visibility settings
4. To restore all of the user interface settings to the original defaults, click **Factory Defaults**.

Use the online Help to get additional information for changing the user interface settings.

---

## Change User Password

This task allows you to change your existing password used for logging onto the HMC. A password verifies your user ID and your authority to log in to the console.

To change your password:

1. Open the **Change User Password** task from the HMC Management work pane.
2. From the **Change User Password** window specify your current password, specify a new password you want to use, and respecify the new password to confirm in the fields provided.
3. Click **OK** to proceed with the changes.

Use the online Help if you need additional information for changing your password.

Related HMC CLI commands:

- "chhmcusr" on page 151

---

## Create Welcome Text

This task allows you to customize the welcome message or to display a warning message that appears on the **Welcome** window before you log onto the HMC. You can use this text to notify users of certain corporate policies or security restrictions applying to the system.

To create a message:

1. Open the **Create Welcome Text** task from the HMC Management work pane.
2. From the **Create Welcome Text** window, enter a message in the input area.
3. Click **OK** to apply the change. The next time you log in to the HMC, your message is displayed.

Use the online Help to get additional information about displaying a message before logging onto the HMC.

Related HMC CLI commands:

- "chusrtea" on page 175

---

## Format Media

This task formats a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key.

You can use this task to format the following DVD-RAMs:

- Backup/restore
- Service data.

You can format a diskette by supplying a user-specified label.

To format a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key:



1. Open the **Format Media** task from the HMC Management work pane.
2. From the **Format Media** window, select the type of media you want to format, then click **OK**.
3. Make sure your media has been correctly inserted, then click **Format**. The **Format Media** progress window is displayed. When the media is formatted, the **Format Media Completed** window is displayed.
4. Click **OK** and then click **Close** to end the task.

Use the online Help if you need additional information for formatting a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key.

---

## Launch Guided Setup Wizard

This task uses a wizard to set up your system and HMC.

1. Open the **Launch Guided Setup Wizard** from the HMC Management work pane.
2. From the **Launch Guided Setup Wizard - Welcome** window it is recommended that you have certain prerequisites on hand. Click **Prerequisites** in the **Launch Guided Setup Wizard - Welcome** window for the information. When you have completed that, this wizard takes you through the following tasks required to set up your system and HMC. As you complete each task, click **Next** to proceed.
  - a. Change HMC Date and Time
  - b. Change HMC passwords
  - c. Create additional HMC users
  - d. Configure HMC Network Settings (This task cannot be performed if you are accessing the **Launch Guided Setup Wizard** remotely.)
  - e. Specify contact information
  - f. Configure connectivity information
  - g. Authorize users to use Electronic Service Agent and configure notification of problem events.
3. Click **Finish** when you have completed all the tasks in the wizard.

Use the online Help or see the *Installation and Configuration Guide for the Hardware Management Console*, SA76-0084, if you need additional information using the HMC setup wizard.

---

## Launch Remote Hardware Management Console

This task is used to start a session to another Hardware Management Console (HMC).

**Note:** You cannot perform this task remotely.

To open another HMC:

1. Open the **Launch Remote Hardware Management Console** task from the HMC Management work pane.
2. From the **Remote Hardware Management Console Addressing Information** window, specify the TCP/IP address or host name of the remote HMC to be contacted.
3. Click **OK** to proceed.

Use the online Help if you need additional information for contacting another HMC.

---

## Lock HMC Screen

This task is used to lock the HMC screen.

**Note:** You cannot perform this task remotely.

To lock the HMC screen:

1. Open the **Lock HMC Screen** task from the HMC Management work pane. The HMC screen is immediately locked.
2. To unlock the screen and get back to the HMC workplace:
  - a. Press the Enter key
  - b. Specify the password of the user ID you are logged in as

---

## Logoff or Disconnect

**Note:** This task is located on the right side of the task bar, click **Logoff** to access. The **Choose to Logoff or Disconnect** window appears.

This task allows you to end the current user session and logs off the HMC or it allows you to disconnect while your tasks continue running. If you disconnect, you can reconnect at a later time to continue working. However, a disconnected session is eventually ended. (This is because disconnected sessions exist only while the HMC application is running. If the HMC is restarted or the console is shut down or rebooted, all session information is lost.) If you log off, this means you no longer need access to the HMC. Logging off the console does not affect the status of the managed systems.

To log off or disconnect from the HMC:

1. Click **Logoff** from the task bar or click the red **X** in the upper right corner of the workplace. The **Choose to Logoff or Disconnect** window appears.
2. Select whether you want to logoff or disconnect, click **OK** to proceed. After you log off or disconnect, the **Welcome to the HMC** window is displayed.

If you chose to disconnect rather than logoff, when you login again, the **Choose a Disconnected Session** window appears. You can do one of the following:

- Select the disconnected session to continue working (click **Reconnect**)
- Start a new session (click **New Session**)
- Delete a selected session (click **Delete**)
- Cancel from connecting (click **Cancel**)

**Note:** The number of windows displayed when you reconnect depends on the state of the session when it was disconnected. One of the windows is the main user interface; additional windows are for each task that was running when the session was disconnected.

---

## Manage Certificates

Use this task to manage the certificates used on your HMC. It provides the capability of getting information on the certificates used on the console. This task allows you to create a new certificate for the console, change the property values of the certificate, and work with existing and archived certificates or signing certificates.

All remote browser access to the HMC must use Secure Sockets Layer (SSL) encryption. With SSL encryption required for all remote access to the HMC, a certificate is required to provide the keys for this encryption. The HMC provides a self-signed certificate that allows this encryption to occur.

To manage your certificates:

1. Open the **Manage Certificates** task from the HMC Management work pane.
2. Use the menu bar from the **Manage Certificates** window for the actions you want to take with the certificates:
  - To create a new certificate for the console, click **Create**, then select **New Certificate**. Determine whether your certificate will be self-signed or signed by a Certificate Authority (CA), then click **OK**.
  - To modify the property values of the self-signed certificate, click **Selected**, then select **Modify**. Make the appropriate changes, then click **OK**.

- To work with existing and archived certificates or signing certificates, click **Advanced**. Then you can choose the following options:
  - Delete existing certificates
  - Work with archived certificates
  - Import certificates
  - View issuer certificates

3. Click **Apply** for all changes to take effect.

Use the online Help if you need additional information for managing your certificates and see Appendix B, “Remote operations,” on page 133 for more information on remotely accessing the HMC.

---

## Manage Data Replication

This task enables or disables customized data replication. Customized data replication allows another HMC to obtain customized console data from or send data to this HMC.

The following types of data can be configured:

- Customer information data
  - Administrator information (customer name, address, telephone number, etc.)
  - System information (administrator name, address, telephone of your system)
  - Account information (customer number, enterprise number, sales branch office, etc.)
- Group data
  - All user-defined group definitions.
- Modem configuration data
  - Configure modem for remote support.
- Outbound connectivity data
  - Configure local modem to RSF
  - Enable an internet connection
  - Configure to an external time source.

**Note:** Customizable console data is accepted from other HMCs only after specific HMCs and their associated allowable customizable data types have been configured.

For more detailed information on customizing console data for data replication, see Appendix C, “Customizable data replication,” on page 139.

Use the online Help to get additional information for enabling or disabling customizable data replication.

---

## Manage Task and Resource Roles

Use this task to define and customize user roles.

**Note:** Predefined roles (default roles) cannot be modified.

A *user role* is a collection of authorizations. A user role can be created to define the set of tasks allowed for a given class of user (*task roles*) or it can be created to define the set of managed objects that are manageable for a user (*managed resource roles*). Once you have defined or customized the user roles you can use the **Manage User Profiles and Access** task to create new users with their own permissions. (See “Manage User Profiles and Access” on page 100.)

The predefined managed resource roles include:

- All System Resources

The predefined task roles include:

- hmcshervicerep (Service Representative)
- hmcviewer (Viewer)
- hmcoperator (Operator)
- hmcpe (Product Engineer)
- hmcshuperadmin (Super Administrator)

To customize managed resource roles or task roles:

1. Open the **Manage Task and Resource Roles** task from the HMC Management work pane.
2. From the **Manage Task and Resource Roles** window, select either **Managed Resource Roles** or **Task Roles**.
3. To add a role, click **Edit** from the menu bar, then click **Add...** to create a new role.  
or  
To copy, remove, or modify an existing role, select the object you want to customize, click **Edit** from the menu bar, then click **Copy...**, **Remove**, or **Modify...**
4. Click **Exit** when you have completed the task.

Use the online Help to get additional information for customizing managed resource roles and task roles.

Related HMC CLI commands:

- "chaccfg" on page 147
- "lssaccfg" on page 209
- "mkaccfg" on page 215
- "rmaccfg" on page 227

---

## Manage User Profiles and Access

Use this task to manage your system users that log on to the HMC. A user profile is a combination of a user ID, permissions, and a text description. Permissions represent the authority levels assigned to the user profile for the objects the user has permission to access.

The user ID and password are used to verify a user's authorization to log on the HMC. The user ID must start with an alphabetic character and consist of 1 to 32 characters. The password has the following rules:

- Must begin with an alphanumeric character.
- Must contain at least seven characters, however, this limit may be changed by your system administrator.
- The characters should be standard 7-bit ASCII characters.
- Valid characters to use for the password can be: A-Z, a-z, 0-9 and special characters (~ ! @ # \$ % ^ & \* ( ) \_ + - = { } [ ] \ : " ; ' ).

The user profile includes managed resource roles and task roles that are assigned to the user. The *managed resource roles* assign permissions for a managed object or group of objects and the *task roles* define the access level for a user to perform on a managed object or group of objects. You can choose from a list of available default managed resource roles, task roles, or customized roles created by using the **Manage Task and Resource Roles** task.

See Appendix A, "HMC tasks and user roles/IDs," on page 127 for a listing of all the HMC tasks and the predefined default user IDs that can perform each task.

The default managed resource roles include:

- All System Resources

The default task roles include:

- hmcshervicerep (Service Representative)

- hmcviewer (Viewer)
- hmcoperator (Operator)
- hmcpe (Product Engineer)
- hmcsuperadmin (Super Administrator).

To add or customize a user profile:

1. Open the **Manage User Profiles and Access** task from the HMC Management work pane.
2. From the **User Profiles** window, if you are creating a new user ID, point to **User** on the menu bar and when its menu is displayed, click **Add....** The **Add User** window is displayed.

or

From the **User Profiles** window, if the user ID already exists in the window, select the user ID from the list, and then point to **User** on the menu bar and when its menu is displayed, click **Modify....** The **Modify User** window is displayed.

3. Complete or change the fields in the window, click **OK** when you are done.

Use the online Help if you need additional information for creating, modifying, copying, or removing a user profile.

Related HMC CLI commands:

- “chhmcusr” on page 151
- “lshmcusr” on page 192
- “mkhmcusr” on page 216
- “rmhmcusr” on page 228

---

## Manage Users and Tasks

This task displays the logged on users and the tasks they are running.

1. Open the **Manage Users and Tasks** task from the HMC Management work pane.
2. From the **Manage Users and Tasks** window, the following information is displayed:
  - User you are logged in as
  - Time you logged in
  - Number of tasks running
  - Your access location
  - Information about tasks that are running:
    - Task ID
    - Task name
    - Targets (if any)
    - Session ID
3. You can choose to log off or disconnect from a session that is currently running by selecting the session from the Users **Logged On** list, then click **Logoff** or **Disconnect**.  
Or, you can choose to switch to another task or end a task by selecting the task from the **Running Tasks** list, then click **Switch To** or **Terminate**.
4. When you have completed this task, click **Close**.

---

## Open 5250 Console

Use this task to open a 5250 emulator session so you can communicate with an i5/OS logical partition.

**Note:** You cannot perform this task remotely.

To open a 5250 console:

1. Open the **Open 5250 Console** task from the HMC Management work pane. The **5250 Setup** window is displayed.

2. From the **5250 Setup** window, you can configure and start your 5250 emulator.

---

## Open Restricted Shell Terminal

Use this task to acquire a command line session.

**Note:** You cannot perform this task remotely.

To open a restricted shell terminal:

1. Open the **Open Restricted Shell Terminal** task from the HMC Management work pane. The **Restricted Shell** window is displayed.
2. From the **Restricted Shell** window you can issue commands remotely through secure shell access to the managed system. This provides consistent results and automates administration of managed systems.

---

## Remote Command Execution

This task is used to enable remote command execution using the ssh facility.

1. Open the **Remote Command Execution** task from the HMC Management work pane.
2. From the **Remote Command Execution** window, select **Enable remote command execution using the ssh facility**.
3. Click **OK**.

See Appendix B, “Remote operations,” on page 133 for more information.

---

## Remote Operation

This task is used to allow the HMC to be accessed at a remote workstation through a web browser.

To enable the HMC remote access:

1. Open the **Remote Operation** task from the HMC Management work pane.
2. Select **Enabled** from the Remote Operation drop-down list, then click **OK**. The HMC can be accessed from a remote workstation using a web browser.

Use the online Help to get additional information for allowing remote access to the HMC.

---

## Remote Virtual Terminal

A Remote Virtual Terminal connection is a terminal connection to a logical partition from another remote HMC. Use this task to enable Remote Virtual Terminal access for remote clients.

1. Open the **Remote Virtual Terminal** task from the HMC Management work pane.
2. From the **Remote Virtual Terminal** window, you can enable this task by selecting **Enable remote virtual terminal connections**.
3. Click **OK** to activate your changes.

Use the online Help to get additional information for enabling a remote terminal connection.

---

## Restore HMC Data

This task is used to select a remote repository for restoring critical backup data for the HMC.

1. Open the **Restore HMC Data** task from the HMC Management work pane.
2. From the **Restore HMC Data** window, you can choose to restore data from a Network File System (NFS) server or a File Transfer Protocol (FTP) server.
3. Click **Next** to proceed or **Cancel** to exit the task without making any changes.

Use the online Help if you need additional information about restoring critical backup data for this HMC.

Related HMC CLI commands:

---

## Save Upgrade Data

This task uses a wizard to save upgrade data to selected media. This data consists of files that were created or customized while running the current software level. Saving this data to selected media is performed prior to an HMC software upgrade.

1. Open the **Save Upgrade Data** task from the HMC Management work pane.
2. From the **Save Upgrade Data** window, this wizard takes you through the steps required for saving your data. Select the type of media you want to save your data to, then click **Next** to proceed through the task windows.
3. Click **Finish** when you have completed the task.

Use the online Help if you need additional information for saving upgrade data.

Related HMC CLI commands:

- “rstupgdata” on page 235
- “saveupgdata” on page 235

---

## Schedule Operations

Use this task to create a schedule for certain operations to be performed on the HMC itself without operator assistance.

Scheduled operations are helpful for situations where automatic, delayed, or repetitious processing of system operations is necessary. A scheduled operation is started at a specified time, without operator assistance to perform the operation. A schedule can be set for one operation or repeated many times.

For example, you could schedule a backup of important HMC information to DVD to occur once, or set up a repeating schedule.

The **Scheduled Operations** task displays the following information for each operation:

- The processor that is the object of the operation.
- The scheduled date
- The scheduled time
- The operation
- The number of remaining repetitions

From the **Scheduled Operations** window you can:

- Schedule an operation to run at a later time
- Define operations to repeat at regular intervals
- Delete a previously scheduled operation
- View details for a currently scheduled operation
- View scheduled operations within a specified time range
- Sort scheduled operations by date, operation, or managed system

An operation can be scheduled to occur one time or it can be scheduled to be repeated. You will be required to provide the time and date that you want the operation to occur. If the operation is scheduled to be repeated, you will be asked to select:

- The day or days of the week that you want the operation to occur. (optional)
- The interval, or time between each occurrence. (required)
- The total number of repetitions. (required)



The operation that can be scheduled for the HMC is:

### **Backup Critical Console Data**

Schedules an operation to back up the critical console hard disk information for the HMC.

To schedule operations on the HMC:

1. Open the **Schedule Operations** task from the HMC Management work pane.
2. From the **Schedule Operations** window, click **Options** from the menu bar to display the next level of options:
  - To add a scheduled operation, point to **Options** and then click **New...**
  - To delete a scheduled operation, select the operation you want to delete, point to **Options** and then click **Delete**.
  - To update the list of scheduled operations with the current schedules for the selected objects, point to **Options** and then click **Refresh**.
  - To view a scheduled operation, select the operation you want to view, point to **View** and then click **Schedule Details...**
  - To change the time of a scheduled operation, select the operation you want to view, point to **View** and then click **New Time Range...**
  - To sort the scheduled operations, point to **Sort** and then click one of the sort categories that appears.
3. To return to the HMC workplace, point to **Options** and then click **Exit**.

Use the online Help to get additional information for scheduling an operation.

---

## **Shut Down or Restart**

This task enables you to shut down (power off the console) or to restart the console.

1. Open the **Shut Down or Restart** task from the HMC Management work pane.
2. From the **Shut Down or Restart** window, you can:
  - Select **Restart the HMC** to automatically restart the HMC once the shut down has occurred.
  - Do not select **Restart the HMC** if you do not want to automatically restart the HMC.
3. Click **OK** to proceed with the shut down, otherwise click **Cancel** to exit the task.

Use the online Help if you need additional information about shutting down or restarting the HMC.

Related HMC CLI commands:

- "hmcshutdown" on page 183

---

## **Test Network Connectivity**

This task displays network diagnostic information for the console's TCP/IP connection. It also allows you to send an echo request (click **Ping**) to a remote host.

To view information concerning the networking configuration on this HMC:

1. Open the **Test Network Connectivity** task from the HMC Management work pane.
2. From the **Test Network Connectivity** window, you can use the following tabs to view the network information.
  - Ping
  - Interfaces
  - Address
  - Routes
  - Address Resolution Protocol (ARP)



- Sockets
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Internet Protocol (IP)

3. Click **Cancel** when you have completed this task.

Use the online Help to get additional information on your console's network information.

Related HMC CLI commands:

- **ping**

---

## Tip of the Day

This task allows you to view information about using the HMC. A different fact or tip is displayed each time you log in.

The **Tip of the Day** window is displayed as long as **Show tips each time you log on** is selected on the window. You can also look at additional information by clicking **Previous Tip** or **Next Tip**.

To prevent this window from displaying each time you log in you can deselect **Show tips each time you log on**, then click **Close**.

To access this task other than having it appear as you log in to the HMC:

1. Open **Tip of the Day** from the HMC Management work pane.
2. From the **Tip of the Day** window, you can select options as previously specified.
3. Click **Close** to save the changes or exit the task.

---

## View HMC Events

This task enables you to view a record of system events occurring on the HMC. System events are individual activities that indicate when processes occur, begin and end, succeed or fail.

1. Open the **View HMC Events** task from the HMC Management work pane.
2. From the **View HMC Events** window, a table is displayed that lists all the events that occurred on the HMC. Initially, the events are displayed in descending order, from the most recent event to the oldest event. The information includes the date, the time, and the console event.
3. Use **View** on the menu bar from the **View Console Events** window to change to a different time range, or to change how the events display in the summary. You can also use the table icons or the **Select Action** menu on the table toolbar to display different variations of the table.
4. When you are done viewing the events, select **View** on the menu bar, then **Exit** to leave the task.

Use the online Help for additional information about viewing HMC events.

Related HMC CLI commands:

- "lssvcevents" on page 209

---

## View Licenses

Use this task to view the Licensed Internal Code (LIC) that you have agreed to for this HMC. This task is displayed when you initially start the HMC.

1. Open the **View Licenses** task from the HMC Management work pane.
2. From the **View Licenses** window, you can click on any of the license links to view more information.

**Note:** This list does not include programs and code provided under separate license agreements.

3. Click **OK** to close the window.

---

## View Network Topology

This task is used to display a tree view of the network nodes known to this Hardware Management Console. Examples of such nodes are managed systems, logical partitions, storage, and other Hardware Management Consoles.

To view the network topology:

1. Open the **View Network Topology** task from the HMC Management work pane.
2. From the **View Network Topology** window, you can do the following:
  - You can view attributes of a node by selecting the node in the tree view that is shown in the left pane under **Current Topology**. Attributes vary according to the type of node. Some examples are IP address, host name, location code, and status. Click **Refresh** to rediscover the topology and to query the nodes again for status and other attributes.
  - You can save a snapshot of the current topology (select an item in the **Current Topology**, then click **Save**) and view it in the saved reference topology. You can view attributes of a node in the saved topology by selecting the node in the tree view that is shown in the left pane under **Saved Topology**.
  - You can test network connectivity to a node by selecting the node in either the current or the saved topology views and click **Ping Current Node** or **Ping Saved Node**, available only for nodes that include an IP address or a host name. The information is displayed in the right pane.
3. Click **Close** when you have completed this task.

Use the online Help if you need additional information for viewing the network topology of the Hardware Management Console.

---

## Chapter 8. Service Management tasks

This chapter alphabetically describes the tasks that are available on the Hardware Management Console (HMC) for the **Service Management** tasks.

To open these tasks, see “Service Management” on page 33.

**Note:** Depending on the task roles assigned to your user ID you may not have access to all the tasks. See Table 10 on page 127 for a listing of the tasks and the user roles allowed to access them.

---

### Create Serviceable Event

This task reports problems that occurred on your Hardware Management Console to the service provider (for example, the mouse does not work) or lets you test problem reporting.

Submitting a problem is dependent upon whether you have customized this Hardware Management Console to use the Remote Support Facility (RSF) and if it is authorized to automatically call for service. If so, the problem information and service request is sent to the service provider automatically with a modem transmission.

To report a problem on your Hardware Management Console:

1. Open the **Create Serviceable Event** task from the tasks pad.
2. From the **Report a Problem** window, select a problem type from the list displayed.
3. Enter a brief description of your problem in the **Problem Description** input field and then click **Request Service**.

or

To test problem reporting from the **Report a Problem** window:

1. Select **Test automatic problem reporting** and enter *This is just a test* in the **Problem Description** input field.
2. Click **Request Service**. The problems are reported to the service provider for the Hardware Management Console. Reporting a problem sends to the service provider the information you provide on **Report a Problem** window, and machine information that identifies the console.

Use the online Help if you need additional information for reporting a problem or testing if problem reporting works.

---

### Format Media

This task formats a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key.

You can use this task to format the following DVD-RAMs:

- Backup/restore
- Service data.

You can format a diskette by supplying a user-specified label.

To format a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key:

1. Open the **Format Media** task from the HMC Management work pane.
2. From the **Format Media** window, select the type of media you want to format, then click **OK**.

3. Make sure your media has been correctly inserted, then click **Format**. The **Format Media** progress window is displayed. When the media is formatted, the **Format Media Completed** window is displayed.
4. Click **OK** and then click **Close** to end the task.

Use the online Help if you need additional information for formatting a DVD-RAM, diskette, or USB 2.0 Flash Drive Memory Key.

---

## Load Serviceable Events

This task allows you to load or reload serviceable events from an XML file.

1. Open the **Load Serviceable Events** task from the Service Management work pane.
2. From the **Load Serviceable Events** window, specify the path and name of the XML file.
3. Click **press for update** to proceed.

---

## Manage Connection Monitoring

This task configures the timers that connection monitoring uses to detect outages and enables or disables connection monitoring for selected machines.

You can view and, if authorized, change connection monitoring settings by machine. Connection monitoring generates serviceable events when communication problems are detected between the HMC and managed systems. If you disable connection monitoring, no serviceable events are generated for networking problems between the selected machine and this HMC.

To monitor the connections:

1. Open the **Manage Connection Monitoring** task from the Service Management work pane.
2. From the **Manage Connection Monitoring** window, adjust the timer settings, if required, and enable or disable the server.
3. Click **OK** when you have completed the task.

Use the online Help if you need additional information about connection monitoring.

---

## Manage Customer Information

This task enables you to customize the customer information for the HMC.

**Note:** If Customizable Data Replication is *Enabled* on this HMC (using the **Manage Data Replication** task), the data specified in this task may change depending on automatic replication from other HMCs configured on your network. For more information on data replication, see "Manage Data Replication" on page 99.

The **Manage Customer Information** window displays the following tabs for providing input:

- Administrator
- System
- Account

To customize your customer information:

1. Open the **Manage Customer Information** task from the Service Management work pane.
2. From the **Manage Customer Information** window, provide the appropriate information on the **Administrator** page.

**Note:** Information is required for fields with an asterisk (\*).

3. Select the **System** and **Account** tabs from the **Manage Customer Information** window to provide additional information.

4. Click **OK** when you have completed the task.

Use the online Help to get additional information about customizing your account information.

---

## Manage Dumps

This task manages procedures for dumps of the selected system.

To manage a dump:

1. Open the **Manage Dumps** task from the Service Management work pane.
2. From the **Manage Dumps** window, select a dump and perform one of the following dump-related tasks:

From **Selected** on the menu bar:

- Copy the dump to media.
- Copy the dump to a remote system.
- Use the call home feature to transmit the dump to your service provider.
- Delete a dump.

From **Actions** on the menu bar:

- Initiate a dump of the hardware and server firmware for the managed system.
- Initiate a dump of the service processor.
- Initiate a dump of the Bulk Power Control service processor.
- Modify the dump capability parameters for a dump type.

From **Status** on the menu bar, you can view the offload progress of the dump.

3. Click **OK** when you have completed this task.

Use the online Help to get additional information for managing dumps.

Related HMC CLI commands:

- “dump” on page 180
- “cpdump” on page 176
- “getdump” on page 181
- “lsdump” on page 189
- “startdump” on page 237

---

## Manage eService Registration

This task allows you to request authorization for Electronic Service Agent. Electronic Service Agent associates your system with a user ID and allows access to system information through the Electronic Service Agent facility. This registration is also used by your operating system to automate service processes for your AIX or i5/OS operation system.

To register a user ID:

1. Open the **Manage eService Registration** task from the Service Management work pane.
2. From the **Manage eService Registration** window, provide a user ID that is registered with the Electronic Service Agent. If you need a user ID, you can register at the IBM Registration website, <https://www.ibm.com/account/profile>.
3. Click **OK** when you have completed this task.

Use the online Help if you need additional information for registering a customer user ID with the eService web site.

---

## Manage Inbound Connectivity

This task allows your service provider to temporarily access your local console, such as the HMC, or the partitions of a managed system.

1. Open the **Manage Inbound Connectivity** task from the Service Management work pane.
2. From the **Customize Inbound Connectivity** Settings window:
  - Use the **Remote Service** tab to provide the information necessary to start an attended remote service session.
  - Use the **Call Answer** tab to provide the information necessary to accept incoming calls from your service provider to start an unattended remote service session.
3. Click **OK** to proceed with your selections.

Use the online Help if you need additional information on managing the inbound connectivity.

---

## Manage Outbound Connectivity

This task allows you to customize the means for outbound connectivity for the HMC to use to connect to remote service.

**Note:** If Customizable Data Replication is **Enabled** on this HMC (using the **Manage Data Replication** task), the data specified in this task may change depending on automatic replication from other HMCs configured on your network. For more information on data replication, see “Manage Data Replication” on page 99.

You can configure this HMC to attempt connections through the local modem, Internet, Internet Virtual Private Network (VPN), or through a remote pass-through system. Remote service is a two-way communication between the HMC and the IBM Service Support System for the purpose of conducting automated service operations. The connection can only be initiated by the HMC. IBM Service Support System cannot and never attempts to initiate a connection to the HMC.

To customize your connectivity information:

1. Open the **Manage Outbound Connectivity** task from the Service Management work pane.
2. From the **Manage Outbound Connectivity** window select **Enable local server as call-home server** (a check mark appears) before proceeding with the task.

**Note:** You must first **Accept** the terms described about the information you provided in this task. This allows the local HMC to connect to your service provider’s remote support facility for call-home requests.

3. The dial information window displays the following tabs for providing input:
  - Local Modem
  - Internet
  - Internet VPN
  - Pass-Through Systems
4. If you want to allow connectivity over a modem, use the **Local Modem** tab, then select **Allow local modem dialing for service**.
  - a. If your location requires a prefix to be dialed in order to reach an outside line, click **Modem Configuration...** and enter the **Dial prefix** in the **Customize Modem Settings** window required by your location. Click **OK** to accept the setting.
  - b. Click **Add...** from the **Local Modem** tab page to add a telephone number. When local modem dialing is allowed, there must be at least one telephone number configured.
5. If you want to allow connectivity over the Internet, use the **Internet** tab, then select **Allow an existing internet connection for service**. Refer to *Installation and Configuration Guide for the Hardware Management Console*, SA76-0084, for more information on configuring the HMC as a call-home server using LAN-based internet and SSL.

6. If you want to configure the use of a VPN over an existing Internet connection to connect from the local HMC to your service provider's remote support facility, use the **Internet VPN** tab.
7. If you want to allow the HMC to use the pass-through systems as configured by the TCP/IP address or host name, use the **Pass-Through Systems** tab.
8. When you complete all the necessary fields, click **OK** to save your changes.

Use the online Help if you need additional information for customizing outbound connectivity information.

---

## Manage POWER4 Service Agent

This task enables or disables the Electronic Service Agent Connection Manager function and specifies the port location for the connection. Electronic Service Agent Connection Manager allows POWER4 systems to use Electronic Service Agent to call home to transmit service and system information to IBM by specifying the port used for connectivity for a single, secure connection.

1. Open the **Manage POWER4 Service Agent** task from the Service Management work pane.
2. From the **Manage POWER4 Service Agent** window, select **Enable Service Agent Connection Manager** (a check mark appears), then provide the connectivity features for the HMC.
3. Click **OK** when you have supplied the necessary information.

Use the online Help if you need additional information for enabling or disabling Electronic Service Agent.

---

## Manage Remote Connections

This task enables you to manage remote connections.

**Note:** The HMC's call-home server service must be enabled for you to use this task. (See "Manage Systems Call-Home" on page 112 for more information.)

The HMC manages remote connections automatically. It puts requests on a queue and processes them in the order in which they are received. However, this task allows you to manage the queue manually, if necessary. You can stop transmissions, move priority requests ahead of others, or delete requests.

To manage remote connections:

1. Open the **Manage Remote Connections** task from the Service Management work pane.
2. From the **Manage Remote Connections** window, a list of transmitting requests being and a list of waiting requests transmitted are displayed. You can select requests from either list and display the available options by clicking **Options** on the menu bar. The options permit you to:
  - Prioritize a selected request (move it to the top of the queue)
  - Cancel selected requests
  - Cancel all active requests (those being transmitted)
  - Cancel all waiting requests
  - Hold the queue (puts queue on hold after completing current active request)
  - Release the queue
  - Close the window and exit

Use the online Help if you need additional information for manually managing remote connections.

---

## Manage Remote Support Requests

This task views or manages call-home requests that the console has submitted.

1. Open the **Manage Remote Support Requests** task from the Service Management work pane.



2. From the **Manage Remote Support Requests** window, a list of active requests and a list of waiting requests are displayed. You can select requests from either list and display the available options by clicking **Options** on the menu bar. The options permit you to:
  - View all call-home servers
  - Cancel selected requests
  - Cancel all active requests
  - Cancel all waiting requests
  - Close the window and exit

Use the online Help if you need additional information for manually managing remote connections.

---

## Manage Serviceable Event Notification

This task adds email addresses that notify you when problem events occur on your system and configures how you want to receive notification of system events from the Electronic Service Agent.

To set up notification:

1. Open the **Manage Serviceable Event Notification** task from the Service Management work pane.
2. From the **Manage Serviceable Event Notification** window, you can do the following:
  - Use the **Email** tab to add the email addresses that will be notified when problem events occur on your system.
  - Use the **SNMP Trap Configuration** tab to specify locations for sending Simple Network Management Protocol (SNMP) trap messages for Hardware Management Console application program interface events.
3. Click **OK** when you have completed this task.

Use the online Help if you need additional information for managing serviceable events notification.

Related HMC CLI commands:

- “chsacfg” on page 161
- “lssacfg” on page 209

---

## Manage Serviceable Events

This task allows you to select the criteria for the set of serviceable events you want to view. When you finish selecting the criteria, you can view the serviceable events that match your specified criteria.

To set the criteria for the serviceable events you to view:

1. Open the **Manage Serviceable Events** task from the Service Management work pane.
2. From the **Manage Serviceable Events** window, provide event criteria, error criteria, and FRU criteria.
3. Click **OK** when you have specified the criteria you want for the serviceable events you want to view.

Use the online Help if you need additional information managing events.

Related HMC CLI commands:

- “chsvcevent” on page 163
- “lssvcevents” on page 209

---

## Manage Systems Call-Home

This task allows you enable or disable the call-home state for managed systems.



**Note:** If Customizable Data Replication is **Enabled** on this HMC (using the **Manage Data Replication** task), the data specified in this task may change depending on automatic replication from other HMCs configured on your network. For more information on data replication, see “Manage Data Replication” on page 99.

By enabling the call-home state for a managed system this causes the console to automatically contact a service center when a serviceable event occurs. When a managed system is disabled, your service representative is not informed of serviceable events.

To manage call-home for the system(s):

1. Open the **Manage Systems Call-Home** task from the Service Management work pane.
2. From the **Manage Systems Call-Home** window, select a system or systems you want to enable or disable the call-home state.
3. Click **OK** when you have completed the task.

Use the online Help if you need additional information for managing serviceable events notification.

---

## Transmit Service Information

Use this task to transmit service information.

1. Open the **Transmit Service Information** task from the Service Management work pane.
2. From the **Transmit Service Information** window, you can work with the following tabs:
  - Select the **Transmit** tab. Use this page to schedule when to transmit service data to your service provider (specifying frequency in days and time of day) and how you want to transmit the service and performance management information.
  - Select the **FTP** tab. Use this page to configure the File Transfer Protocol (FTP) information for the FTP server, with or without a firewall, for off loading service information. This service information is extended error data consisting of problem related-data about problems opened on the HMC for the HMC or managed system.
  - Select the **Transmit Service Data to IBM** tab. Use this page to provide the ability to send information that is stored on the HMC hard disk that can be used for problem determination. The data may be **traces**, **logs**, or **dumps** and the destination for the data may be the IBM Service Support System, a diskette, USB flash memory drive, or a DVD-RAM. Before you can send information to the IBM Service Support System, Phone Server and Remote Service must be **enabled**. To enable remote service, see “Remote Operation” on page 102. To enable telephone server, see “Manage Outbound Connectivity” on page 110.
3. Click **OK** when you have completed the task.

Use the online Help for additional information about transmitting service information.

Related HMC CLI commands:

- “chsacfg” on page 161
- “lssacfg” on page 209



---

## Chapter 9. Updates

**Updates** displays tasks to manage Licensed Internal Code (LIC) on your HMC, managed system, power subsystem, or I/O adapters.

Use the **Update HMC** button to update Licensed Internal Code on the HMC. Before updating LIC on the HMC, see “Update HMC.”

Other tasks are used to update managed system, power subsystem, and I/O adapter LIC. To launch these tasks, see “Launching tasks for managed objects” on page 24. The following sets of tasks are represented in the tasks pad, tasks menu, or context menu. The tasks listed in the tasks pad change as selections are made in the work area. The context is always listed at the top of the tasks pad in the format Task: Object.

To display the tasks:

1. Select the **Updates** node in the navigation pane.
2. Select a managed object to apply updates on.
3. From the tasks pad, click on the task you want to perform.
4. The tasks pad provides the following tasks required to install corrective service:
  - “Change Licensed Internal Code for the current release” on page 117
  - “Upgrade Licensed Internal Code to a new release” on page 121
  - “Flash Side Selection” on page 124
  - “Check system readiness” on page 124
  - “View system information” on page 124

---

### Update HMC

When the **Updates** node is selected in the navigation pane, current code levels for the HMC are displayed in the work pane.

Under **HMC Code level** is displayed:

- Version
- Release
- Service Pack
- Build Level
- Base Version
- Serial Number of the HMC
- Bios Version on the HMC

The Fix Central web site at <http://www.ibm.com/eserver/support/fixes> offers online media ordering, installation instructions and related technical information on code updates of the HMC. Before updating the HMC code level, verify the current levels on your HMC and check on the web site to determine if an update is needed or recommended.

Before updating the HMC code level, you should:

- Backup critical HMC data to a DVD or a remote system so that the HMC can be restored in the event of a problem in updating. For more information on backing up HMC data, see “Back up HMC Data” on page 93.

Depending on the complexity of the fix you are applying, you may want to:

- Backup system profile and partition profile data for each system managed by the HMC before updating, so that current profile data can be restored, if necessary. For more information about backing up profile data, see “Manage Partition Data” on page 49
- Record HMC configuration information to enable you to restore the current configuration to the newly updated system:
  1. Record scheduled operations on the HMC. For information on viewing current scheduled operations, see “Schedule Operations” on page 103.
  2. Record whether **Enable remote command execution using the ssh facility** is checked in the “Remote Command Execution” on page 102 task under HMC Management.

Once the tasks above have been performed, select the **Update HMC** button to update the HMC LIC. You will be prompted for the location of the update. Updates can be performed from media or from a remote location.

---

## Managed System Updates

When a managed system is selected, **Updates** tasks perform a guided update of managed system, power subsystem, or I/O Licensed Internal Code.

The following are represented in the **Updates** tasks:

- “Change Licensed Internal Code for the current release” on page 117
- “Upgrade Licensed Internal Code to a new release” on page 121
- “Flash Side Selection” on page 124
- “Check system readiness” on page 124
- “View system information” on page 124

Licensed Internal Code (LIC) can be changed in two ways. You can upgrade the LIC installed on a managed system to a new release, or update the existing LIC running on the system.

An update of a current LIC release may fix problems or add additional function. Updating LIC may or may not be a disruptive process. Updates that do not disrupt the system are called concurrent updates. To update the LIC currently installed on the managed system, use the **Change Licensed Internal Code for the current release** task.

A new release of LIC may add support for new hardware or add new function. Upgrading LIC to a new release is *always a disruptive process* requiring a complete shut down, power off, and restart of the system. To upgrade LIC to a new release, use the **Upgrade Licensed Internal Code to a new release** task.

Concurrent updates allow the system and the applications running on the system to continue to run as the LIC update is applied. This appreciably lessens the system downtime associated with LIC maintenance. Most updates released will be concurrent. However, certain types of problems are critical to fix and can be fixed only with a disruptive update. Using the **View system information** task, you are able to view the levels of LIC available in a repository and determine which of the available updates are concurrent and which are disruptive.

If the update is disruptive, you are given the option of installing and activating (incurring the disruption) or deferring the activation to a more convenient time. Concurrent updates can only be done for managed system LIC.

New releases of LIC (upgrades) and updates to these releases are available from the following repositories:

- IBM service web site
- IBM support system
- DVD - a DVD can be ordered from IBM or a DVD may be created that contains downloaded LIC

- FTP site - a site accessible to your HMC by FTP that contains a previously downloaded level of LIC
- HMC hard drive - LIC may be downloaded directly to the HMC's hard drive or the hard drive may contain a previously downloaded level of LIC

Use the **Flash Side Selection** task to select which flash side will be active after the next activation. (This task is intended for service user mode only.)

Use the **Check system readiness** task to check that all systems selected are in the correct state for LIC update.

Choose the **View system information** task to view the level of LIC currently installed on your managed system or I/O. When a repository is selected, **View system information** also displays retrievable levels of LIC available in the repository.

## Change Licensed Internal Code for the current release

Use this task to apply updates to the currently installed Licensed Internal Code (LIC) on your system.

This task requires access to a service repository, either a remote location, the HMC hard drive, or a DVD drive.

LIC updates can be downloaded directly from IBM's service web site or IBM's support system during the update process.

If you have completed a code update from a repository to one of your managed systems or power subsystems, that code is available in the Hard Drive repository on the HMC for installation on other systems. You can select **Hard Drive** to update other managed systems or power subsystems with the same code.

LIC updates can also be downloaded and written to a DVD or to another system available to your HMC using FTP. You can select DVD drive or FTP site to install the LIC update from these locations.

Multiple managed systems can be updated simultaneously by selecting them from the target list.

Files are selectively downloaded to the HMC to apply LIC updates. From this task, you can:

- View current levels of Licensed Internal Code on a managed system, power subsystem, or I/O.
- View retrievable levels of Licensed Internal Code in a repository.
- Install and activate LIC updates (update to a new level of LIC).
- Remove and activate LIC updates (downgrade to a previous level of LIC).

See "Example: Change Licensed Internal Code for the Current Release" on page 118 for more information.

Select **Start Change Licensed Internal Code wizard** to perform a guided update of managed system, power, and I/O Licensed Internal Code (LIC):

1. A **System readiness check** is automatically performed to check that the system is in the right state for LIC update. If the readiness check fails, actions needed to correct the problems preventing the update are reported to you.
2. Choose a repository from which to update your system. You can update from IBM's service web site, IBM's support system, or, if you have already downloaded an update to the HMC, an FTP site, or a DVD and if you want to update from those locations, choose that option.
3. If you choose **FTP site**, you are prompted for a user ID, password, and the directory in which the update is located.
4. Select the type of update to install, **Managed system and Power LIC** or **I/O LIC**. If there are no LIC updates available in the repository for the type of update chosen, no prompts for installation occur.

5. Confirm that the update as displayed is the correct update. Displayed is the chosen repository, the target or targets of the update, the concurrency status of the target (disruptive or concurrent), and the type of installation. To change the update, select **Advanced Options**.
6. If no changes are desired, continue with the update. Accept the license agreement.
7. Confirm the update.
8. A progress window displays until the update completes.

Select **View system information** to examine current LIC levels on a managed system, power subsystem, or I/O, including levels retrievable from a repository.

Select **Advanced features** to update managed system and power LIC with more options and additional targeting choices.

Related HMC CLI commands:

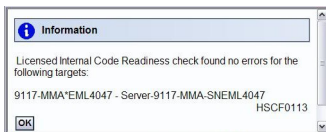
- “lslic” on page 199
- “updlic” on page 238

## Example: Change Licensed Internal Code for the Current Release

In this example, the managed system is currently running at an activated level 26. We wish to update the managed system to level 28. We have previously downloaded this update to another system. We will FTP to this system to install the new level of LIC on our managed system.

To update the LIC currently installed on the managed system, use the **Change Licensed Internal Code for the current release task**:

1. Under **System Management**, choose **Updates**.
2. Select **Change Licensed Internal Code for the Current Release**.
3. Select **Start Change Licensed Internal Code Wizard**.
4. A **System readiness check** is automatically performed to check that the system is in the right state for LIC update. In this example, the readiness check reports that there are no errors preventing the update action:



5. Since the update in this example is located in an FTP directory on another system, choose **FTP site** for the repository.
6. Enter the **FTP site**, **User ID**, **Password**, and the **Directory** on the system where the update is located:

**FTP Site Access Information**

Enter the FTP site address and account access information.

FTP site: 9.00.00.00

User ID: hscroot

Password: ●●●●●●

☐ Accessing a mounted Discovery CD

Directory: /home/hscroot/b0402b\_0713.310

Change Directory...

OK Cancel Help

7. Select **Next** to start the Change Licensed Internal Code wizard.
8. From the Change Licensed Internal Code Wizard panel, confirm that the update as displayed is the desired update. Displayed is the chosen repository, the target or targets of the update, the concurrency status of the target (disruptive or concurrent), and the type of installation:

**Change Licensed Internal Code Wizard**

Select Managed System and Power LIC to install updates. Click Advanced to view the concurrency status of the targets, to change the selected targets, or to select a different installation type.

Current LIC repository location: FTP site

☒ Managed System and Power LIC

Concurrence status: All updates are disruptive.

Current installation type selection: Disruptive install and activate - Power off automatically, if necessary.

Advanced Options...

< Back Next > Finish Cancel Help

The repository we selected (FTP site) contains only one update. There may be multiple updates available in a repository. This repository contains a Managed System and Power LIC update that can only be installed disruptively. The managed system will have to be powered down and restarted before the update will take effect. We can choose to change the installation to defer the disruption to a later time, if desired.

9. Select **Advanced Options** to view more information about the update:

**Managed System and Power Licensed Internal Code (LIC) Concurrency**

Click a table row and click View Information to see the activated and retrievable LIC levels for that target.

Current LIC repository location: FTP site

Select	Target	Target Name	Concurrency Status
<input checked="" type="radio"/>	<input checked="" type="checkbox"/>	Server-9117-MMA-SNEML4047	All must be disruptively activated.

View Information...

Select the type of installation to perform

☐ Concurrent install and activate

☐ Concurrent install only, with deferred disruptive activate

☒ Disruptive install and activate - Power off automatically, if necessary. (Shortest overall update time)

☐ Disruptive install and activate - Delay power off with confirmation. (Shortest system down time)

OK Cancel Help

10. Select the desired target (our managed system) and **View Information** to see the currently activated level of LIC on our managed system and the level of LIC available in the repository (FTP site):

**Managed System and Power Licensed Internal Code (LIC) Level Details**

Click a table row and click View Details to see additional information about the LIC levels based on the current type of installation.

Target name: Server-9117-MMA-SNEML4047

Current LIC repository location: FTP site

Type of installation: Disruptive install and activate - Power off automatically, if necessary.

Select	EC Number	LIC Type	Machine Type/ Model/ Serial Number	Activated Level	Retrievable Concurrent Activate Level	Retrievable Disruptive Activate Level
<input type="radio"/>	01EM310	Managed System	9117-MMA-EML4047 26	NA	NA	28

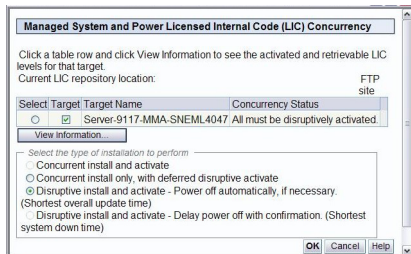
View Details

Close Help



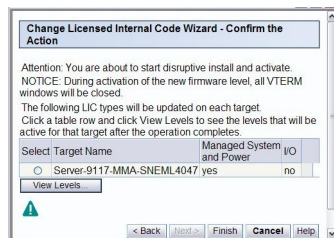
The **Activated Level** of LIC on the managed system is level 26. The activated level of LIC is the level that is currently running on the managed system. The **Retrievable Concurrent Activate Level** of LIC is the level of LIC available in the repository that can be activated without system downtime. In the repository we chose, there were no non-disruptive updates available. The **Retrievable Disruptive Activate Level** is the update we have chosen for this installation. A disruptive level of LIC cannot be activated without disruption. We could choose to defer the disruption.

11. Select **Close** to return to the **Managed System and Power LIC Concurrency** panel:



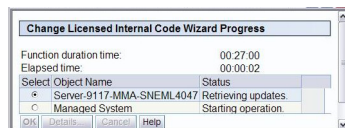
We could choose to defer disruption by selecting **Concurrent install only, with deferred disruptive activate**. The installation of the update to LIC would occur now, but the *activation* of the update would not occur until the next IPL of the managed system. In this example, we will instead incur the disruption now and leave the selection as is, **Disruptive install and activate - Power off automatically, if necessary**.

12. **Accept** the License Agreement.
13. **Confirm** the installation:

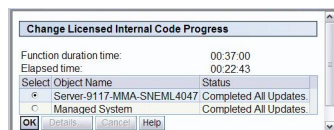


When updating LIC, you may be updating multiple targets with multiple LIC types. You are notified if the levels to be installed are disruptive. In this example, we confirm that the disruptive level of LIC should be installed by clicking **Finish** and **OK** at the confirmation panel.

14. The **Change LIC Wizard Progress** window displays the update progress:



Until the update completes:



15. We can view the levels of LIC on the system to confirm that the update has taken place. From the **Change License Internal Code Wizard**, select **View System Information**. From the **Specify LIC Repository** panel, select **None - Display Current Values** to view the existing LIC levels on the managed system:



Server:9117-MMA-SNEML4047									
Target name:				Server:9117-MMA-SNEML4047					
Current LIC update status:				Enabled					
Current LIC repository location:				None					
EC Number	LIC Type	Machine Type/ Model/ Serial Number	Installed Level	Activated Level	Accepted Level	Unactivated Deferred Level	Platform IPL Level	Update Control	
01EM310	Managed System	9117-MMA*EML4047	28	28	26				HMC
<input type="button" value="View ID Levels"/> <input type="button" value="View Power PDU Levels"/> <input type="button" value="Close"/> <input type="button" value="Help"/>									

The **Installed Level of LIC** is the level just installed, **28**. Since we incurred a disruptive activation of the updated level, the **Activated Level** is also the level just installed, **28**. If we had chosen to *defer* the activation, the **Activated Level** of LIC would have been the previous level, **26**. The **Activated Level of LIC** is written to the t-side (temporary side) of the Flexible Service Processor.

The **Accepted Level** of LIC is the previous level, **26**. A new level of LIC is installed and activated on the t-side of the FSP. Once testing of the new level, **28** has occurred, or when another level is to be installed (i.e. level **29**), the new level, **28** is Accepted, which copies the level from the t-side of the FSP to the p-side (permanent side). This allows you to return to the previous level of LIC should testing prove problematic. In this example, the update we have just installed (level **28**) has not yet been Accepted, so the **Accepted Level** of LIC is at the old level, level **26**.

We have successfully updated the Licensed Internal Code on the managed system from level 26 to level 28!

## Upgrade Licensed Internal Code to a new release

A new release level of Licensed Internal Code (LIC) supports major new function such as the introduction of new hardware models and significant function or features enabled by firmware. In addition to the new function and hardware support, new release levels also contain fixes. Upgrading from one release level to another is disruptive to system operations.

Release levels can be skipped. You can upgrade from release level A to release level D without having to install release level B and C. New release levels of LIC are installed with the this task.

To install a new release of Licensed Internal Code:

1. When you select **Upgrade Licensed Internal Code to a new release**, a readiness check is performed on the system before the task progresses. If the readiness check fails, actions needed to correct the problems preventing the upgrade will be reported to you.
2. Choose a repository from which to upgrade your system. You may upgrade from IBM's service web site, IBM's support system, or, if you have already downloaded an upgrade to the HMC, an FTP site, or a DVD and want to upgrade from those locations, choose that option.
3. Select the desired LIC update, managed system or power subsystem.
4. Once verification of the repository content and targeted systems completes, the license agreement panel displays. Select **Accept** on the license agreement panel, and the confirmation panel displays.
5. If any actions are listed at the bottom of the confirmation panel, complete them, and then click **OK** to confirm that the upgrade should begin. A progress panel displays the results as the upgrade proceeds. At the end of the process, the new release level of LIC will be installed on both the t-side (temporary side) and the p-side (permanent side).

Related HMC CLI commands:

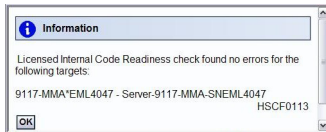
- "lslic" on page 199
- "updlic" on page 238

## Example: Upgrade Licensed Internal Code to a New Release

In this example, the managed system is currently running at release EC Number 01EM310. We wish to upgrade the LIC on the managed system to release NEWLEVEL. We have previously downloaded this new release of LIC to another system. We will FTP to this system to install the new release of LIC on our managed system.

To upgrade the LIC currently installed on the managed system, use the **Upgrade Licensed Internal Code to a New Release** task.

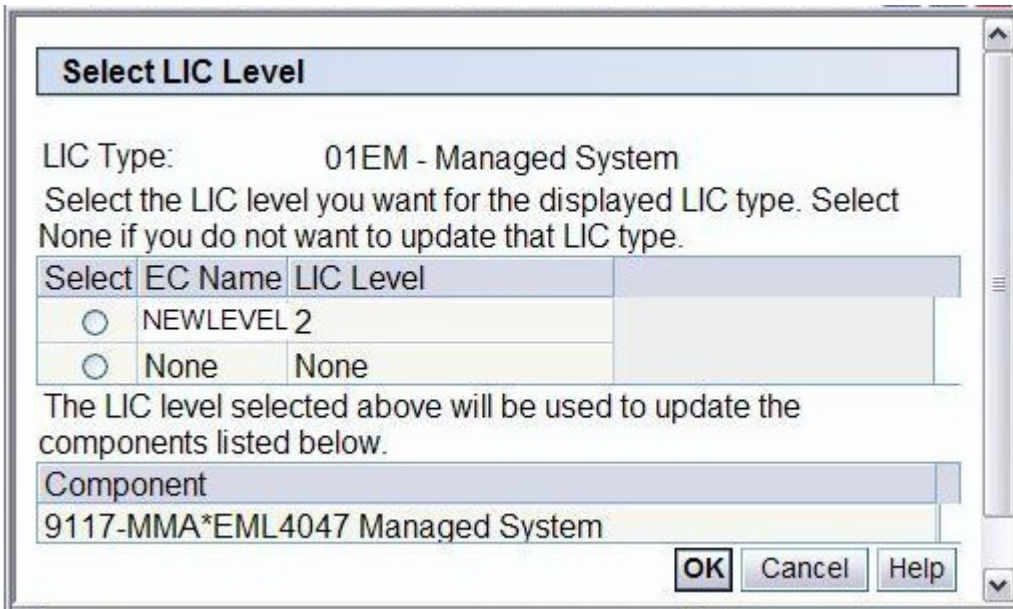
1. Under **System Management**, choose **Updates**.
2. Select **Upgrade Licensed Internal Code to a New Release**.
3. A **System readiness check** is automatically performed to check that the system is in the right state for LIC upgrade to a new release. In this example, the readiness check reports that there are no errors preventing the upgrade action:



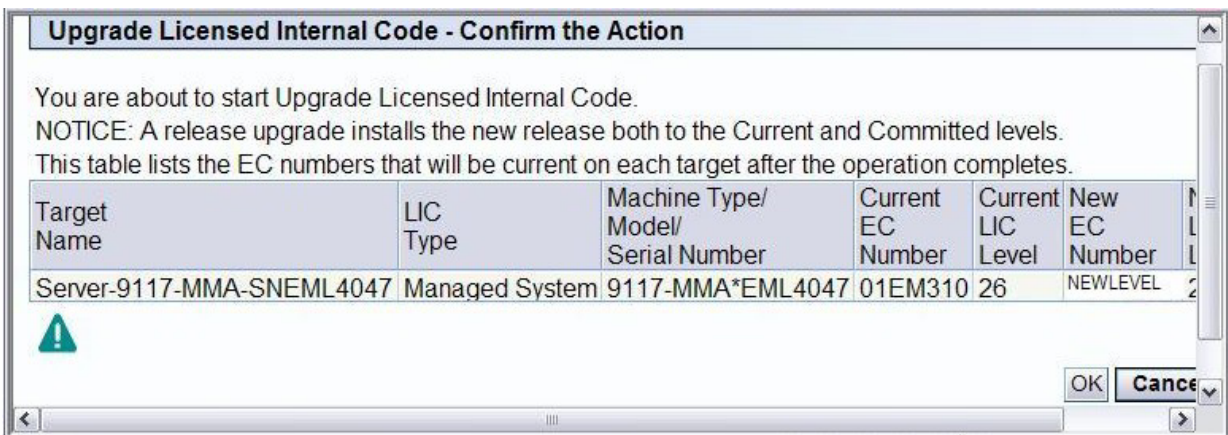
4. Since the new release in this example is located in an FTP directory on another system, choose **FTP site** for the repository.
5. Enter the **FTP site**, **User ID**, **Password**, and the **Directory** on the system where the new release is located:



6. From the **Select LIC Level** panel, we select **NEWLEVEL** and **OK** to confirm the level desired:

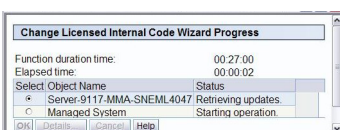


7. **Accept** the License Agreement.
8. Confirm the installation:

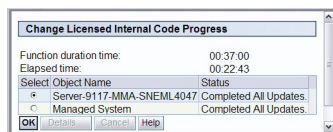


The **Current EC Number** is 01EM310. This is the release currently running on the managed system. The **Current LIC Level** is 26. The **New EC Number** is NEWLEVEL. This is the release that will be installed. After the installation, the LIC running on the t-side (temporary side) of the Flexible Service Processor and the LIC installed on the p-side (permanent side) of the Flexible Service Processor will be the NEWLEVEL release. Both the **Activated** and **Accepted** levels of LIC will be at the same level as the new release.

9. Select **OK** to upgrade the managed system to the new release. A progress panel is displayed as the upgrade is installed:



Until the update completes:



## Flash Side Selection

Use this task to select which flash side will be active after the next activation.

**Note:** This task is intended for Service User mode only.

**Attention:** If you select p-side for the next activation, this action disables concurrent Licensed Internal Code (LIC) update.

The flash side is the nonvolatile storage location in the flexible service processor (FSP), divided into t-side (temporary side) and p-side (permanent side), allowing for storing two levels of code. When the p-side is selected, concurrent LIC update is disabled.

Related HMC CLI commands:

- “lslic” on page 199
- “updlic” on page 238

## Check system readiness

Use this task to confirm that the managed system is in the correct state to perform a Licensed Internal Code update or upgrade successfully.

Before updating or upgrading Licensed internal code, all managed systems to be updated must be in Operating, Standby, Power Off, or Recovery state. All Flexible Service Processors (FSP) for the managed system must be properly connected to the HMC. Any problems found during the check will be reported to you to correct before updating LIC. A readiness check will automatically be performed before any update or upgrade begins.

Related HMC CLI commands:

- “lslic” on page 199
- “updlic” on page 238

## View system information

Use this task to examine current LIC levels on the managed system, including installed, activated, and accepted levels. If a repository is selected, this task also displays retrievable levels available in a repository.

The **Installed** level of LIC is the level that will be activated and loaded into memory at the next system restart. The **Activated** level of LIC is the level that is activated and loaded into memory at this time. The **Accepted** level of LIC is a committed level of LIC that can be returned to, if necessary. This is the level of code on the p-side (permanent side). The **Unactivated Deferred** level of LIC is the latest unactivated level that contains deferred updates. A deferred update requires a system restart to activate.

**Concurrent LIC update status** indicates whether concurrent LIC update is enabled or disabled. A concurrent update can be installed and activated without rebooting any partitions or disrupting applications.

**Reason for disablement** indicates why concurrent LIC update is disabled. This might include:

- The permanent side is active
- A temporary LIC level is active

A concurrent LIC update can be installed and activated without rebooting partitions or disrupting applications.

Related HMC CLI commands:

- “lslic” on page 199
- “updlic” on page 238



---

## Appendix A. HMC tasks and user roles/IDs

This appendix lists the tasks you can perform using the Hardware Management Console (HMC) and the user roles/IDs that are associated with that task.

You can, however, create customized user profiles which would allow you to have unique user IDs and multiple user roles. The management of these user roles is performed by using the **Manage Task and Resource Roles** task. The **Manage User Profiles and Access** task provides the ability to define which user role is associated with each specific user ID.

Table 10 alphabetically lists the HMC Management and Service Management tasks and the corresponding user roles/IDs that can perform these tasks.

Table 11 on page 128 lists the Systems Management tasks that can be performed on managed objects and the corresponding user roles that can perform these tasks.

*Table 10. HMC Management and Service Management tasks and default user roles*

Tasks	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Backup HMC Data	X	X		X
Change Date and Time	X	X		X
Change Language and Locale	X	X	X	X
Change Network Settings	X	X		X
Change User Interface Settings	X	X	X	X
Change User Password	X	X	X	X
Create Serviceable Event		X		X
Create Welcome Text	X	X		
Format Media	X	X		X
Launch Guided Setup Wizard		X		
Launch Remote Hardware Management Console	X	X	X	X
Load Serviceable Events	X	X	X	X
Lock HMC Screen	X	X	X	X
Logoff or Disconnect	X	X	X	X
Manage Certificates		X		
Manage Connection Monitoring	X	X	X	X
Manage Customer Information	X	X		X
Manage Data Replication	X	X		
Manage Dumps	X	X		X
Manage eService Registration	X	X		
Manage Inbound Connectivity	X	X		X
Manage Outbound Connectivity	X	X		X
Manage POWER4 Service Agent	X	X		

Table 10. HMC Management and Service Management tasks and default user roles (continued)

Tasks	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Manage Remote Connections	X	X		X
Manage Remote Support Requests	X	X	X	X
Manage Serviceable Event Notification	X	X		X
Manage Serviceable Events		X		X
Manage Systems Call-Home	X	X		X
Manage Task and Resource Roles		X		
Manage User Profiles and Access		X		
Manage Users and Tasks	X	X	X	X
Open 5250 Console	X	X		X
Open Restricted Shell Terminal	X	X	X	X
Remote Command Execution	X	X		X
Remote Virtual Terminal	X	X		X
Remote Operation	X	X	X	X
Restore HMC Data	X	X		X
Save Upgrade Data	X	X		X
Schedule Operations	X	X		
Shut Down or Restart	X	X		X
Test Network Connectivity	X	X	X	X
Tip of the Day	X	X	X	X
Transmit Service Information	X	X		
View HMC Events	X	X		X
View Licenses	X	X	X	X
View Network Topology	X	X	X	X
View System Data		X		

Table 11. Systems Management tasks performed on managed objects and default user roles

Tasks	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Properties	X	X	X	X
Update Password	X	X		X
Change Default Profile	X	X		X
<b>Operations</b>				
Power On	X	X		X
Power Off	X	X		X
Activate	X	X		X
Restart	X	X		X



Table 11. Systems Management tasks performed on managed objects and default user roles (continued)

Tasks	User roles/IDs			
	Operator (hmcoperator)	Super Administrator (hmcsuperadmin)	Viewer (hmcviewer)	Service Representative (hmcservicerep)
Shut Down	X	X		X
LED Status: View System Attention LED	X	X	X	X
LED Status: Identify LED	X	X	X	X
LED Status: Test LED	X	X	X	X
Manage Attention LED	X	X	X	X
Schedule Operations	X	X		
Advanced System Management (ASM)	X	X		X
Utilization Data: Enable	X	X		X
Utilization Data: Disable	X	X		X
Utilization Data: View	X	X	X	X
Utilization Data: Refresh	X	X		X
Rebuild	X	X		
Change Password		X		

Configuration				
Create Logical Partition: AIX or Linux	X	X		
Create Logical Partition: VIO Server	X	X		
Create Logical Partition: i5/OS	X	X		
System Plans: Create		X		
System Plans: Deploy		X		
System Plans: Import		X		
System Plans: Export		X		
System Plans: Remove		X		
System Plans: View		X		
Manage Custom Groups	X	X		X
View Workload Management Groups	X	X	X	X
Partition Availability Priority	X	X		
Manage System Profiles	X	X	X	X
Manage Partition Data: Restore	X	X		
Manage Partition Data: Initialize	X	X		
Manage Partition Data: Backup	X	X		X
Manage Partition Data: Delete	X	X		
Save Current Configuration	X	X		X

Connections				
Service Processor Status	X	X	X	X
Reset or Remove Connections	X	X		X
Disconnect Another HMC		X		

Add Managed System	X	X		
<b>Hardware (Information)</b>				
Adapters: GX+	X	X	X	X
Adapters: Host Channel	X	X	X	X
Adapters: Host Ethernet	X	X	X	X
Adapters: Switch Network Interface	X	X	X	X
View RIO Topology	X	X	X	X
Virtual I/O Adapters	X	X	X	X
<b>Dynamic Logical Partitioning</b>				
Processor	X	X		X
Memory	X	X		X
Physical Adapters	X	X		X
Virtual Adapter	X	X		X
Host Ethernet	X	X		X

<b>Updates</b>				
Change Licensed Internal Code for the current release		X		X
Upgrade Licensed Internal Code to a new release		X		X
Flash Side Selection		X		X
Check system readiness		X		X
View system readiness		X		X
<b>Console Window</b>				
Open Terminal Window	X	X		X
Close Terminal Connection	X	X		X
Open Shared 5250 Console	X	X		X
Open Dedicated 5250 Console	X	X		X
<b>Serviceability</b>				
Manage Serviceable Events		X		X
Create Serviceable Event		X		X
Reference Code History	X	X	X	X
Control Panel Functions: (20) Type, Model, Feature		X		
Hardware: Add FRU		X		X
Hardware: Add Enclosure		X		X
Hardware: Exchange FRU		X		X
Hardware: Exchange Enclosure		X		X
Hardware: Remove FRU		X		X
Hardware: Remove Enclosure		X		X
Hardware: Power on/off I/O Unit		X		X
Manage Dumps	X	X		X
Collect VPD	X	X	X	X

Edit MTMS		X		
FSP Failover: Setup		X		
FSP Failover: Initiate		X		

Capacity on Demand (CoD)				
Enter CoD code		X		
View History Log	X	X	X	X
Processor: View Capacity Settings	X	X	X	X
Processor/CUoD: View Code Information	X	X	X	X
Processor/On/Off CoD: Manage		X		
Processor/On/Off CoD: View Capacity Settings	X	X	X	X
Processor/On/Off CoD: View Billing Information	X	X	X	X
Processor/On/Off CoD: View Code Information	X	X	X	X
Processor/Trial CoD: Stop		X		
Processor/Trial CoD: View Capacity Settings	X	X	X	X
Processor/Trial CoD: View Code Information	X	X	X	X
Processor/Reserve CoD: Manage		X		
Processor/Reserve CoD: View Capacity Settings	X	X	X	X
Processor/Reserve CoD: View Code Information	X	X	X	X
Processor/Reserve CoD: View Shared Processor Utilization	X		X	X
Advanced POWER Virtualization: Enter Activation Code		X		
Advanced POWER Virtualization: View History Log	X	X	X	X
Advanced POWER Virtualization: View Code Information	X	X	X	X
Enterprise Enablement: Enter Activation Code		X		
Enterprise Enablement: View History Log	X	X	X	X
Enterprise Enablement: View Code Information	X	X	X	X
Other Advanced Functions: Enter Activation Code		X		
Other Advanced Functions: View History Log	X	X	X	X
Other Advanced Functions: View Code Information	X	X	X	X



## Appendix B. Remote operations

Remote operations use the Graphical User Interface (GUI) used by a local Hardware Management Console (HMC) operator (see Figure 18) or the command line interface (CLI) on the HMC. You can perform operations remotely in the following ways:

- Use a remote HMC
- Use a Web browser to connect to a local HMC
- Use an HMC remote command line

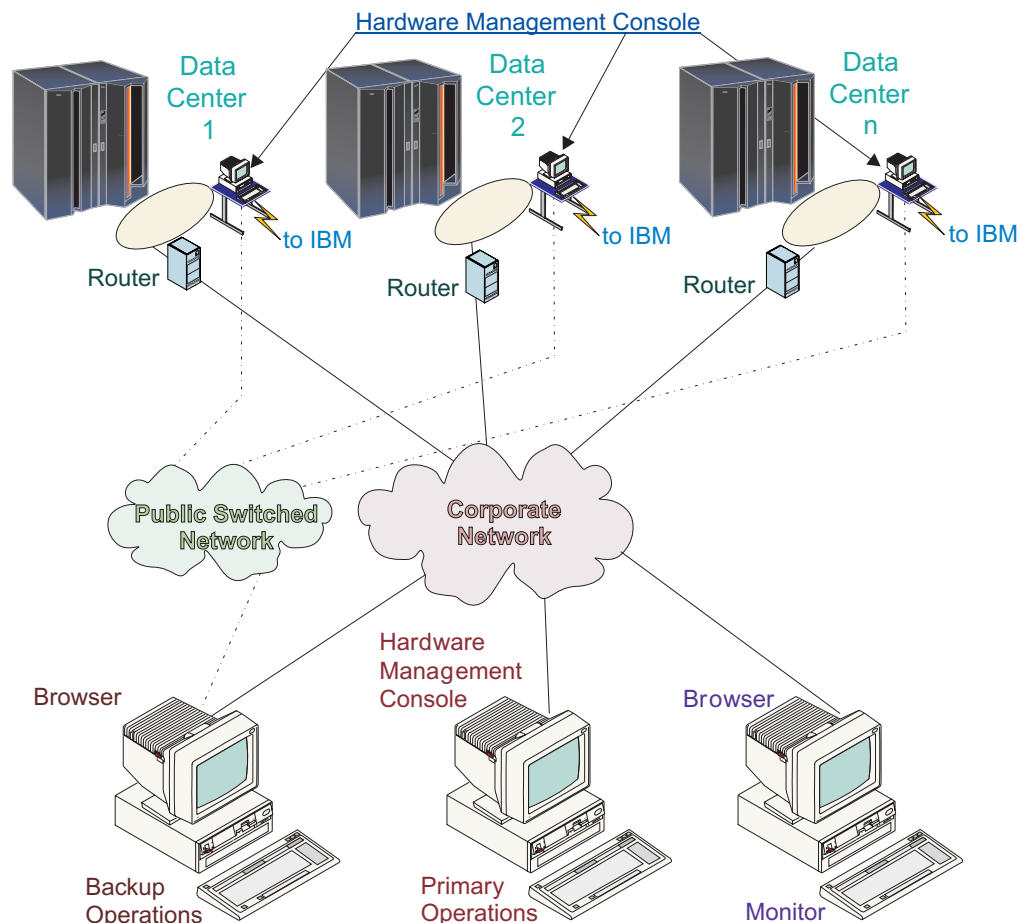


Figure 18. Remote Operation Configuration

The *remote HMC* is an HMC that is on a different subnet from the service processor, therefore the service processor cannot be autodiscovered with IP multicast.

To determine whether to use a remote HMC or Web browser connected to a local HMC, consider the scope of control that you need. A remote HMC defines a specific set of managed objects that are directly controlled by the remote HMC, while a Web browser to a local HMC has control over the same set of managed objects as the local HMC. The communications connectivity and communication speed is an additional consideration; LAN connectivity provides acceptable communications for either a remote HMC or Web browser control.

---

## Using a remote HMC

A remote HMC gives the most complete set of functions because it is a complete HMC; only the process of configuring the managed objects is different from a local HMC.

As a complete HMC, a remote HMC has the same setup and maintenance requirements as a local Hardware Management Console. A remote HMC needs LAN TCP/IP connectivity to each managed object (service processor) that is to be managed; therefore, any customer firewall that may exist between the remote HMC and its managed objects must permit HMC to service processor communications to occur. A remote HMC may also need communication with another HMC for service and support. Table 12 shows the ports a remote HMC uses for communications.

*Table 12. Ports used by a Remote HMC for Communications*

Port	Use
udp 9900	HMC to HMC discovery
tcp 9920	HMC to HMC commands

A remote HMC needs connectivity to IBM (or another HMC that has connectivity to IBM) for service and support. The connectivity to IBM may be in the form of access to the internet (through a company firewall), or a dialed connection through a customer-provided switched phone connection using the supplied modem (see “Manage Outbound Connectivity” on page 110). A remote HMC cannot use the supplied modem for communication with a local HMC or a service processor.

Performance (that is, time to perform an operation) and the availability of the status information and access to the control functions of the service processor depends on the reliability, availability, and responsiveness of the customer network that interconnects the remote HMC with the managed object. A remote HMC monitors the connection to each service processor and attempts to recover any lost connections and can report those connections that cannot be recovered.

Security for a remote HMC is provided by the HMC user-login procedures in the same way as a local HMC. As with a local HMC, all communication between a remote HMC and each service processor is encrypted. Certificates for secure communications are provided, and can be changed by the user if desired (see “Manage Certificates” on page 98).

TCP/IP access to the remote HMC is controlled through its internally managed firewall and is limited to HMC related functions.

---

## Using a Web browser

If you need occasional monitoring and control of managed objects connected to a single local HMC, use a Web browser. An example of using the Web browser might be an off-hours monitor from home by an operator or system programmer.

Each HMC contains a Web server that can be configured to allow remote access for a specified set of users. If a customer firewall exists between the Web browser and the local HMC, then the ports need to be accessible and the firewall should allow incoming requests on these ports. Table 13 shows the ports a Web browser needs for communication to an HMC.

*Table 13. Ports used by a Web browser for communications to the HMC*

Port	Use
tcp 443	Secure browser access to Web server communication
tcp 8443	Secure browser access to Web server communication
tcp 9960	Browser applet communication

After an HMC has been configured to allow Web browser access, a Web browser gives an enabled user access to all the configured functions of a local HMC, except those functions that require physical access to the HMC such as those that use the local diskette or DVD media. The user interface presented to the remote Web browser user is the same as that of the local HMC and is subject to the same constraints as the local HMC.

The Web browser can be connected to the local HMC using a LAN TCP/IP connection and using only encrypted (HTTPS) protocols. Logon security for a Web browser is provided by the HMC user-login procedures. Certificates for secure communications are provided, and can be changed by the user (see “Manage Certificates” on page 98).

Performance (that is, time to perform an operation) and the availability of the status information and access to the control functions of the managed objects depends on the reliability, availability, and responsiveness of the network that interconnects the Web browser with the local HMC. Because there is no direct connection between the Web browser and the individual managed objects, the Web browser does not monitor the connection to each service processor, does not do any recovery, and does not report any lost connections. These functions are handled by the local HMC.

The Web browser system does not require connectivity to IBM for service or support and maintenance of the browser and system level is the responsibility of the customer.

If the URL of the HMC is specified using the format `https://xxx.xxx.xxx.xxx` (where `xxx.xxx.xxx.xxx` is the IP address) and Microsoft Internet Explorer is used as the browser, a hostname mismatch message is displayed. To avoid this message, a Firefox browser is used or a hostname is configured for the HMC, using the **Change Network Settings** task (see “Change Network Settings” on page 94), and this hostname is specified in the URL instead of an IP address. Namely, using the format `https://hostname.domain_name` or `https://hostname` (for example, using `https://hmc1.ibm.com` or `https://hmc1`).

---

## Using the HMC remote command line

An alternative to performing HMC tasks is using the command line interface (CLI).

From a local HMC, the interface is available by right-clicking on the desktop (outside of the HMC web user interface screen), click **Terminals** and **rshlogin**. A restricted shell command line window is displayed. You can also open the **Open Restricted Shell Terminal** task from the HMC Management work pane.

You can use the command line interface in the following situations:

- When consistent results are required. If you have to administer several managed systems, you can achieve consistent results by using the command line interface. The command sequence can be stored in scripts and run remotely.
- When automated operations are required. After you have developed a consistent way to manage the managed systems, you can automate the operations by invoking the scripts from batch-processing applications, such as the **cron** daemon, from other systems.

## Setting up secure script execution between SSH clients and the HMC

HMCs typically are placed inside the machine room where managed systems are located, so you might not have physical access to the HMC. In this case, you can remotely access it using either the remote client or the remote command line interface. You must ensure that your script executions between SSH clients and the HMC are secure.

**Note:** To enable scripts to run unattended between an **SSH** client and an HMC, the SSH protocol must already be installed on the client’s operating system.

To enable scripts to run unattended between an **SSH** client and an HMC, do the following:

1. Open the **Remote Command Execution** task from the HMC Management work pane.
2. From the **Remote Command Execution** window, select **Enable remote command execution using the ssh facility**.
3. Create an HMC user with one of the following roles:
  - Super administrator (hmcsuperadmin)
  - Service representative (hmcservicerep)
4. On the client's operating system, run the SSH protocol key generator. To run the SSH protocol key generator, do the following:
  - a. To store the keys, create a directory named `$HOME/.ssh` (either RSA or DSA keys can be used).
  - b. To generate public and private keys, run the following command:

```
ssh-keygen -t rsa
```

The following files are created in the `$HOME/.ssh` directory:

```
private key: id_rsa
public key: id_rsa.pub
```

The write bits for both group and other are turned off. Ensure that the private key has a permission of 600.

5. On the client's operating system, use `ssh` and run the **mkauthkeys** command to update the HMC user's `authorized_keys2` file on the HMC by using the following command:

```
ssh userid@hostname "mkauthkeys -add '<the key string from $HOME/.ssh/id_dsa
```

You can use the following procedure to delete the key from the HMC by modifying various files:

1. On the logical partition, use the **scp** command to copy the `authorized_keys2` file from the HMC to the logical partition, as follows:

```
scp userid@host_name :.ssh/authorized_keys2 /tmp/mykeyfile
```
2. In the `/tmp/mykeyfile` file, remove the line that contains the key and host name of the system that you want to be able to run HMC commands remotely.
3. On a logical partition, use the **scp** command to copy the new file to the HMC:

```
scp /tmp/mykeyfile userid@host_name ".ssh/authorized_keys2"
```
4. If you want to enable password prompting for all hosts that access the HMC through **ssh**, use the **ssh** command to remove the key file from the HMC:

```
scp userid@hostname:.ssh/authorized_keys2 authorized_keys2
```
5. Edit the `authorized_keys2` file and remove all lines in this file, then copy it back to the HMC. For example:

```
scp authorized_keys joe@somehost:.ssh/authorized_keys2
```

You can also use the command line to delete the key from the HMC by using the **mkauthkeys** command. For example:

```
ssh userid@hostname "mkauthkeys --remove 'joe@somehost'"
```

## Enabling and disabling HMC remote commands

You can enable or disable the remote command line interface access to the HMC by using the SSH facility.

To enable or disable remote commands, you must have a user ID with one of the following roles:

- Super administrator
- Service representative

To enable or disable remote commands, do the following:

1. Open the **Remote Command Execution** task from the HMC Management work pane.



2. From the **Remote Command Execution** window:
  - To enable remote commands, select **Enable remote command execution using the ssh facility**.
  - To disable remote commands, make sure **Enable remote command execution using the ssh facility** is not selected.
3. Click **OK** to proceed.

---

## Web browser requirements

HMC Web browser support requires HTML 2.0, JavaScript 1.0, Java Virtual Machine (JVM), and cookie support in browsers that will connect to the HMC. Contact your support personnel to assist you in determining if your browser is configured with a Java Virtual Machine. The Web browser must use the HTTP 1.1 protocol; and if you are using a proxy server, the HTTP 1.1 protocol must be enabled for the proxy connections. Additionally, pop-ups must be enabled for all HMCs addressed in the browser if running with pop-ups disabled. The following browsers have been tested:

### Microsoft Internet Explorer 6.0 or later

If the Microsoft Internet Explorer browser is configured to use an internet proxy, then include local intranet addresses in the exception list. Consult your network administrator for more information. If you still need to use the proxy, access the HMC then enable **Use HTTP 1.1 through proxy connections** under the **Advanced** tab in your **Internet Options** window.

### Firefox 1.5.0.6 or later

For Firefox 2.0 make sure the JavaScript option to raise or lower windows and move or resize existing windows is enabled. To enable this option, go to the **Content** tab in the browser's **Options** dialog, click **Advanced...** next to the **Enable JavaScript** option, then select **Raise or lower windows** and **Move or resize existing windows** options, then click **OK** to enable. These features allow you to switch easily between HMC tasks and to resize the task window.

---

## Preparing to use the Web browser

Before you can use a Web browser to access an HMC, you must:

- Configure the HMC to allow remote control for specified users.
- For LAN-based connections, know the TCP/IP address of the HMC to be controlled, and have correctly set up any firewall access between the HMC and the Web browser.
- Have a valid user ID and password assigned by the access administrator for HMC Web access.

---

## Logging on the HMC from a LAN connected Web browser

Use the following steps to log in to the HMC from a LAN connected Web browser:

1. Ensure that your Web browser PC has LAN connectivity to the desired HMC.
2. From your Web browser, enter the URL of the desired HMC, using the format **https://hostname.domain\_name** (for example: **https://hmc1.ibm.com**) or **https://xxx.xxx.xxx.xxx**.

If this is the first access of the HMC for the current Web browser session you can receive a certificate error. This certificate error is displayed if:

- The Web server contained in the HMC is configured to use a self-signed certificate and the browser has not been configured to trust the HMC as an issuer of certificates, or
- The HMC is configured to use a certificate signed by a Certificate Authority (CA) and the browser has not been configured to trust this CA.

In either case, if you know that the certificate being displayed to the browser is the one used by the HMC, you can continue and all communications to the HMC will be encrypted.

If you do not want to receive notification of a certificate error for the first access of any browser session, you can configure the browser to trust the HMC or the CA. In general, to configure the browser:

- You must indicate that the browser will permanently trust the issuer of the certificate, or
- By viewing the certificate and installing, to the database of trusted CAs, the certificate of the CA that issued the certificate used by the HMC.

If the certificate is self-signed, the HMC itself is considered the CA that issued the certificate.

3. When prompted, enter the user name and password assigned by your administrator.

---

## Appendix C. Customizable data replication

The Customizable Data Replication service provides the ability to configure a set of Hardware Management Consoles (HMCs) to automatically replicate any changes to certain types of data so that the configured set of HMCs automatically keep this data synchronized without manual intervention.

**Note:** Before enabling this replication service, you may want to save your original data settings in case you need to restore these settings at a future time. See “Save Upgrade Data” on page 103.

The following types of data can be configured:

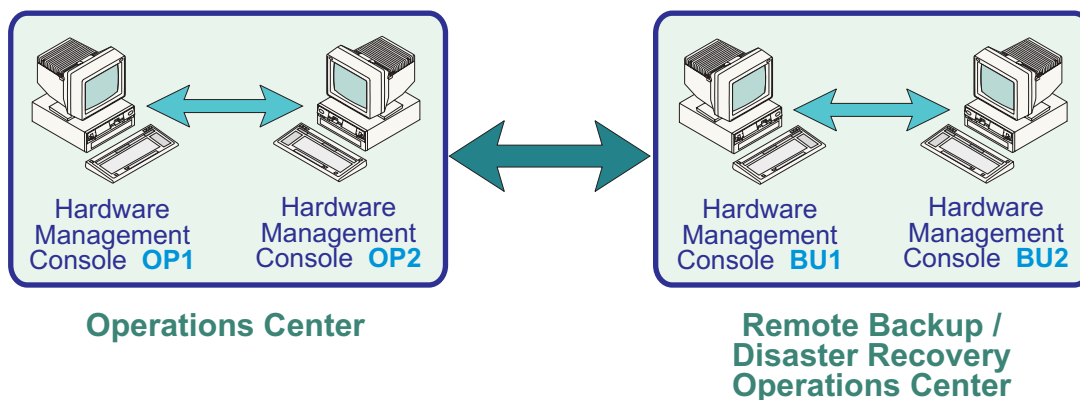
- Customer information data
  - Administrator information (customer name, address, telephone number, etc.)
  - System information (administrator name, address, telephone of your system)
  - Account information (customer number, enterprise number, sales branch office, etc.)
- Group data
  - All user-defined group definitions.
- Modem configuration data
  - Configure modem for remote support.
- Outbound connectivity data
  - Configure local modem to RSF
  - Enable an internet connection
  - Configure to an external time source

The Customizable Data Replication service can be enabled for the following types of operations:

- **Peer-to-Peer** (see “Peer-to-Peer replication”).  
Provides automatic replication of the selected customized data types between peer HMCs. Changes made on any of these consoles are replicated to the other consoles.
- **Master-to-Slave** (see “Master-to-Slave replication” on page 141).  
Provides automatic replication of the selected customized data types from one or more designated master HMCs to one or more designated slave HMCs. Changes made on a master(s) console are automatically replicated to the slave console(s).

---

### Peer-to-Peer replication



1. Log in the HMC using a user ID that has administrator roles.

2. Open the **Manage Data Replication** task from the HMC Management work pane. The **Manage Data Replication** window is displayed.
3. Select **Enable** in the **Customizable Data Replication** box.
4. The **Manage Data Replication** window is displayed.
5. Click **New** under **Data Source(s)**. The **Manage Data Replication** window is displayed.
6. Select a *Hardware Management Console* to be used as a data source from the **Discovered Console Information** list, and click **Add**.  
or  
Enter the *TCP/IP address* of the Hardware Management Console to be a used as a data source in the **TCP/IP Address Information** field, and then click **Find**.
7. The **Manage Data Replication** window redisplay as shown in

**Manage Data Replication**

Customizable Data Replication

☒ Enable ☐ Disable

Data Source(s)

endDefiant1

New

Delete

Customizable Data Types

Select	Data Types
<input type="checkbox"/>	Customer Information Data
<input checked="" type="checkbox"/>	Group Data
<input checked="" type="checkbox"/>	Modem Configuration Data
<input type="checkbox"/>	Outbound Connectivity Data

Local Customizable Data Change Warnings

Select the customizable data types that should generate warnings when that type of data is manually changed on this Hardware Management Console and are also configured to be replicated from one or more data sources.

Select	Data Warning Types
<input type="checkbox"/>	Customer Information Data
<input type="checkbox"/>	Group Data
<input type="checkbox"/>	Modem Configuration Data
<input type="checkbox"/>	Outbound Connectivity Data

Save Push to Slaves Sync from Master Status Cancel Help

Figure 19. Configure customizable data replication window - example 1

8. Select the types of data from the **Customizable Data Types** list that you want to replicate from a peer HMC currently selected under **Data Source(s)**.
9. Choose one of the following actions:
  - Click **Save** to close the Manage Data Replication window.
  - Click **Push to Slaves** to transfer all local levels to any communicating slave. The slaves, if they are running this level of code, are instructed to accept the levels from the master, regardless of the value of their current levels.
  - Click **Sync from Master** to invalidate the local levels for all properties that are defined to have a master. This results in an immediate level set where the master(s) provide their levels to the local machine. This option is not available if the local HMC is not defined to have any data sources.
  - Click **Status** to show the status of this task on this machine.
10. Repeat steps 1 through 9 on each of the HMCs you want to act as peers with one another.

11. Once communication is established between the HMCs, the requested types of customizable data are automatically replicated from one HMC to the other immediately following the change in the data itself.

---

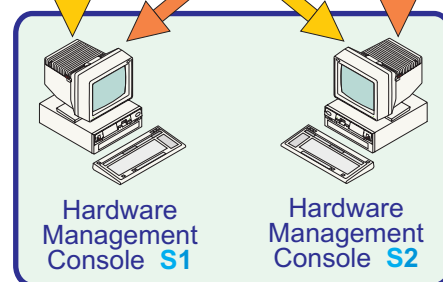
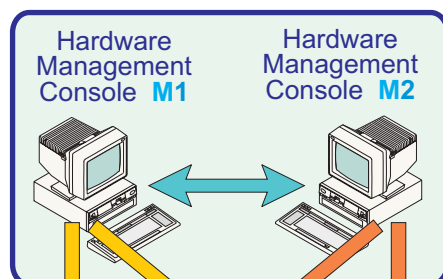
## Master-to-Slave replication

### Operations Center



### Machine Room

### Operations Center



### Machine Room

Setting up a Master Console(s):

1. Log in the HMC using a user ID that has administrator roles.
2. Open the **Manage Data Replication** task from the HMC Management work pane. The **Manage Data Replication** window is displayed.
3. Select **Enable** in the **Customizable Data Replication** box, then click **Save**.

**Note:** If you want to configure additional master consoles, see “Peer-to-Peer replication” on page 139

Setting up the Slave Console(s):

1. Log in the HMC using a user ID that has administrator roles.
2. Open the **Manage Data Replication** task. The **Manage Data Replication** window is displayed.
3. Select **Enable** in the **Customizable Data Replication** box.
4. The **Manage Data Replication** window is displayed.
5. Click **New** under **Data Source(s)**. The **Manage Data Replication** window is displayed.
6. Select a *Hardware Management Console* to be used as a master data source from the **Discovered Console Information** list, then click **Add**.  
or  
Enter the *TCP/IP address* of the HMC to be a used as the master data source in the **TCP/IP Address Information** field, then click **Find**.
7. The **Manage Data Replication** window redisplay as shown in

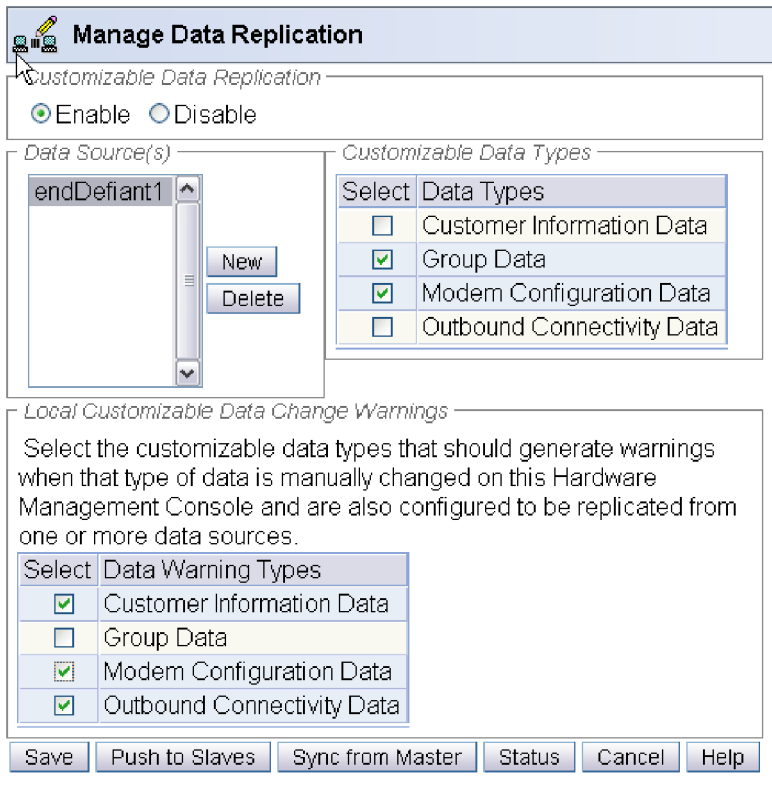


Figure 20. Configure customizable data replication window - example 2

8. Select the types of data from the **Customizable Data Types** list that you want to accept from the HMC currently selected under **Data Source(s)**.

**Note:** When configuring a HMC as a slave, you should check the types of customizable data from the **Local Customizable Data Change Warnings** list that should generate warnings to a user when manual changes are made to that data on this HMC.

9. Choose one of the following actions:
  - Click **Save** to close the Manage Data Replication window.
  - Click **Push to Slaves** to transfer all local levels to any communicating slave. The slaves, if they are running this level of code, are instructed to accept the levels from the master, regardless of the value of their current levels.
  - Click **Sync from Master** to invalidate the local levels for all properties that are defined to have a master. This results in an immediate level set where the master(s) provide their levels to the local machine. This option is not available if the local Hardware Management Console is not defined to have any data sources.
  - Click **Status** to show the status of this task on this machine.
10. Repeat **steps 1** through **9** on any additional HMCs that you want to configure as a slave.
11. Once communication is established between all of the HMCs, the master console(s) remains synchronized with each other, providing redundancy in the event that one of the master consoles becomes unavailable. The slave console(s) are kept synchronized with whichever master console provides the data to them first.

---

## Data replication

As data is replicated from one Hardware Management Console to another, an internal level indicator for the data being replicated is incremented each time the data is altered on the data source. Each Hardware Management Console keeps track of the level indicator for each type of data and will not accept data from a data source when the level indicator is not greater than that on the receiving Hardware Management Console.

If for some reason there is a need to force the replication of data from one or more data sources and the level indicator on the receiving Hardware Management Console is greater than that of the data sources, do the following:

1. Log in the HMC using a user ID that has administrator roles.
2. Open the **Manage Data Replication** task from the HMC Management work pane. The **Manage Data Replication** window is displayed (**Enable** should be selected).
3. Deselect all the data types from the **Customizable Data Types** list on the **Manage Data Replication** window.

**Note:** If you just want to reset the level indicator for a particular data type, just deselect that data type.

4. Click **Save** to remember the changes and to close the **Manage Data Replication** window.
5. Start the **Manage Data Replication** task again by repeating **step 2**.
6. Select the types of data from the **Customizable Data Types** list that were just deselected in **step 3**.
7. Click **Save** to remember the changes and to close the **Manage Data Replication** window.

**Note:** Deselecting and then reselecting the data types resets the internal level indicators for the specified types of data and forces replication of the data from the data sources.





---

## Appendix D. HMC commands

This appendix alphabetically describes the HMC commands you can use to perform tasks on the HMC. This information, including examples, is available from the HMC command line using the **man** command. You can also refer to the *Command Line Support* education module (<http://www.ibm.com/servers/resourcelink/lib03030.nsf/page>) and “Using the HMC remote command line” on page 135 for more information.

To view the command information, type **man** and then the command name. For example, to learn more about the “Create a user for the HMC” (**mkhmcusr**) command, type the following at the command line:

```
man mkhmcusr
```

---

### asmmenu

Provides access to Advanced System Management menu.

#### Synopsis

```
asmmenu --ip <IP address of system> [--help]
```

#### Description

**asmmenu** provides access to the Advanced System Management menu. This command takes the IP address or host name of the managed system and launches the Advanced System Management menu using the browser on the Hardware Management Console (HMC).

#### Options

**--ip** The IP address or host name of the managed system.

**--help** Display the help text for this command and exit.

---

### bkconsdata

Back up console data.

#### Synopsis

```
bkconsdata -r {dvd | ftp | nfs | none} [-h host-name] [-u user-ID] [--passwd password] [-l mount-resource-location] [-o "mount-command-options"] [-d remote-directory] [--help]
```

#### Description

**bkconsdata** backs up critical Hardware Management Console (HMC) data, which is HMC data that is stored on the HMC hard disk. This backup data may be used to restore the HMC if the HMC needs to be reinstalled from the HMC recovery CDs in the event of an HMC hard disk failure.

#### Options

**-r** The archive option for the backup data. Valid values are **dvd** for the DVD drive on the HMC, **ftp** for a remote FTP site, **nfs** for an NFS mounted remote file system, or **none**. The **none** option is used to remove the backup task lock allowing this task to be re-executed immediately.

**-h** The host name or IP address of the remote FTP or NFS server.

This option is required when backing up the data to a remote FTP site or NFS file system. Otherwise, this option is not valid.

**-u** The user ID to use to log in to the remote FTP site.

This option is required when backing up the data to a remote FTP site. Otherwise, this option is not valid.

**--passwd**

The password to use to log in to the remote FTP site. If this option is omitted, you will be prompted to enter the password.

This option is only valid when backing up the data to a remote FTP site.

**-l** The mount resource location defined on the NFS server where the backup data will be written.

This option is required when backing up the data to a remote NFS file system. Otherwise, this option is not valid.

**-o** Options to be passed to the mount command used to mount the remote NFS file system where the backup data will be written. The options must be enclosed in double quotes.

This option is only valid when backing up the data to a remote NFS file system.

**-d** The directory on the remote FTP or NFS server to which to write the backup data. If this option is not specified when backing up the data to a remote FTP site, the backup data will be written to the user's home directory. If this option is not specified when backing up the data to a remote NFS file system, the backup data will be written to the mount-resource-location on the NFS server.

This option is only valid when backing up the data to a remote FTP site or NFS file system.

**--help** Display the help text for this command and exit.

---

## bkprofdata

Back up profile data.

### Synopsis

**bkprofdata -m** *managed-system* **-f** *file* [**--force**] [**--help**]

### Description

**bkprofdata** backs up profile data for the *managed-system*.

The **rstprofdata** command can be used to restore profile data for the *managed-system*.

The **rmprofdata** command can be used to remove a profile data backup file.

### Options

**-m** The name of the managed system for which to back up profile data. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.

**-f** The name of the backup file where the profile data is to be written. If *file* is not fully qualified, *file* will be written to the **/var/hsc/profiles/serial-number** directory on the HMC (*serial-number* is the serial number of the managed system).

If *file* already exists, this command will fail unless the **--force** option is specified.

To back up the profile data to removable media, the media must be present in the removable media device and the device must be mounted with the **mount** command before this command is issued. The **lsmediadev** command can be used to display all of the removable media devices on the HMC.

- force** This option allows the specified backup file to be overwritten if it already exists. If the specified backup file already exists and this option is not specified, the backup will fail.
- help** Display the help text for this command and exit.

---

## chaccfg

Change access control configuration.

### Synopsis

```
chaccfg -t {resourcerole | taskrole} {-f configuration-file | -i "configuration-data"} [--help]
```

### Description

**chaccfg** changes the configuration of an access control role.

### Options

- t** The type of access control role to change. Valid values are **resourcerole** for managed resource role and **taskrole** for task role.

- f** The name of the file containing the configuration data needed to change the access control role.

The configuration data consists of attribute name/value pairs, which are in comma separated value (CSV) format. These attribute name/value pairs form a configuration record. A line feed marks the end of a configuration record. There can only be one configuration record in the file.

The format of a configuration record is as follows:

```
attribute-name=value,attribute-name=value,...<LF>
```

Note that certain attributes accept a comma separated list of values, as follows:

```
"attribute-name=value,value,...",...<LF>
```

When a list of values is specified, the attribute name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a `'\'` character.

If `'+='` is used in the attribute name/value pair instead of `'='`, then the specified *value* is added to the existing value for the attribute if the attribute is numerical. If the attribute is a list, then the specified *value(s)* is added to the existing list.

If `'-='` is used in the attribute name/value pair instead of `'='`, then the specified *value* is subtracted from the existing value for the attribute if the attribute is numerical. If the attribute is a list, then the specified *value(s)* is deleted from the existing list.

The `'+='` and `'-='` operators can only be used when changing a managed resource role.

Attribute names for managed resource roles:

**name** name of the managed resource role to change (required)

**resources**

comma separated list of managed resource objects (required)

Attribute names for task roles:

**name** name of the task role to change (required)

**resources**

comma separated list of tasks (required)

The **-f** and the **-i** options are mutually exclusive.

**-i** This option allows you to enter configuration data on the command line, instead of using a file. Data entered on the command line must follow the same format as data in a file, and must be enclosed in double quotes.

The **-i** and the **-f** options are mutually exclusive.

**--help** Display the help text for this command and exit.

---

## chcod

Change Capacity on Demand.

### Synopsis

To enter a CoD code:

```
chcod -o e -m managed-system -k CoD-code [--help]
```

To activate or change On/Off CoD resources:

```
chcod -o a -m managed-system -c onoff -r {mem | proc} -q quantity-of-resources -d number-of-days [--help]
```

To activate or change Reserve CoD processors:

```
chcod -o a -m managed-system -c reserve -r proc-q quantity-of-processors [--help]
```

To deactivate all On/Off CoD, all Reserve CoD, or all Trial CoD resources:

```
chcod -o d -m managed-system -c {onoff | reserve | trial} -r {mem | proc} [--help]
```

### Description

**chcod** performs Capacity on Demand (CoD) operations on the *managed-system*.

**chcod** is used to enter a CoD code for the *managed-system*. It is also used to activate On/Off CoD and Reserve CoD resources, or to deactivate On/Off CoD, Reserve CoD, or Trial CoD resources. CoD resources are either memory or processors.

### Options

**-o** The CoD operation to perform. Valid values are **e** to enter a CoD code, **a** to activate or change On/Off CoD or Reserve CoD resources, and **d** to deactivate all On/Off CoD, all Reserve CoD, or all Trial CoD resources.

To change the number of On/Off CoD resources or days that are currently activated, specify an activate operation with this option, specify the total number of activated On/Off CoD resources that you want with the **-q** option, and specify the number of days that you want them for with the **-d** option. An activate operation is to be used regardless of whether the total number of activated On/Off CoD resources is being increased, decreased, or kept the same. A deactivate operation is to be used only when you no longer want to have any activated On/Off CoD resources.

To change the number of Reserve CoD processors that are currently activated, specify an activate operation with this option, and specify the total number of activated Reserve CoD processors that you want with the **-q** option. An activate operation is to be used regardless of whether the total number of activated Reserve CoD processors is being increased or decreased. A deactivate operation is to be used only when you no longer want to have any activated Reserve CoD processors.

**Note:** CUoD and Trial CoD resources are activated by entering CoD codes.

- m** The name of the managed system for which the CoD operation is to be performed. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- k** The CoD code (key) to enter. Letters may be entered in either upper case or lower case.
- c** The CoD type. Valid values are **onoff** for On/Off CoD, **reserve** for Reserve CoD, and **trial** for Trial CoD.
- r** The CoD resource type. Valid values are **mem** for memory and **proc** for processors.
- q** The quantity of On/Off CoD or Reserve CoD resources requested. The value specified must be a whole number which is greater than 0.  
  
When requesting On/Off CoD memory, the value specified must be in megabytes, and it must be a multiple of 1024 megabytes.
- d** The number of days for which the On/Off CoD resources are requested.
- help** Display the help text for this command and exit.

---

## chhmc

Change Hardware Management Console configuration information.

### Synopsis

To change remote access settings:

```
chhmc -c {ssh | xntp} -s {enable | disable} [--help]
```

To add or remove an entry in the syslog configuration file:

```
chhmc -c syslog -s {add | remove} {-a IP-address | -h host-name} [--help]
```

To add or remove an entry in the network time protocol configuration file:

```
chhmc -c xntp -s {add | remove} {-a IP-address | -h host-name} [--ntpversion 1 | 2] [-nm network-mask] [-i interface] [--help]
```

To configure whether keyboard mapping configuration will occur at the next reboot:

```
chhmc -c kbdcfg -s {enable | disable} [--help]
```

To configure the network as a startup device:

```
chhmc -c netboot -s {enable | disable} [--help]
```

To configure an alternate disk partition on HMC as a startup device:

**chhmc -c altdiskboot -s {enable | disable} --mode {install | upgrade} [--help]**

To permit or deny IP addresses from utilizing HMC services:

**chhmc -c {ssh | service} -s {add | remove} -a IP-address [-nm network-mask] [-i interface] [--help]**

If **-nm** is omitted, the default network mask will be **255.255.255.255**.

If **-i** is omitted, the rule will be applied to all interfaces.

To add or remove entries from the DNS server search order or the domain suffix search order:

**chhmc -c network -s {add | remove} [-ns DNS-server] [-ds domain-suffix] [--help]**

To change network settings for a specific network interface:

**chhmc -c network -s modify -i interface [-a IP-address] [-nm network-mask] [--lparcomm {on | off}] [--help]**

To change other network settings:

**chhmc -c network -s modify [-h host-name] [-d network-domain-name] [-g gateway] [--help]**

To change the locale for the HMC:

**chhmc -c locale -s modify -l locale [--help]**

To change the HMC date and time, or time zone:

**chhmc -c date -s modify [--datetime date-time] [--clock {local | utc}] [--timezone {time-zone | none}] [--help]**

## Description

**chhmc** changes Hardware Management Console (HMC) configuration information, such as remote access settings and network settings.

## Options

- c** The type of configuration to be modified. Valid values are **ssh**, **syslog**, **xntp**, **network**, **kbdcfg**, **netboot**, **altdiskboot**, **locale**, **service**, and **date**.
- s** The new state value of the configuration. Valid values are **enable**, **disable**, **add**, **modify**, and **remove**.
- i** The interface to configure, such as **eth0**.
- a** The network IP address.
- nm** The network mask.
- lparcomm** The LPAR communication setting for the network interface.
- d** The network domain name.
- h** The host name.
- g** The default gateway IP address.
- ns** The nameserver IP address to add or remove.

- ds**     The domain suffix to add or remove.
- ntpversion**  
The ntp version if the server is not at NTP version 3 and above.
- mode**  
The mode to use when startup from the alternate disk partition. Default value is **upgrade**. Valid values are **install** and **upgrade**.
- l**     The locale. For a list of all locales supported by the HMC, issue the **lshmc -L** command.  
  
For the new locale to take effect for the local HMC console, you must log off the console and log back on. For the new locale to take effect for the HMC command line, you must reboot the HMC.
- datetime**  
The new date and time to set on the HMC's clock. *date-time* must be specified using the following format:  
  
*MMDDhhmm[[CC]YY][.ss]*  
  
where *MM* is the month, *DD* is the day, *hh* is the hour in 24 hour format, *mm* is the minutes, *CC* is the century, *YY* is the year, and *ss* is the seconds.  
  
This option is required when the **--clock** option is specified.  
  
You must reboot the HMC after setting the date and time.
- clock**  
The BIOS clock type. Valid values are **local** and **utc**.
- timezone**  
The time zone to set for the HMC. *time-zone* must be specified in *continent/city* format. Specify **none** to remove the time zone setting.  
  
You must reboot the HMC after setting the time zone.
- help** Display the help text for this command and exit.

---

## chhmcusr

Change a Hardware Management Console user.

### Synopsis

```
chhmcusr -u user-name -t {assign | desc | name | passwd | pwage | taskrole} [-o {a | r}] [-r {resource | resourcerole}] [-v new-attribute-value] [--help]
```

### Description

**chhmcusr** changes an attribute of a Hardware Management Console (HMC) user.

### Options

- u**     The user name of the HMC user to change.
- t**     The user attribute to change. Valid values are **assign** for the user's access control managed resource object assignment or managed resource role assignment, **desc** for the user's description, **name** for the user's user name, **passwd** for the user's password, **pwage** for the number of days until the user's password expires, and **taskrole** for the user's access control task role.
- o**     The managed resource object or role assignment operation to perform. Valid values are **a** to add a managed resource object or role to the user and **r** to remove a managed resource object or role from the user.

This option is required when changing the user's managed resource object assignment or managed resource role assignment. This option is not valid when changing any other user attribute.

**-r** The type of access control assignment to change. Valid values are **resource** for managed resource object assignment and **resource** for managed resource role assignment.

This option is required when changing the user's managed resource object assignment or managed resource role assignment. This option is not valid when changing any other user attribute.

**-v** The new value for the attribute being changed. When changing the user's managed resource object assignment, specify the managed resource object to be added or removed.

When changing the user's managed resource role assignment, specify the managed resource role to be added or removed.

When changing the user's description, specify the new description with this option. The new description can be any string.

When changing the user's user name, specify the new user name with this option. The new user name must not be longer than 32 characters, and it must begin with a letter.

When changing the user's password, you can either specify the new password with this option, or you can omit this option and you will be prompted to enter the password. The new password must be at least 7 characters in length.

When changing the number of days until the user's password expires, specify the new number of days with this option.

When changing the user's access control task role, specify the new task role with this option. Valid values are **hmcsuperadmin**, **hmcoperator**, **hmcviewer**, **hmcpe**, **hmcservice**, or a user-defined task role.

This option is required when changing any user attribute other than the user's password.

**--help** Display the help text for this command and exit.

---

## chhwres

Change hardware resources.

### Synopsis

To add, remove, or move a physical I/O slot:

```
chhwres -r io -m managed-system -o {a | r | m} {-p partition-name | --id partition-ID} [{-t target-partition-name | --tid target-partition-ID} -l slot-DRC-index [-a "attributes"] [-w wait-time] [-d detail-level] [--force]
```

To set physical I/O attributes:

```
chhwres -r io -m managed-system -o s {-p partition-name | --id partition-ID} --subtype {iopool | taggedio} -a "attributes"
```

To add or remove a virtual I/O adapter:

```
chhwres -r virtualio -m managed-system -o {a | r} {-p partition-name | --id partition-ID} [--subtype {eth | scsi | serial}] [-s virtual-slot-number] [-a "attributes"] [-w wait-time] [-d detail-level] [--force]
```

To set virtual I/O attributes:



```
chhwres -r virtualio -m managed-system -o s [{-p partition-name | --id partition-ID}] --subtype {eth | hsl | virtualopti} -a "attributes"
```

To add, remove, or move memory:

```
chhwres -r mem -m managed-system -o {a | r | m} {-p partition-name | --id partition-ID} [{-t target-partition-name | --tid target-partition-ID}] -q quantity [-w wait-time] [-d detail-level] [--force]
```

To set memory attributes:

```
chhwres -r mem -m managed-system -o s -a "attributes"
```

To add, remove, or move processing resources:

```
chhwres -r proc -m managed-system -o {a | r | m} {-p partition-name | --id partition-ID} [{-t target-partition-name | --tid target-partition-ID}] [--procs quantity] [--procunits quantity] [--5250cpwpercent percentage] [-w wait-time] [-d detail-level] [--force]
```

To set processing attributes:

```
chhwres -r proc -m managed-system -o s {-p partition-name | --id partition-ID -a "attributes"
```

To add, remove, or move a Host Ethernet Adapter (HEA) logical port (POWER6 servers only):

```
chhwres -r hea -m managed-system -o {a | r | m} {-p partition-name | --id partition-ID} [{-t target-partition-name | --tid target-partition-ID}] -l HEA-adapter-ID [--physport physical-port-ID] -g port-group --logport logical-port-ID [-a "attributes"] [-w wait-time] [-d detail-level] [--force]
```

To set HEA attributes (POWER6 servers only):

```
chhwres -r hea -m managed-system -o s -l HEA-adapter-ID [--physport physical-port-ID] -g port-group -a "attributes"
```

## Description

**chhwres** changes the hardware resource configuration of the *managed-system*. **chhwres** is used to perform dynamic logical partitioning (DLPAR) operations.

## Options

**-r** The type of hardware resources to change. Valid values are **io** for physical I/O, **virtualio** for virtual I/O, **mem** for memory, **proc** for processing resources, and **hea** for Host Ethernet Adapter (HEA) resources.

HEA resources are only supported on POWER6 servers.

### --subtype

The subtype of hardware resources to change. Valid physical I/O resource subtypes are slot for I/O slots, **iopool** for I/O pools, and **taggedio** for tagged I/O resources. Valid virtual I/O resource subtypes are **eth** for virtual ethernet, **scsi** for virtual SCSI, **serial** for virtual serial, **hsl** for High Speed Link (HSL) OptiConnect, and **virtualopti** for virtual OptiConnect resources.

This option is required for physical I/O or virtual I/O set operations, and for virtual I/O add operations.

This option is not valid for memory, processor, or HEA operations.

**-o** The operation to perform. Valid values are **a** to add hardware resources to a partition, **r** to

remove hardware resources from a partition, **m** to move hardware resources from one partition to another, and **s** to set hardware resource related attributes for a partition, an HEA, or the managed-system.

- p** The name of the partition for which the operation is to be performed. For a move operation, this is the source partition (the partition the resources will be moved from) for the operation. To perform an add, remove, or move operation, the partition must be in the running state.
- You can either use this option to specify the name of the partition for which the operation is to be performed, or use the **--id** option to specify the partition's ID. The **-p** and the **--id** options are mutually exclusive.
- A partition is required to be specified with this option or the **--id** option for all operations except a virtual ethernet, memory, or HEA set operation.
- id** The ID of the partition for which the operation is to be performed. For a move operation, this is the source partition (the partition the resources will be moved from) for the operation. To perform an add, remove, or move operation, the partition must be in the running state.
- You can either use this option to specify the ID of the partition for which the operation is to be performed, or use the **-p** option to specify the partition's name. The **--id** and the **-p** options are mutually exclusive.
- A partition is required to be specified with this option or the **-p** option for all operations except a virtual ethernet, memory, or HEA set operation.
- t** The name of the target partition for a move operation. The partition must be in the running state.
- You can either use this option to specify the name of the target partition, or use the **--tid** option to specify the ID of the partition. The **-t** and the **--tid** options are mutually exclusive.
- A target partition is required to be specified with this option or the **--tid** option for a move operation. This option is not valid for any other operation.
- tid** The ID of the target partition for a move operation. The partition must be in the running state.
- You can either use this option to specify the ID of the target partition, or use the **-t** option to specify the name of the target partition. The **--tid** and the **-t** options are mutually exclusive.
- A target partition is required to be specified with this option or the **-t** option for a move operation. This option is not valid for any other operation.
- l** When adding, removing, or moving a physical I/O slot, use this option to specify the DRC index of the slot.
- When performing an HEA operation, use this option to specify the adapter ID of the HEA for which the operation is to be performed.
- This option is not valid for any other operation.
- s** The virtual slot number of the virtual I/O adapter to add or remove.
- When adding a virtual I/O adapter, if this option is not specified then the next available virtual slot number will be assigned to the virtual I/O adapter.
- When removing a virtual I/O adapter, this option is required.
- q** The quantity of memory to add, remove, or move. The *quantity* specified must be in megabytes, it must be a multiple of the memory region size for the *managed-system*, and it must be greater than 0.
- procs** When adding or removing processing resources to or from a partition using dedicated processors, or when moving processing resources from a partition using dedicated processors to another partition using dedicated processors, use this option to specify the quantity of dedicated processors to add, remove, or move.

When adding or removing processing resources to or from a partition using shared processors, or when moving processing resources from a partition using shared processors to another partition using shared processors, use this option to specify the quantity of virtual processors to add, remove, or move.

When moving processing resources from a partition using dedicated processors to a partition using shared processors, use this option to specify the quantity of dedicated processors to be moved from the source partition and added as shared processors to the target partition.

This option is not valid when moving processing resources from a partition using shared processors to a partition using dedicated processors. The **--procunits** option must be used instead.

The *quantity* of processing resources specified with this option must be a whole number greater than 0.

#### **--procunits**

When adding or removing processing resources to or from a partition using shared processors, or when moving processing resources from a partition using shared processors to another partition using shared processors, use this option to specify the quantity of processing units to add, remove, or move.

When moving processing resources from a partition using shared processors to a partition using dedicated processors, use this option to specify the quantity of shared processors to be moved from the source partition and added as dedicated processors to the target partition.

This option is not valid when moving processing resources from a partition using dedicated processors to a partition using shared processors. The **--procs** option must be used instead.

When moving processing resources from a partition using shared processors to a partition using dedicated processors, the *quantity* of processing units specified with this option must be a whole number. Otherwise, the *quantity* of processing units specified with this option can have up to 2 decimal places. In either case, the *quantity* specified must be greater than 0.

#### **--5250cpwpercent**

The percentage of 5250 Commercial Processing Workload (CPW) to add, remove, or move. The *percentage* specified can have up to 2 decimal places, and it must be greater than 0.

This option is only valid for i5/OS partitions and can only be used when the *managed-system* supports the assignment of 5250 CPW percentages to partitions.

#### **--physport**

The ID of the HEA physical port. This option is required when adding an HEA logical port to a partition. This option is also required when setting HEA physical port attributes. This option is not valid for any other operation.

- g** The HEA port group. This option is required for all HEA operations, and is not valid for any other operation.
- w** The elapsed time, in minutes, after which an add, remove, or move operation will be stopped. *wait-time* must be a whole number. If wait-time is 0, the operation will not be timed out.  
If this option is not specified, a default value of 5 minutes is used.  
This option is valid for all add, remove, and move operations for AIX, Linux, and virtual I/O server partitions. This option is also valid for memory add, remove, and move operations for i5/OS partitions.
- d** The level of detail to be displayed upon return of an add, remove, or move operation. Valid values are 0 (none) through 5 (highest).  
If this option is not specified, a default value of 0 is used.  
This option is valid for all add, remove, and move operations for AIX, Linux, and virtual I/O server partitions.

**--force** This option allows you to force a remove or move operation to be performed for a physical I/O slot that is currently in use (varied on) by an i5/OS partition.

This option also allows you to force an add, remove, or move operation to be performed for an AIX, Linux, or virtual I/O server partition that does not have an RMC connection to the HMC. If this command completes successfully, you will need to restart your operating system for the change to take affect. You should only use this option if you intentionally configured your LAN to isolate the HMC from the operating system of your partition.

**-a** The configuration data needed to create virtual I/O adapters or set hardware resource related attributes. The configuration data consists of attribute name/value pairs, which are in comma separated value (CSV) format. The configuration data must be enclosed in double quotes.

The format of the configuration data is as follows:

*attribute-name=value,attribute-name=value,...*

Note that certain attributes accept a comma separated list of values, as follows:

*"attribute-name=value,value,...",...*

When a list of values is specified, the attribute name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a `'\'` character.

If `'+='` is used in the attribute name/value pair instead of `'='`, then the specified *value* is added to the existing value for the attribute if the attribute is numerical. If the attribute is a list, then the specified *value(s)* is added to the existing list.

If `'-='` is used in the attribute name/value pair instead of `'='`, then the specified *value* is subtracted from the existing value for the attribute if the attribute is numerical. If the attribute is a list, then the specified *value(s)* is deleted from the existing list.

Valid attribute names for attributes that can be set when adding, removing, or moving a physical I/O slot:

**slot\_io\_pool\_id**

Valid attribute names for setting I/O pool attributes:

**lpar\_io\_pool\_ids**

comma separated

Valid attribute names for setting tagged I/O resources (i5/OS partitions only):

**load\_source\_slot**

DRC index of I/O slot, or virtual slot number

**alt\_restart\_device\_slot**

DRC index of I/O slot, or virtual slot number

**console\_slot**

DRC index of I/O slot, virtual slot number, or the value **hmc**

**alt\_console\_slot**

DRC index of I/O slot, or virtual slot number

**op\_console\_slot**

DRC index of I/O slot, or virtual slot number

Valid attribute names for adding a virtual ethernet adapter:

**ieee\_virtual\_eth**

Valid values:

**0** - not IEEE 802.1Q compatible

1 - IEEE 802.1Q compatible

Required

**port\_vlan\_id**

Required

**addl\_vlan\_ids**

**is\_trunk**

Valid values:

0 - no

1 - yes

**trunk\_priority**

Valid values are integers between 1 and 15, inclusive

Required for a trunk adapter

Valid attribute names for adding a virtual SCSI adapter:

**adapter\_type**

Valid values are client or server

Required

**remote\_lpar\_id** | **remote\_lpar\_name**

One of these attributes is required for a **client** adapter

**remote\_slot\_num**

Required for a **client** adapter

Valid attribute names for adding a virtual serial adapter:

**adapter\_type**

Valid values are **client** or **server**

Required

**remote\_lpar\_id** | **remote\_lpar\_name**

One of these attributes is required for a **client** adapter

**remote\_slot\_num**

Required for a **client** adapter

**supports\_hmc**

The only valid value is 0 for no.

Valid attribute names for setting virtual ethernet attributes:

**mac\_prefix**

Valid attribute names for setting HSL OptiConnect attributes (i5/OS partitions only):

**hsl\_pool\_id**

Valid values are:

0 - HSL OptiConnect is disabled

1 - HSL OptiConnect is enabled

Valid attribute names for setting virtual OptiConnect attributes (i5/OS partitions only):

**virtual\_opti\_pool\_id**

Valid values are:

0 - virtual OptiConnect is disabled

1 - virtual OptiConnect is enabled

Valid attribute names for setting memory attributes:

**requested\_num\_sys\_huge\_pages**

Valid attribute names for setting processing attributes:

**sharing\_mode**

Valid values for partitions using dedicated processors are:

**keep\_idle\_procs** - never share processors

**share\_idle\_procs** - share processors only when partition is inactive

**share\_idle\_procs\_active** - share processors only when partition is active (POWER6 servers only)

**share\_idle\_procs\_always** - always share processors (POWER6 servers only)

Valid values for partitions using shared processors are:

**cap** - capped

**uncap** - uncapped

**uncap\_weight**

Valid attribute names when adding an HEA logical port:

**vlan\_id\_list**

comma separated

**lhea\_capabilities**

Comma separated list of Logical Host Ethernet adapter (LHEA) capabilities, with each capability having one of the following formats:

*capability*

or

*5/ieq/nieq/qp/cq/mr*

where *ieq* (interruptible event queues), *niesq* (non-interruptible event queues), *qp* (queue pairs), *cq* (completion queues), and *mr* (memory regions) each specify the resource amount in addition to the base minimum.

Valid values for capability:

**0** - base minimum

**1** - low

**2** - medium

**3** - high

**4** - dedicated

For example:

**5/22/128/1021/1019/63424**

Valid attribute names for setting HEA physical port attributes:

**conn\_speed**

Valid values are:

**auto** - system selects automatically

**10** - 10 Mbps

**100** - 100 Mbps

**1000** - 1 Gbps

**10000** - 10 Gbps

**duplex**

Valid values are:

**auto** - system selects automatically

**full** - full duplex  
**max\_rcv\_packet\_size**  
Valid values are:  
    **1500** - 1500 bytes per frame (non-jumbo)  
    **9000** - 9000 bytes per frame (jumbo)  
**flow\_control**  
Valid values are:  
    **0** - disable flow control  
    **1** - enable flow control  
**promisc\_lpar\_name** | **promisc\_lpar\_id**

Valid attribute names for setting HEA port group attributes:

**pend\_port\_group\_mcs\_value**

**--help** Display the help text for this command and exit.

---

## chkmedia

Check media readiness.

### Synopsis

**chkmedia -r {dvd | diskette | usbdiskette | usbflashmem} [--help]**

### Description

**chkmedia** allows a user to test for media readiness on the Hardware Management Console (HMC). The media devices that can be tested for readiness are the DVD drive (DVD-RAM media only), the internal diskette drive, a USB diskette drive, and a USB flash memory device. In order to test for media readiness, a small amount of data is written to, read from, then deleted from the specified media. No other diagnostic actions are performed on the media or the media device.

### Options

**-r** The media device to be tested for readiness. Valid values are **dvd** for the internal DVD drive, **diskette** for the internal diskette drive, **usbdiskette** for an external diskette drive connected to the HMC with a USB cable, or **usbflashmem** for a flash memory device that is connected to a USB port on the HMC.

**--help** Display the help text for this command and exit.

---

## chled

Change LED.

### Synopsis

**chled -r sa -t {phys | virtualallpar | virtualsys} -m managed-system -o {on | off} [{-p partition-name | --id partition-ID}] [--help]**

### Description

**chled** changes the state of an LED on the *managed-system*.

### Options

**-r** The type of LED resource to change. The only valid value is **sa** for System Attention (SA) LED.



- t** The type of System Attention (SA) LED to change. Valid values are **phys** for the physical SA LED for the *managed-system*, **virtuallpar** for a virtual partition SA LED, or **virtualsys** for the virtual SA LED for the *managed-system*.
  - m** The name of the managed system on which to change the LED. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
  - o** The operation to perform on the LED. Valid values are **on** to activate the LED, and **off** to deactivate the LED.  
The value **on** is not valid when changing the physical SA LED for the *managed-system*.
  - p** The name of the partition for which the virtual partition SA LED is to be changed.  
To change a virtual partition SA LED, you must either use this option to specify the name of the partition for which the LED is to be changed, or use the **--id** option to specify the partition's ID. The **-p** and the **--id** options are mutually exclusive.  
This option is not valid when changing the physical SA LED or the virtual SA LED for the *managed-system*.
  - id** The ID of the partition for which the virtual partition SA LED is to be changed.  
To change a virtual partition SA LED, you must either use this option to specify the ID of the partition for which the LED is to be changed, or use the **-p** option to specify the partition's name. The **--id** and the **-p** options are mutually exclusive.  
This option is not valid when changing the physical SA LED or the virtual SA LED for the *managed-system*.
  - help** Display the help text for this command and exit.
- 

## chlpoutil

Change utilization data collection settings.

### Synopsis

**chlpoutil -r config [-m *managed-system*] -s *sample-rate* [--help]**

### Description

**chlpoutil** changes the Hardware Management Console (HMC) settings for utilization data collection for managed systems.

### Options

- r** The type of utilization data collection resources to change. The only valid value is **config** for configuration settings.
- m** The name of the managed system for which the settings for utilization data collection are to be changed. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name, or if the HMC does not currently have a connection to the managed system.  
If this option is not specified, then the HMC settings for utilization data collection for all of the systems currently managed by this HMC, and for all of the systems for which utilization data has



been previously collected by this HMC will be changed. Even though utilization data collection is enabled for a managed system, the HMC will only collect utilization data for that managed system if the HMC currently has a connection to that managed system.

This command only changes the settings for utilization data collection for this HMC. Utilization data collection by other HMCs for the same managed systems is not affected.

**-s** The rate, in seconds, at which to sample the utilization data. Sample rates of **0** and **3600** are the only valid values. A sample rate of **0** disables utilization data collection, and a sample rate of **3600** enables utilization data collection with hourly sampling.

**--help** Display the help text for this command and exit.

---

## chsfacfg

Change Service Agent configuration.

### Synopsis

To change customer email notification settings:

```
chsfacfg -t email -o {enable | disable | setsmtp | add | remove | test} [-a {email-address | all}] [--events {all | callhome}] [-h host-name] [-p port-number]
```

To change FTP firewall settings:

```
chsfacfg -t ftpfirewall [-o {add | remove}] [-h host-name] [-p port-number] [-u user-ID] [--passwd password] [--passive passive-mode] [--fwtype firewall-type] [-n name]
```

To change FTP offload server settings:

```
chsfacfg -t ftpoffload [-o {enable | disable}] [-h host-name] [-p port-number] [-u user-ID] [--passwd password] [--passive passive-mode] [-d directory]
```

To change SNMP trap configuration:

```
chsfacfg -t snmp -o {add | remove} -a {SNMP-address | all} [--events SNMP-trap-list]
```

### Description

**chsfacfg** changes the Service Agent configuration.

### Options

**-t** The type of Service Agent configuration information to change. Valid values are **email** for customer email notification settings, **ftpfirewall** for FTP firewall settings, **ftpoftload** for FTP offload server settings, and **snmp** for SNMP trap configuration..

**-o** The operation to perform. Valid values are:

**enable**

enable customer email notification or FTP offload of service information

**disable**

disable customer email notification or FTP offload of service information

**setsmtp**

set the SMTP server information for customer notification email

**add**     add a notification email address, add a name to the exclusion list for the FTP firewall server, or add an address for SNMP trap notifications

**remove**

Remove a notification email address, remove a name from the exclusion list for the FTP firewall server, or remove an address from the SNMP trap notification list

**test**     Send a test email to a notification email address.

**-a**     The email address to add, remove, or test for customer notification email or the SNMP address to add or remove for SNMP trap notifications. SNMP addresses are specified in the form *Community-Name@IP-Address*.

When performing a remove or test operation for a customer notification email address, **all** can be specified with this option instead of a specific email address. If **all** is specified, then the remove or test operation will be performed for all notification email addresses.

When performing a remove operation for an SNMP address, **all** can be specified with this option instead of a specific SNMP address. If **all** is specified, then the remove operation will be performed for all SNMP trap notification addresses.

This option is required when adding, removing, or testing a customer notification email address. This option is not valid for any other operation.

**--events**

When adding a customer email notification address, specify the type of problem events for which the email address is to be notified. Valid values are **all** for all problem events, and **callhome** for only call home problem events. If this option is not specified, then the email address will be notified for all problem events.

When adding an address for SNMP trap notifications, specify the list of SNMP traps for which the SNMP address is to be notified. If there is more than one SNMP trap, the SNMP traps must be separated by blanks. The defined SNMP traps can be listed by issuing the command **Issacfg -t snmptrapnames**.

This option is only valid when adding a customer email notification address or when adding an SNMP address for SNMP trap notifications.

**-h**     When enabling customer email notification or setting the SMTP server information for customer notification email, use this option to specify the host name or IP address of the SMTP server.

When changing the FTP firewall settings, use this option to specify the host name or IP address of the firewall server.

When changing the FTP offload server settings, use this option to specify the host name or IP address of the FTP offload server.

This option is required when setting the SMTP server information for customer notification email.

**-p**     When setting the SMTP server information for customer notification email, use this option to specify the port number to use on the SMTP server. The default port number for an SMTP server is 25.

When changing the FTP firewall settings, use this option to specify the port number to use on the firewall server.

When changing the FTP offload server settings, use this option to specify the port number to use on the FTP offload server.

The default port number for an FTP offload server or firewall server is 21.

**-u**     When changing the FTP firewall settings, use this option to specify the user ID to use to log in to the firewall server.

When changing the FTP offload server settings, use this option to specify the user ID to use to log in to the FTP offload server.

**--passwd**

When changing the FTP firewall settings, use this option to specify the password to use to log in to the firewall server. If this option is omitted, you will be prompted to enter the password.

When changing the FTP offload server settings, use this option to specify the password to use to log in to the FTP offload server. If this option is omitted, you will be prompted to enter the password.

**-d** The directory to use on the FTP offload server.

**--passive**

When changing the FTP firewall settings, use this option to specify the passive mode to use. Valid values are **on** for always use PASV, **off** for always use PORT, and **optional** for try PASV then PORT.

When changing the FTP offload server settings, use this option to specify the passive mode to use. Valid values are **on** for always use PASV and **off** for always use PORT.

**--fwtype**

The FTP firewall type to use when offloading service information. Valid values are:

**0** - do not use a firewall

**1** - connect to firewall server, but send "USER user@real.host.name"

**2** - connect to firewall server, log in with "USER fwuser" and "PASS fwpassword", and then "USER user@real.host.name"

**3** - connect to and log in to firewall server, and then use "SITE real.host.name" followed by "USER user" and "PASS password"

**4** - connect to and log in to firewall server, and then use "OPEN real.host.name" followed by "USER user" and "PASS password"

**5** - connect to firewall server, but send "USER user@fwuser@real.host.name" and "PASS pass@fwpass" to log in

**6** - connect to firewall server, but send "USER fwuser@real.host.name" and "PASS fwpass" followed by "USER user" and "PASS password" to complete the login

**7** - connect to firewall server, but send "USER user@real.host.name fwuser" and "PASS pass" followed by "ACCT fwpass" to complete the login

This option is only valid when changing the FTP firewall settings.

**-n** The host name or domain name to add to or remove from the exclusion list for the firewall server. The exclusion list is a list of domains or hosts where the firewall should not be used.

This option is required when adding or removing a name in the exclusion list for the FTP firewall server. This option is not valid for any other operation.

**--help** Display the help text for this command and exit.

---

## chsvcevent

Updates serviceable events on the HMC.

### Synopsis

**chsvcevent -o {close | closeall} [-p problem-number -h analyzing-HMC] [--help]**

### Description

**chsvcevent** closes serviceable events on the Hardware Management Console (HMC).

## Options

- o** The operation to perform. Valid values are **close** to close the serviceable event specified using the **-p** and **-h** options, and **closeall** to close all serviceable events on this HMC.
- p** The problem number of the serviceable event to close. This option is required when closing a single serviceable event. This option is not allowed when closing all serviceable events.  
The problem number can be obtained using the **lssvcevents** command.
- h** The analyzing HMC for the serviceable event to close. This option is required when closing a single serviceable event. This option is not allowed when closing all serviceable events.  
The analyzing HMC can be obtained using the **lssvcevents** command.
- help** Display the help text for this command and exit.

---

## chsyscfg

Change system resources.

## Synopsis

```
chsyscfg -r {lpar | prof | sys | sysprof | frame} {-m managed-system | -e managed-frame} {-f configuration-file | -i "configuration-data"} [--help]
```

## Description

**chsyscfg** changes the attributes of partitions, partition profiles, or system profiles for the *managed-system*. It can also change the attributes of the *managed-system*.

**chsyscfg** can also change the attributes of the *managed-frame*.

## Options

- r** The type of resources to change. Valid values are **lpar** for partitions, **prof** for partition profiles, **sys** for the managed system, **sysprof** for system profiles, and **frame** for the managed frame.
- m** The name of either the managed system to be changed, or the managed system which has the system resources to be changed. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.  
This option is required when changing the attributes of partitions, partition profiles, system profiles, or the managed system. This option is not valid otherwise.
- e** The name of the managed frame to be changed. The name may either be the user-defined name for the managed frame, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the type, *mmm* is the model, and *sssssss* is the serial number of the managed frame. The *ttt-mmm\*sssssss* form must be used if there are multiple managed frames with the same user-defined name.  
This option is required when changing the attributes of the managed frame. This option is not valid otherwise.
- f** The name of the file containing the configuration data needed to change the resources. The configuration data consists of attribute name/value pairs, which are in comma separated value (CSV) format. These attribute name/value pairs form a configuration record. A line feed marks the end of a configuration record. The file must contain one configuration record for each

resource to be changed, and each configuration record must be for the same resource type. If the resource type is the managed system or the managed frame, then the file must contain only one configuration record.

The format of a configuration record is as follows:

*attribute-name=value,attribute-name=value,...<LF>*

Note that certain attributes accept a comma separated list of values, as follows:

*"attribute-name=value,value,...",...<LF>*

When a list of values is specified, the attribute name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a '\ ' character.

If '+=' is used in the attribute name/value pair instead of '=', then the specified *value* is added to the existing value for the attribute if the attribute is numerical. If the attribute is a list, then the specified *value(s)* is added to the existing list.

If '-=' is used in the attribute name/value pair instead of '=', then the specified *value* is subtracted from the existing value for the attribute if the attribute is numerical. If the attribute is a list, then the specified *value(s)* is deleted from the existing list.

Attribute names for partitions:

**name | lpar\_id**

name or ID of the partition to change (required)

**new\_name**

**default\_profile**

**ipl\_source**

i5/OS only

Valid values are **a**, **b**, **c**, or **d**

**allow\_perf\_collection**

Valid values are:

**0** - do not allow

**1** - allow

This attribute replaces the **shared\_proc\_pool\_util\_auth** attribute. Setting this attribute also sets the **shared\_proc\_pool\_util\_auth** attribute to the same value.

**shared\_proc\_pool\_util\_auth**

Valid values are:

**0** - do not allow authority

**1** - allow authority

This attribute has been deprecated. Use the **allow\_perf\_collection** attribute instead.

Setting this attribute also sets the **allow\_perf\_collection** attribute to the same value.

**work\_group\_id**

**lpar\_avail\_priority**

POWER6 servers only

Valid values are **0** - **255**.

**electronic\_err\_reporting**

i5/OS only, POWER6 servers only

Valid values are:

**0** - disable

**1** - enable

Attribute names for partition profiles:

**name** name of the partition profile to change (required)

**lpar\_name** | **lpar\_id**  
 name or ID of the partition for which the profile to change is defined (required)

**new\_name**

**min\_mem**  
 megabytes

**desired\_mem**  
 megabytes

**max\_mem**  
 megabytes

**min\_num\_huge\_pages**  
 AIX and LINUX only

**desired\_num\_huge\_pages**  
 AIX and LINUX only

**max\_num\_huge\_pages**  
 AIX and LINUX only

**bsr\_arrays**  
 POWER6 servers only

**proc\_mode**  
 Valid values are:  
     **ded** - dedicated processors  
     **shared** - shared processors

**min\_procs**

**desired\_procs**

**max\_procs**

**min\_proc\_units**

**desired\_proc\_units**

**max\_proc\_units**

**min\_5250\_cpw\_percent**  
 Only valid for i5/OS partitions in managed systems that support the assignment of 5250

**desired\_5250\_cpw\_percent**  
 Only valid for i5/OS partitions in managed systems that support the assignment of 5250  
 CPW percentages

**max\_5250\_cpw\_percent**  
 Only valid for i5/OS partitions in managed systems that support the assignment of 5250  
 CPW percentages

**sharing\_mode**  
 Valid values are:  
     **keep\_idle\_procs** - never share processors  
     **share\_idle\_procs** - share processors only when partition is inactive  
     **share\_idle\_procs\_active** - share processors only when partition is active (POWER6  
 servers only)  
     **share\_idle\_procs\_always** - always share processors (POWER6 servers only)

Valid values for partitions using shared processors are:  
     **cap** - capped  
     **uncap** - uncapped

**uncap\_weight**

**io\_slots**  
 Comma separated list of I/O slots, with each I/O slot having the following format:  
*slot-DRC-index/slot-IO-pool-ID/is-required*

Both '/' characters must be present, but optional values may be omitted. Optional values  
 are *slot-IO-pool-ID*.

Valid values for *is-required*:  
     **0** - no  
     **1** - yes

**lpar\_io\_pool\_ids**  
comma separated

**load\_source\_slot**  
i5/OS only  
DRC index of I/O slot, or virtual slot number

**alt\_restart\_device\_slot**  
i5/OS only  
DRC index of I/O slot, or virtual slot number

**console\_slot**  
i5/OS only  
DRC index of I/O slot, DRC index of HEA logical port (POWER6 servers only), virtual slot number, or the value **hmc**

**alt\_console\_slot**  
i5/OS only  
DRC index of I/O slot

**op\_console\_slot**  
i5/OS only  
DRC index of I/O slot

**auto\_start**  
Valid values are:  
0 - off  
1 - on

**boot\_mode**  
AIX, Linux, and virtual I/O server only  
Valid values are:  
**norm** - normal  
**dd** - diagnostic with default boot list  
**ds** - diagnostic with stored boot list  
**of** - Open Firmware OK prompt  
**sms** - System Management Services

**power\_ctrl\_lpar\_ids | power\_ctrl\_lpar\_names**  
comma separated

**conn\_monitoring**  
Valid values are:  
0 - off  
1 - on

**hsl\_pool\_id**  
i5/OS only  
Valid values are:  
0 - HSL OptiConnect is disabled  
1 - HSL OptiConnect is enabled

**virtual\_opti\_pool\_id**  
i5/OS only  
Valid values are:  
0 - virtual OptiConnect is disabled  
1 - virtual OptiConnect is enabled

**max\_virtual\_slots**

**virtual\_eth\_adapters**  
Comma separated list of virtual ethernet adapters, with each adapter having the following format:  
*virtual-slot-number/is-IEEE/port-vlan-ID/additional-vlan-IDs/trunk-priority/is-required*

All 5 '/' characters must be present, but optional values may be omitted. Optional values are *additional-vlan-IDs* and *trunk-priority*.

Valid values for *is-IEEE* and *is-required*:

- 0 - no
- 1 - yes

Valid values for *trunk-priority*:

- 0 - this adapter is not a trunk adapter
- 1 - 15 - this adapter is a trunk adapter with the specified priority

#### **virtual\_scsi\_adapters**

Comma separated list of virtual SCSI adapters, with each adapter having the following format:

*virtual-slot-number/client-or-server/remote-lpar-ID/remote-lpar-name/remote-slot-number/is-required*

All 5 '/' characters must be present, but optional values may be omitted. Optional values for server adapters are *remote-lpar-ID*, *remote-lpar-name*, and *remote-slot-number*. Optional values for client adapters are *remote-lpar-ID* or *remote-lpar-name* (one of those values is required, but not both).

Valid values for *client-or-server*:

- client**
- server**

Valid values for *is-required*:

- 0 - no
- 1 - yes

#### **virtual\_serial\_adapters**

Comma separated list of virtual serial adapters, with each adapter having the following format:

*virtual-slot-number/client-or-server/supports-HMC/remote-lpar-ID/remote-lpar-name/remote-slot-number/is-required*

All 6 '/' characters must be present, but optional values may be omitted. Optional values for server adapters are *supports-HMC*, *remote-lpar-ID*, *remote-lpar-name*, and *remote-slot-number*. Optional values for client adapters are *remote-lpar-ID* or *remote-lpar-name* (one of those values is required, but not both), and the *supports-HMC* value is not allowed.

Valid values for *client-or-server*:

- client**
- server**

Valid values for *supports-HMC*:

- 0 - no

Valid values for *is-required*:

- 0 - no
- 1 - yes

#### **hca\_adapters**

AIX, Linux, and virtual I/O server only

Comma separated list of Host Channel adapters (HCA), with each adapter having the following format:

*adapter-ID/GUID/capability*

All 3 values must be specified for each adapter.



Valid values for *capability*:

- 1 - low
- 2 - medium
- 3 - high
- 4 - dedicated

#### **lhea\_logical\_ports**

POWER6 servers only

Comma separated list of Logical Host Ethernet adapter (LHEA) logical ports, with each logical port having the following format:

*adapter-ID/port-group/physical-port-ID/ logical-port-ID/allowed-VLAN-IDs*

All 4 '/' characters must be present, but optional values may be omitted. Optional values are allowed-VLAN-IDs.

#### **lhea\_capabilities**

POWER6 servers only

Comma separated list of LHEA capabilities, with each capability having one of the following formats:

*adapter-ID/capability*

or

*adapter-ID/5/ieq/nieq/qc/cq/mr*

where *ieq* (interruptible event queues), *n timer* (non-interruptible event queues), *qp* (queue pairs), *cq* (completion queues), and *mr* (memory regions) each specify the resource amount in addition to the base minimum.

Valid values for *capability*:

- 0 - base minimum
- 1 - low
- 2 - medium
- 3 - high
- 4 - dedicated

#### **sni\_device\_ids**

AIX, Linux, and virtual I/O server only

Comma separated list of Switch Network Interface (SNI) adapter device IDs

#### **work\_group\_id**

#### **redundant\_err\_path\_reporting**

Valid values are:

- 0 - disable
- 1 - enable

#### **electronic\_err\_reporting**

i5/OS only, POWER6 servers only

Valid values are:

- 0 - disable
- 1 - enable

#### **lpar\_proc\_compat\_mode**

POWER6 servers only

Valid values are:

- default** - default architected processor mode
- POWER6\_enhanced** - POWER6 enhanced processor mode

Attribute names for a managed system:

**new\_name**

**power\_off\_policy**

Valid values are:

- 0 - power off after all partitions are shut down
- 1 - do not power off after all partitions are shut down

**service\_lpar\_id**

Specify **none** to remove the service partition assignment

**service\_lpar\_name****power\_on\_option**

Valid values are **autostart** or **standby**

**power\_on\_side**

Valid values are **perm** or **temp**

**power\_on\_speed**

Valid values are **slow** or **fast**

**power\_on\_speed\_override**

Valid values are **none**, **slow**, or **fast**

**sp\_failover\_enabled**

Valid values are:

- 0 - disable service processor failover
- 1 - enable service processor failover

Attribute names for system profiles:

**name** name of the system profile to change (required)

**new\_name**

**lpar\_names** | **lpar\_ids**

comma separated

**profile\_names**

comma separated

Attribute names for a managed frame:

**new\_name**

**frame\_num**

The **-f** and the **-i** options are mutually exclusive.

- i** This option allows you to enter configuration data on the command line, instead of using a file. Data entered on the command line must follow the same format as data in a file, and must be enclosed in double quotes.

When this option is used, only a single resource can be changed.

The **-i** and the **-f** options are mutually exclusive.

- help** Display the help text for this command and exit.

## chsyspwd

Change system password.

### Synopsis

**chsyspwd -t** {**access** | **admin** | **general**} {**-m** *managed-system* | **-e** *managed-frame*} [**--passwd** *current-password*] [**--newpasswd** *new-password*] [**--help**]

### Description

**chsyspwd** changes a password for the *managed-system* or the *managed-frame*.

## Options

- t** The password to change. Valid values are **access** for the Hardware Management Console (HMC) Access password, **admin** for the Advanced System Management (ASM) Administrator password, and **general** for the ASM General password.
- m** The name of the managed system for which to change the password. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.  
  
The **-m** and the **-e** options are mutually exclusive.
- e** The name of the managed frame for which to change the password. The name may either be the user-defined name for the managed frame, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the type, *mmm* is the model, and *sssssss* is the serial number of the managed frame. The *ttt-mmm\*sssssss* form must be used if there are multiple managed frames with the same user-defined name.  
  
The **-e** and the **-m** options are mutually exclusive.
- passwd** The current password. If this option is omitted, you will be prompted to enter the current password.
- newpasswd** The new password. If this option is omitted, you will be prompted to enter the new password.  
  
The new password must be at least 4 characters in length, and cannot be longer than 63 characters.
- help** Display the help text for this command and exit.

---

## chsysstate

Change partition state or system state.

## Synopsis

To power on a managed system:

```
chsysstate -m managed-system -r sys -o {on | onstandby | onsysprof} [-f system-profile-name] [-k keylock-position]
```

To power off a managed system:

```
chsysstate -m managed-system -r sys -o off [--immed]
```

To restart a managed system:

```
chsysstate -m managed-system -r sys -o off --immed --restart
```

To rebuild a managed system or a managed frame:

```
chsysstate {-m managed-system | -e managed-frame} -r {sys | frame} -o rebuild
```

To recover partition data for a managed system:

**chsysstate -m *managed-system* -r sys -o recover**

To initiate service processor failover for a managed system:

**chsysstate -m *managed-system* -r sys -o spfailover**

To set the keylock position for a managed system or a partition:

**chsysstate -m *managed-system* -r {sys | lpar} -o chkey -k *keylock-position* [{-n *partition-name* | --id *partition-ID*}]**

To activate a partition:

**chsysstate -m *managed-system* -r lpar -o on {-n *partition-name* | --id *partition-ID*} [-f *partition-profile-name*] [-k *keylock-position*] [-b *boot-mode*] [-i *IPL-source*]**

To shut down or restart a partition:

**chsysstate -m *managed-system* -r lpar -o {shutdown | osshutdown | dumprestart | retrydump} {-n *partition-name* | --id *partition-ID*} [--immed] [--restart]**

To perform an operator panel service function on a partition:

**chsysstate -m *managed-system* -r lpar -o {dston | remotdstoff | remotdston | consoleservice | iopreset | iopdump} {-n *partition-name* | --id *partition-ID*}**

To validate or activate a system profile:

**chsysstate -m *managed-system* -r sysprof -n *system-profile-name* [-o on] [--continue] [--test]**

To power off all of the unowned I/O units in a managed frame:

**chsysstate -e *managed-frame* -r frame -o unownediooff**

To power off all of the unowned I/O units in a managed frame:

**chsysstate -e *managed-frame* -r frame -o unownediooff**

## Description

**chsysstate** changes the state of a partition, the *managed-system*, or the *managed-frame*.

## Options

**-m** The name of the managed system on which to perform the operation. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.

This option is required when performing a partition, system profile, or managed system operation.

This option is not valid otherwise.

**-e** The name of the managed frame on which to perform the operation. The name may either be the user-defined name for the managed frame, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the

type, *mmm* is the model, and *sssssss* is the serial number of the managed frame. The *tttt-mmm\*sssssss* form must be used if there are multiple managed frames with the same user-defined name.

This option is required when performing a managed frame operation. This option is not valid otherwise.

**-r** The type of resource on which to perform the operation. Valid values are **lpar** for partition, **sys** for managed system, **sysprof** for system profile, and **frame** for managed frame.

**-o** The operation to perform. Valid values are:

**on** activates a partition or a system profile, or powers on the *managed-system*. When powering on the *managed-system*, partitions that are marked as auto start and partitions that were running when the system was powered off are activated.

**onstandby**  
powers on the *managed-system* to standby state.

**onsysprof**  
powers on the *managed-system* then activates a system profile. Only those partitions in the system profile are activated.

**off** powers off the managed-system. If the **--immed** option is specified, a fast power off (operator panel function 8) is performed, otherwise a normal power off is performed. If both the **--immed** and the **--restart** options are specified, a restart (operator panel function 3) of the *managed-system* is performed.

**rebuild**  
rebuilds the *managed-system* or the *managed-frame*.

**recover**  
recovers partition data for the *managed-system* by restoring the data from the backup file on the HMC.

**spfailover**  
initiates service processor failover for the *managed-system*.

**chkey** sets the keylock position for a partition or the *managed-system*.

**shutdown**  
shuts down a partition. If the **--immed** option is specified, an immediate shut down (operator panel function 8) is performed, otherwise a delayed shut down is performed. If both the **--immed** and the **--restart** options are specified, an immediate restart (operator panel function 3) of the partition is performed.

**osshutdown**  
issues the AIX "shutdown" command to shut down an AIX or virtual I/O server partition. If the **--immed** option is specified, the AIX "shutdown -F" command is issued to immediately shut down the partition. If the **--restart** option is specified, the "r" option is included on the AIX shutdown command to restart the partition.

**dumprestart**  
initiates a dump on the partition and restarts the partition when the dump is complete (operator panel function 22).

**retrydump**  
retries the dump on the partition and restarts the partition when the dump is complete (operator panel function 34). This operation is valid for i5/OS partitions only.

**dston** activates dedicated service tools for the partition (operator panel function 21). This operation is valid for i5/OS partitions only.

**remotedstoffs**

disables a remote service session for the partition (operator panel function 65). This operation is valid for i5/OS partitions only.

**remotedston**

enables a remote service session for the partition (operator panel function 66). This operation is valid for i5/OS partitions only.

**iopreset**

resets or reloads the failed IOP (operator panel function 67). This operation is valid for i5/OS partitions only.

**iodump**

allows use of the IOP control storage dump (operator panel function 70). This operation is valid for i5/OS partitions only.

**unownedioff**

powers off all of the unowned I/O units in a managed frame.

- f When activating a partition, use this option to specify the name of the partition profile to use. This option is required unless the *managed-system* is in the manufacturing default configuration. If the *managed-system* is in the manufacturing default configuration and this option is not specified, the partition will be activated with no configuration changes and the *managed-system* will remain in the manufacturing default configuration. If the *managed-system* is in the manufacturing default configuration and this option is specified, the partition will be activated with the configuration specified by *partition-profile-name* and the manufacturing default configuration will be permanently exited.

When powering on a managed system with a system profile, use this option to specify the name of the system profile to use. This option is required.

- k The keylock position to set. Valid values are **manual** and **norm** for normal.  
This option is required when setting the keylock position for a partition or a managed system.  
This option is optional when powering on a managed system or activating a partition.

**--immed**

If this option is specified when powering off a managed system, a fast power off is performed.

This option must be specified when restarting a managed system.

If this option is specified when shutting down or restarting a partition, an immediate shut down or restart is performed.

**--restart**

If this option is specified, the partition or managed system will be restarted.

- n When performing a system profile operation, use this option to specify the name of the system profile on which to perform the operation.  
  
When performing a partition operation, use either this option to specify the name of the partition on which to perform the operation, or use the **--id** option to specify the partition's ID. The **-n** and the **--id** options are mutually exclusive for partition operations.
- id When performing a partition operation, use either this option to specify the ID of the partition on which to perform the operation, or use the **-n** option to specify the partition's name. The **--id** and the **-n** options are mutually exclusive for partition operations.
- b The boot mode to use when activating an AIX, Linux, or virtual I/O server partition. Valid values are **norm** for normal, **dd** for diagnostic with default boot list, **ds** for diagnostic with stored boot list, **of** for Open Firmware OK prompt, or **sms** for System Management Services.
- i The IPL source to use when activating an i5/OS partition. Valid values are **a**, **b**, **c**, or **d**.

**--test** If this option is specified when performing a system profile operation, the system profile is validated.

**--continue**

If this option is specified when activating a system profile, remaining partitions will continue to be activated after a partition activation failure occurs.

**--help** Display the help text for this command and exit.

---

## chusrtca

Displays welcome text at local console login or displays text when remotely login using SSH..

### Synopsis

**chusrtca** [-o { a | r | ab | rb}] [-f *welcome-file*] [-b *banner-file*] [-c] [--help]

### Description

**chusrtca** provides a method to deploy text file(s) containing welcome or warning message and present to all users who login locally on the Hardware Management Console (HMC). The text file must be named **WelcomeFile.txt**. A banner file can also be specified, to have its contents displayed prior to login with SSH. The banner file must first be copied to the HMC, then it will be copied to a location accessible by SSH daemon. The banner file must be named **BannerFile.txt**.

### Options

**-o** Enables (**e**), disables (**d**) the display of the Terms and Conditions panel at login. Adds (**a**) or removes (**r**) the HTML file containing the Terms and Conditions. Add banner (**ab**) and remove banner (**rb**) can only be specified when deploying a banner file. There is no need to enable or disable the display of banner file contents.

**-l** Adds (**a**) or removes (**r**) the text file containing the welcome text. Add banner (**ab**) and remove banner (**rb**) can only be specified when deploying a banner file.

**-f** The text file whose contents will be used as welcome, when login locally on the HMC, must be named **WelcomeFile.txt**.

**-b** The text file whose contents will be used as banner, when remotely login using SSH, must be named **BannerFile.txt**.

**-c** Removes the welcome or the banner file from the HMC filesystem. This option requires the **-f** or **-b** flags.

**--help** Display the help text for this command and exit.

---

## chvet

Activate Capacity on Demand advanced functions.

### Synopsis

**chvet** -o **e** -m *managed-system* -k *activation-code* [--help]

### Description

**chvet** performs activation of Capacity on Demand (CoD) advanced functions on the *managed-system*. CoD advanced functions include Advanced POWER Virtualization and Enterprise Enablement.

### Options

- o** The operation to perform. The only valid value is **e** to enter an activation code.
- m** The name of the managed system for which the activation is to be performed. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- k** The activation code (key) to enter. Letters may be entered in either upper case or lower case.
- help** Display the help text for this command and exit.

---

## cpdump

Copy dumps.

### Synopsis

```
cpdump -r {dvd | ftp} -f "file1 file2 ...fileN" [-h host-name] [-u user-ID] [--passwd password] [-d directory]
[--help]
```

### Description

**cpdump** copies managed system dumps and managed frame dumps from the Hardware Management Console (HMC) to DVD or a remote FTP site.

Use the **lsdump** command to list the managed system dumps and managed frame dumps that reside on the HMC.

### Options

- r** The storage location to where the dumps will be copied. Valid values are **dvd** for the DVD drive on the HMC and **ftp** for a remote FTP site.
- f** The file name of the dump to be copied. If multiple dumps are to be copied, the file names must be separated by blanks and enclosed in double quotes.
- h** The host name or IP address of the remote FTP site.  
This option is required when copying a dump to a remote FTP site. Otherwise, this option is not valid.
- u** The user ID to use to log in to the remote FTP site.  
This option is required when copying a dump to a remote FTP site. Otherwise, this option is not valid.
- passwd**  
The password to use to log in to the remote FTP site. If this option is omitted, you will be prompted to enter the password.  
This option is only valid when copying a dump to a remote FTP site.
- d** The directory to use on the remote FTP site. If this option is omitted, the dumps will be copied to the home directory of the user.  
This option is only valid when copying a dump to a remote FTP site.
- help** Display the help text for this command and exit.



---

## cpsysplan

Copy system plan.

### Synopsis

```
cpsysplan -r {ftp | media} -f file-name -o {import | export} [-h host-name] [-p ftp-port-number] [-u user-ID]
[--passwd password] [-d directory] [--check] [--help]
```

### Description

**cpsysplan** copies a system plan file between the Hardware Management Console (HMC) and either removable media or a remote host.

### Options

- r** The location where the system plan file will be copied to or from. Valid values are **ftp** for a remote FTP site and **media** for removable media. If **media** is specified, the media must be present in the removable media device and the device must be mounted with the **mount** command before this command is issued. The **lsmediadev** command can be used to display all of the removable media devices on the HMC.
- f** Specifies the name of the system plan file that is to be copied. The filename itself is restricted to the alphanumeric (upper and lower) as well as a set of special characters (comma, period, hyphen, underscore, and space). Of this set, there are the positional restriction in that the name cannot begin with period nor hyphen.  
  
**cpsysplan** performs a raw file copy. It does not parse or validate the system plan file content.  
  
The file will be searched for in the system plan file directory on the HMC when copying from the HMC. When copying to the HMC, the file will be written to this directory. If the file already exists, it will be overwritten unless the **--check** option is specified.  
  
The file name must end with the **.sysplan** suffix.
- o** Specifies if the file is to be copied to or from the system plan file directory on the HMC. Valid values are **export** to copy the file from the HMC to the resource location specified or **import** to copy the file from the resource location specified to the system plan file directory on the HMC.
- h** The host name or IP address of the remote FTP site.  
  
This option is required when copying a file to or from a remote FTP site. Otherwise, this option is not valid.
- p** The port number to use for the remote FTP site. If this option is omitted, the default FTP port 21 will be used.  
  
This option is only valid when copying a file to or from a remote FTP site.
- u** The user ID to use to log in to the remote FTP site.  
  
This option is required when copying a file to or from a remote FTP site. Otherwise, this option is not valid.
- passwd** The password to use to log in to the remote FTP site. If this option is omitted, you will be prompted to enter the password.  
  
This option is only valid when copying a file to or from a remote FTP site.
- d** The optional directory to use when copying a file to or from a remote FTP site.

This option is required when copying a system plan file to or from media. The directory is the name of the mounted removable media where the file is read from when **-o import** is specified or written to when **-o export** is specified.

**--check**

Specifies that when importing a file, this command should check the system plan directory and fail with an error if the file with the name specified with the **-f** option already exists.

This option is only valid when **-o import** is specified.

**--help** Display the help text for this command and exit.

---

## defsysplanres

Define system plan resource.

### Synopsis

**defsysplanres -r osinstall -n resource-name -v "resource-value" [-d "resource-description"] [--help]**

### Description

**defsysplanres** defines a system plan resource for use by system plans deployed from the Hardware Management Console (HMC).

### Options

- r** Specifies the type of system plan resource to define. The only valid value is **osinstall** for an operating system (OS) installation resource.  
  
This command does not create the resource. It sets the reference to an OS installation resource that can later be used within system plans that are deployed from the HMC where the resource has been defined. This resource is defined only to the HMC and not to any system plan or managed system. If the resource defined appears with a location attribute in a system plan, the plan location will be used instead.
- n** Specifies the name of the system plan resource to define. This will be used to get the plan resource location attribute when a system plan that needs to use the resource is deployed.  
  
Specify **vios** with this option to define the OS installation resource for installing a Virtual I/O Server with a system plan  
  
Specify **i5osv5r3m0** with this option to define the OS installation resource for installing the i5/OS V5R3M0 release with a system plan.  
  
Specify **sles9** with this option to define the OS installation resource for installing the SLES9 LINUX operating system with a system plan.  
  
Specify **rhel4** with this option to define the OS installation resource for installing the Red Hat 4 LINUX operating system with a system plan.  
  
Specify **aix52** with this option to define the OS installation resource for installing the AIX V5R2 operating system with a system plan.  
  
Specify **aix53** with this option to define the OS installation resource for installing the AIX V5R3 operating system with a system plan.  
  
Otherwise the name specified with this option is the name of the resource to define.
- v** Specifies the value of the resource. This value is not checked for validity by the command. It is treated as a string value.
- d** Specifies a description for the resource. This is an open text description field.

**--help** Display the help text for this command and exit.

---

## deploysysplan

Deploy system plan.

### Synopsis

**deploysysplan -f** *file-name* **-o** {**dv** | **v** | **d**} [**-m** *managed-system*] [**--force**] [**--plan** *plan-number*] [**-v**] [**-i** "*deployment-plan-step-identifier*"] [**--help**]

### Description

**deploysysplan** deploys a managed system's partition plan from a system plan file.

### Options

- f** Specifies the name of the file that contains the system plan that is to be deployed. The file must exist in the system plan file directory on the Hardware Management Console (HMC). This file will not be changed by the **deploysysplan** command.  
The file name must end with the **.sysplan** suffix.
- o** Specifies the deployment option to be used when deploying the system plan.  
Use the **dv** option to validate the system plan on the managed system, and if it is valid, to deploy it.  
Use the **v** option to validate the system plan on the managed system but not deploy it.  
Use the **d** option to skip validation of the system plan against the managed system, and just deploy the plan-specified partitions and profiles on the managed system.
- m** Specifies the managed system's name where the plan should be deployed. The system plan optionally specifies the managed system's name where that system plan was intended to be deployed. If a managed system name is specified with this option, that name would override the plan-provided name. If no managed system name was specified in the system plan file then this option is required.  
The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- force** If the managed system has existing partitions that the system plan contains that are in an active state, this option allows this command to proceed. Otherwise, if active partitions are found, this command will fail with an error message.
- plan** System plan files can contain more than one system plan. If the file contains more than one plan, this option specifies the number of the system plan to deploy. If this number is not specified, then the first system plan in the file is deployed. If there is only one system plan in the file, this option is ignored.
- v** When **-o v** is specified, this option specifies that a list of identifiers that identify the steps of the validated system plan should be written to stdout. These steps are part of the plan but not yet implemented on the managed system. Otherwise, this list will not be written out.  
When **-o dv** or **-o d** is specified, this option specifies that a list of log entries that record the steps performed as part of deploying the system plan should be written to stdout. Otherwise, this list will not be written out.
- i** A delimiter separated list of identifiers representing the desired steps in the specified system plan

to implement on the managed system. If this option is specified without any identifiers, then all of the steps in the plan will be performed as it is deployed on the managed system. If this list is not specified, then all the steps in the plan will be performed.

The values representing the system plan steps to be performed will be separated by a blank delimiter and the entire list must be enclosed in double quotes.

When this option is specified, only the system plan steps identified in this list will be performed. The system plan steps can be specified in any order but must identify deployment steps that appear in the system plan specified by the input file. The command processing will fail and none of the identified steps will be performed if an identifier is passed that does not identify a step in the system plan file.

Steps specified might be determined by command processing that already have been completed on the managed system. That will be logged by the command processing, however, is not an error.

This option is useful when only specific steps in a system plan file are desired to be performed. The command processing does not validate that the resulting deployment is valid but it will determine that dependent steps in the system plan will be checked for and enforced. The command processing will fail and none of the identified steps will be performed if there are dependent steps that are not specified. (For example a partition profile must exist before a system plan step to install its OS can be specified.)

**--help** Display the help text for this command and exit.

---

## dump

Perform dump operation.

### Synopsis

**dump -m *managed-system* -t *sys* -o *set* -a "*attributes*" [--help]**

### Description

**dump** sets the system dump parameters for the managed-system. This operation is only supported for POWER6 servers.

### Options

- m** The name of the managed system from which to set the system dump parameters. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- t** The type of dump for which to set the dump parameters. Valid values are **sys** for system dump.
- o** The dump operation to perform. Valid values are **set** to set the system dump parameters. The **set** operation is only supported for POWER6 servers.
- a** The configuration data needed to set the system dump parameters. The configuration data consists of attribute name/value pairs, which are in comma separated value (CSV) format. The configuration data must be enclosed in double quotes.

The format of the configuration data is as follows:

*attribute-name=value,attribute-name=value,...*

Valid attribute names:

### **as\_needed**

Specifies when to collect system dumps.

Valid values:

- 0 - do not collect system dumps
- 1 - collect system dumps as necessary

Setting **as\_needed** to 0 will remove the ability of service personnel to diagnose server errors. Do not set **as\_needed** to 0 unless directed to do so by your hardware service representative.

### **sys\_hardware**

Specifies how much hardware data to collect when a system dump occurs.

Valid values:

- auto** - collect hardware data based on the system dump event that occurred
- max** - collect as much hardware data as possible

Setting **sys\_hardware** to **max** will cause system dumps to take longer to complete. Do not set **sys\_hardware** to **max** unless directed to do so by your hardware service representative.

### **sys\_firmware**

Specifies how much system firmware data to collect when a system dump occurs.

Valid values:

- auto** - collect the primary data in memory owned by system firmware
- max** - collect the primary data in memory owned by system firmware plus all TCEs
- io** - collect the primary data in memory owned by system firmware plus all PCI TCEs
- virtualio** - collect the primary data in memory owned by system firmware plus all virtual I/O TCEs
- hps** - collect the primary data in memory owned by system firmware plus all High Performance Switch (HPS) TCEs
- hcaio** - collect the primary data in memory owned by system firmware plus all Host Channel Adapter (HCA) TCEs

Setting **sys\_firmware** to **max**, **io**, **virtualio**, **hps**, or **hcaio** will cause system dumps to take longer to complete. Do not set **sys\_firmware** to one of these values unless directed to do so by your hardware service representative.

**--help** Display the help text for this command and exit.

---

## **getdump**

Get dump.

### **Synopsis**

**getdump** {-m *managed-system* | -e *managed-frame*} -t {pss | sp | sys} [-s {a | b | p | s}] [--help]

### **Description**

**getdump** offloads a dump from the *managed-system* or the *managed-frame* to the Hardware Management Console (HMC). The dump is written to a file in the **/dump** directory on the HMC.

The **lsdump** command can be used to list the dumps that are available on the *managed-system* or the *managed-frame*.

### **Options**

- m** The name of the managed system from which to offload the dump. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.  
  
This option is required when offloading a service processor dump or a platform dump. This option is not valid otherwise.
- e** The name of the managed frame from which to offload the dump. The name may either be the user-defined name for the managed frame, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the type, *mmm* is the model, and *sssssss* is the serial number of the managed frame. The *ttt-mmm\*sssssss* form must be used if there are multiple managed frames with the same user-defined name.  
  
This option is required when offloading a power subsystem dump. This option is not valid otherwise.
- t** The dump to offload. Valid values are **pss** for the power subsystem dump, **sp** for the service processor dump, or **sys** for the platform dump.
- s** When offloading a power subsystem dump, use this option to specify the side of the managed frame's bulk power assembly (BPA) from which to offload the dump. Valid values are **a** for side A and **b** for side B.  
  
When offloading a service processor dump, use this option to specify the service processor from which to offload the dump. Valid values are **p** for the primary service processor and **s** for the secondary service processor. If this option is not specified, the service processor dump will be offloaded from the primary service processor.
- help** Display the help text for this command and exit.

---

## getupgfiles

Get upgrade files.

### Synopsis

**getupgfiles -h** *host-name* **-u** *user-ID* [**--passwd** *password*] **-d** *remote-directory* [**--help**]

### Description

**getupgfiles** obtains required files for a Hardware Management Console (HMC) upgrade from a directory on an FTP server. The files will be transferred onto a special partition on the HMC hard drive. After the files have been transferred, the **chhmc** command can be used to allow the HMC to boot from this partition and perform the upgrade.

### Options

- h** The host name or IP address of the remote FTP server.
- u** The user ID to use to log in to the remote FTP site.
- passwd** The password to use to log in to the remote FTP site. If this option is omitted, you will be prompted to enter the password.
- d** The remote directory on the FTP server where the files will be obtained. If all the required files are not present in this directory, this command will fail.
- help** Display the help text for this command and exit.

---

## hmcshutdown

Shut down the Hardware Management Console.

### Synopsis

**hmcshutdown** **-t** {**now** | *number-of-minutes*} [**-r**] [**--help**]

### Description

**hmcshutdown** shuts down the Hardware Management Console (HMC). If requested, the HMC will be rebooted after the shutdown completes.

### Options

- t**      The number of minutes to wait before starting the shutdown. If **now** is specified, the shutdown will be started immediately.
- r**      Reboot the HMC after the shutdown. If this option is omitted, the HMC will be halted after the shutdown.
- help** Display the help text for this command and exit.

---

## hmcwin

Provides screen capture on HMC.

### Synopsis

**hmcwin** { **-o** **c** | **v** | **r** } **-f** *file-name* [**--help**]

### Description

**hmcwin** provides screen capture on the HMC.

### Options

- o**      **c** captures the screen and saves it in *file-name*. The file will be saved under the user's \$HOME/.screen\_capture/ directory. **v** displays the image stored in file *file-name* from the user's \$HOME/.screen\_capture/ directory. When using the **v** option, left mouse click on the displayed window or enter Ctrl-c to dismiss it. **r** removes the file *file-name* under the user's \$HOME/.screen\_capture directory.
- f**      The file name to be used to create or remove the screen captured file under the user's \$HOME/.screen\_capture directory.
- help** Display the help text for this command and exit.

---

## installios

Network install a Virtual I/O Server Logical Partition.

### Synopsis

**installios** [**-p** *partition-name* **-i** *ipaddr-or-hostname* **-S** *subnet-mask* **-g** *gateway* **-d** *path* **-s** *system-name* **-m** *mac-address* **-r** *profile* [**-n**] [**-P** *speed*] [**-D** *duplex*] [**-l** *language*]] | **-u**

### Description



**installios** installs the Virtual I/O Server. It must be run from the HMC. All of the flags are optional. If no flags are provided, the **installios** wizard will be invoked and the user will be prompted to interactively enter the information contained in the flags.

## Options

- s** Specifies the managed system. The name of the managed system maintained by the HMC. This name must match the name shown on the HMC, not a host name.
- p** Specifies the partition name. The name of the LPAR that will be installed with Virtual I/O Server operating system. This partition must be of type Virtual I/O Server and the name given for it must match the name shown on the HMC, not a host name.
- r** Specifies the *profile* name. The name of the *profile* that contains the hardware resources being installed to.
- d** Specifies the *path* to installation images. Either */dev/cdrom* or the *path* to a system backup of the Virtual I/O Server created by the **backupios** command. The *path* may also specify a remote location mountable by NFS such as *hostname:/path\_to\_backup*
- i** Specifies the client IP address. The IP address with which the client's network interface will be configured for network installation of the Virtual I/O Server operating system.
- S** Specifies the client subnet mask. The subnet mask with which the client's network interface will be configured for network installation of the Virtual I/O Server operating system.
- g** Specifies the client *gateway*. The default *gateway* that the client will use during network installation of the Virtual I/O Server operating system.
- m** Specifies the client MAC address. The MAC address of the client network interface through which the network installation of the Virtual I/O Server will take place.
- P** Specifies *speed* (optional) The communication *speed* with which to configure the client's network interface. This value can be 10, 100, or 1000, and is 100 by default if this flag is not specified.
- D** Specifies duplex (optional). The duplex setting with which to configure the client's network interface. This value can be full or half and is set to full by default if this flag is not specified.
- n** Specifies not to configure the client's network interface (optional): If this flag is specified, then the client's network interface will not be configured with the IP settings specified in the flags given to this command after the installation has completed.
- l** Specifies *language* (optional): The *language* in which the license agreement will be displayed before the installation. Upon viewing the license, a prompt will be shown asking if the license is to be accepted. If the prompt is answered with y, then the installation will proceed and the Virtual I/O Server license will be automatically accepted after the installation. If the prompt is answered with n, then the **installios** command will exit and the installation will not proceed. If this flag is not specified, then the installation will proceed, but the Virtual I/O Server will not be usable until the license is manually accepted after the installation.
- u** Unconfigure **installios** (optional). Will manually unconfigure the **installios** installation resources. This flag is only needed if a problem occurs during the installation and **installios** does not automatically unconfigure itself.
- help** Display the help text for this command and exit.



---

## logssh

Log ssh command usage.

### Synopsis

logssh

### Description

**logssh** is a script that can be added to a user's **authorized\_keys2** file to restrict a user from being able to open a pseudo-tty using ssh. Furthermore, it will log all commands executed by the user in syslog. This command is not intended to be run interactively.

---

## lpar\_netboot

Retrieve MAC address and physical location code from network adapters for a partition or instruct a partition to network boot.

### Synopsis

To retrieve MAC address and physical location code:

```
lpar_netboot -M -n [-v] [-x] [-f] [-i] [-A] -t ent [-D -s speed -d duplex -S server -G gateway -C client]  
partition-name partition-profile managed-system
```

To perform network boot:

```
lpar_netboot [-v] [-x] [-f] [-i] [-g args] [{-A -D | [-D] -l physical-location-code | [-D] -m MAC-address}] -t ent  
-s speed -d duplex -S server -G gateway -C client partition-name partition-profile managed-system
```

To retrieve MAC address and physical location code on a system supporting a full system partition:

```
lpar_netboot -M -n [-v] [-x] [-f] [-i] [-A] -t ent [-D -s speed -d duplex -S server -G gateway -C client]  
managed-system managed-system
```

To perform network boot on a system supporting a full system partition:

```
lpar_netboot [-v] [-x] [-f] [-i] [-g args] [{-A -D | [-D] -l physical-location-code | [-D] -m MAC-address}] -t ent  
-s speed -d duplex -S server -G gateway -C client managed-system managed-system
```

### Description

**lpar\_netboot** instructs a logical partition to network boot by having it send out a bootp request to a server specified with the **-S** option. The server can be an AIX NIM server serving SPOT resources or any server serving network boot images. If specified with the **-M** and **-n** options, **lpar\_netboot** will return the Media Access Control (MAC) address and the physical location code for a network adapter of the type specified with the **-t** option. When the **-m** option is specified, **lpar\_netboot** will boot a partition using the network adapter which has the specified MAC address. When the **-l** option is specified, **lpar\_netboot** will boot a partition using the network adapter which has the specified physical location code. The MAC address and physical location code of a network adapter is dependent upon the hardware resource allocation in the partition profile the partition was booted with. The **lpar\_netboot** command requires arguments for partition name, partition profile, and the name of the managed system which has the partition.

### Options

- A** Return all adapters of the type specified with the **-t** option.
- C** The IP address of the partition to network boot.
- D** Perform a ping test and use the adapter that successfully pings the server specified with the **-S** option.
- G** The gateway IP address of the partition specified with the **-C** option.
- M** Discover network adapter MAC address and physical location code.
- S** The IP address of the machine from which to retrieve the network boot image during network boot.
- d** The duplex setting of the partition specified with the **-C** option. Valid values are **full**, **half**, and **auto**.
- f** Force close the virtual terminal session for the partition.
- g** Specify generic arguments for booting the partition.
- i** Force immediate shutdown of the partition. If this option is not specified, a delayed shutdown will be performed.
- l** The physical location code of the network adapter to use for network boot.
- m** The MAC address of the network adapter to use for network boot.
- n** Instruct the partition to not network boot.
- s** The speed setting of the partition specified with the **-C** option. Valid values are **10**, **100**, **1000**, and **auto**.
- t** The type of adapter for MAC address or physical location code discovery or for network boot. The only valid value is **ent** for ethernet.
- v** Display additional information during command execution.
- x** Display debug output during command execution.

**partition-name**

The name of the partition.

**partition-profile**

The name of the partition profile.

**managed-system**

The name of the managed system which has the partition.

**--help** Display the help text for this command and exit.

---

## lpcfgop

Perform a partition configuration image operation.

### Synopsis

**lpcfgop -m** *managed-system* **-o** {**clear** | **dump**} [**--help**]

### Description

**lpcfgop** clears or dumps partition configuration data on the *managed-system*.

### Options

**-m** The name of the managed system on which to perform the operation. The name may either be

the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.

**-o** The operation to perform. Valid values are **clear** or **dump**.

The **clear** operation clears all partition configuration data on the *managed-system* and sets the configuration back to its original state. This operation can only be performed when the *managed-system* is in the Standby state.

The **dump** operation dumps all partition configuration data on the *managed-system* to a file. The file is written to the **/tmp** directory on the Hardware Management Console (HMC).

**--help** Display the help text for this command and exit.

---

## lsaccfg

List access control configuration information.

### Synopsis

```
lsaccfg -t {resource | resourcerole | taskrole} [--script] [--filter "filter-data"] [-F [attribute-names]
[--header]] [--help]
```

### Description

**lsaccfg** lists managed resource objects, managed resource roles, or task roles.

### Options

**-t** The type of access control objects to list. Valid values are **resource** for managed resource objects, **resourcerole** for managed resource roles, and **taskrole** for task roles.

**--script**

List managed resource objects in a format that can be used as input to the **chaccfg**, **chhmcusr**, and **mkaccfg** commands. This option is only valid when listing managed resource objects.

**--filter** The filter to apply to the access control objects to be listed. A filter is used to select which access control objects of the specified type are to be listed. If a filter is not used, then all of the access control objects of the specified type will be listed. For example, specific task roles can be listed by using a filter to specify the names of the task roles to list. Otherwise, if no filter is used, then all of the task roles on this Hardware Management Console (HMC) will be listed.

The filter data consists of filter name/value pairs, which are in comma separated value (CSV) format. The filter data must be enclosed in double quotes.

The format of the filter data is as follows:

```
"filter-name=value,filter-name=value,..."
```

Note that certain filters accept a comma separated list of values, as follows:

```
"filter-name=value,value,...",..."
```

When a list of values is specified, the filter name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a `'\'` character.

Multiple values can be specified for each filter.

Valid filter names for managed resource objects:

**resource\_type**

Specify resource type(s):  
**cec** - managed system objects  
**lpar** - partition objects

Valid filter names for managed resource roles:

**resourceroles**

Specify managed resource role name(s)

Valid filter names for task roles:

**taskroles**

Specify task role name(s)

**-F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each access control object. If no attribute names are specified, then values for all of the attributes for each access control object will be displayed.

When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.

This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.

**--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

---

## lscod

List Capacity on Demand information.

### Synopsis

**lscod -t {bill | cap | code | hist | util} -m managed-system [-c {cuod | mobile | onoff | reserve | trial | trialex | trialstd | utility | utilityen}] [-r {mem | proc}] [-F [attribute-names] [--header]] [--help]**

### Description

**lscod** lists Capacity on Demand (CoD) information for the *managed-system*.

Reserve CoD is only supported on POWER5 servers. Utility CoD is only supported on POWER6 servers.

### Options

- t** The type of CoD information to list. Valid values are **bill** for On/Off CoD billing information, **cap** for CoD capacity information, **code** for information used to generate CoD codes, **hist** for the CoD history log, and **util** for shared processor pool utilization information.
- m** The name of the managed system for which CoD information is to be listed. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- c** The CoD type. Valid values are **cuod** for CUoD (permanent), **mobile** for Mobile CoD, **onoff** for

On/Off CoD, **reserve** for Reserve CoD, **trial** for Trial CoD, **utility** for Utility CoD or Utility CoD reporting codes, **utilityen** for Utility CoD enablement codes, **trialexc** for Trial CoD exception request codes, and **trialstd** for Trial CoD standard request codes.

This option is required when listing CoD capacity information or CoD code generation information. If this option is not specified when listing shared processor pool utilization information, this option defaults to Reserve CoD. This option is not valid when listing the CoD history log.

To list Trial CoD capacity information, specify **trial** with this option. To list Trial CoD code generation information, specify **trialexc** or **trialstd** with this option.

To list Utility CoD capacity information, specify **utility** with this option. To list Utility CoD code generation information, specify **utility** for Utility CoD reporting codes or **utilityen** for Utility CoD enablement codes.

**mobile** can only be specified when listing CoD code generation information.

Reserve CoD is only supported on POWER5 servers. Utility CoD is only supported on POWER6 servers.

**-r** The CoD resource type. Valid values are **mem** for memory and **proc** for processors.

This option is required when listing On/Off CoD billing information, CoD capacity information, CoD code generation information, or shared processor pool utilization information. This option is not valid when listing the CoD history log.

**-F** A delimiter separated list of attribute names representing the desired CoD attribute values to display. If this option is specified without any attribute names, then all of the CoD attributes for the type of CoD listing specified will be displayed.

When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.

This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.

**--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

---

## lsdump

List dump information.

### Synopsis

To list the dumps that are available on a managed system or managed frame:

```
lsdump {-m managed-system | -e managed-frame} [-r avail] [-s {a | b | p | s}] [-F [attribute-names]  
[--header]]
```

To list the managed system dumps and managed frame dumps that are available on the HMC:

```
lsdump -h [-r avail] [--filter "filter-data"] [-F [attribute-names] [--header]]
```

To list the system dump parameters (POWER6 servers only):

**lsdump -m** *managed-system* **-r** *parm* [**-F** *[attribute-names]*] [**--header**]

## Description

**lsdump** lists the dumps that are available on the *managed-system* or the *managed-frame*. **lsdump** can also list the managed system dumps and the managed frame dumps that are available on the Hardware Management Console (HMC).

**lsdump** also lists the system dump parameters for the managed-system. This is only supported for POWER6 servers.

The **getdump** command can be used to offload an available dump from the *managed-system* or the *managed-frame* to the HMC.

The **cpdump** command can be used to copy a dump from the HMC to DVD or a remote FTP site.

## Options

- m** The name of the managed system for which available dumps or system dump parameters are to be listed. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.  
  
Either this option, the **-e** option, or the **-h** option is required. The **-m**, **-e**, and the **-h** options are mutually exclusive.
- e** The name of the managed frame for which available dumps are to be listed. The name may either be the user-defined name for the managed frame, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the type, *mmm* is the model, and *sssssss* is the serial number of the managed frame. The *tttt-mmm\*sssssss* form must be used if there are multiple managed frames with the same user-defined name.  
  
Either this option, the **-m** option, or the **-h** option is required. The **-e**, **-m**, and the **-h** options are mutually exclusive.
- h** List the managed system dumps and managed frame dumps that are available on the HMC.  
  
Either this option, the **-m** option, or the **-e** option is required. The **-h**, **-m**, and the **-e** options are mutually exclusive.
- r** The type of dump resources to list. Valid values are *avail* for available dumps, and *parm* for system dump parameters. If this option is not specified, available dumps will be listed.  
  
System dump parameters can only be listed on POWER6 servers.
- s** When listing dumps that are available on a managed frame, use this option to specify the side of the managed frame's bulk power assembly (BPA) for which available dumps are to be listed. Valid values are **a** for side A and **b** for side B.  
  
When listing dumps that are available on a managed system, use this option to specify the service processor for which available dumps are to be listed. Valid values are **p** for the primary service processor and **s** for the secondary service processor. If this option is not specified, available dumps on the primary service processor will be listed. Platform dumps are only available from the primary service processor.  
  
This option is not valid when listing the managed system dumps and managed frame dumps that are available on the HMC.
- filter** The filter to apply to the available dumps to be listed. The filter is used to select the type of dump that is to be listed. If no filter is specified, then all of the available dumps will be listed.

The filter data consists of filter name/value pairs, which are in comma separated value (CSV) format. The filter data must be enclosed in double quotes.

The format of the filter data is as follows:

*"filter-name=value,filter-name=value,..."*

Valid filter names for this command:

#### **dump\_type**

Only one value may be specified.

Valid values are:

**pss** for power subsystem dumps

**sp** for service processor dumps

**sys** for system dumps

This option is not valid when listing the dumps that are available on a managed system or managed frame, or when listing the system dump parameters.

- F** A delimiter separated list of attribute names representing the desired dump attribute values to display. If this option is specified without any attribute names, then all of the dump attributes will be displayed.

When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.

This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.

#### **--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

- help** Display the help text for this command and exit.

---

## **lshmc**

List Hardware Management Console configuration information.

### **Synopsis**

**lshmc** {-b | -l | -L | -n | -r | -v | -V} [-F *[attribute-names]*] [--header]] [--help]

### **Description**

**lshmc** lists Hardware Management Console (HMC) configuration information. This command can be used to list the BIOS level, current locale, supported locales, network settings, remote access settings, Vital Product Data (VPD) information, and version information for the HMC.

### **Options**

- b** List the BIOS level of the HMC.  
This option cannot be specified with the **-l**, **-L**, **-n**, **-r**, **-v**, or **-V** options.
- l** List the current locale for the HMC.  
This option cannot be specified with the **-b**, **-L**, **-n**, **-r**, **-v**, or **-V** options.
- L** List all of the locales supported for the HMC.



- This option cannot be specified with the **-b**, **-l**, **-n**, **-r**, **-v**, or **-V** options.
- n** List the network settings for the HMC.  
This option cannot be specified with the **-b**, **-l**, **-L**, **-r**, **-v**, or **-V** options.
- r** List the remote access settings for the HMC.  
This option cannot be specified with the **-b**, **-l**, **-L**, **-n**, **-v**, or **-V** options.
- v** List the VPD information for the HMC.  
This option cannot be specified with the **-b**, **-l**, **-L**, **-n**, **-r**, or **-V** options.
- V** List the version information for the HMC.  
This option cannot be specified with the **-b**, **-l**, **-L**, **-n**, **-r**, or **-v** options.
- F** A delimiter separated list of attribute names representing the desired attribute values to display. If this option is specified without any attribute names, then all of the attributes for the type of HMC configuration information specified will be displayed.  
  
When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.  
  
This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.
- header** Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.
- help** Display the help text for this command and exit.

---

## lshmcusr

List Hardware Management Console user information.

## Synopsis

**lshmcusr** [**--script**] [**--filter** "*filter-data*"] [**-F** [*attribute-names*]] [**--header**]] [**--help**]

## Description

**lshmcusr** lists Hardware Management Console (HMC) user information.

## Options

- script** List managed resource objects in a format that can be used as input to the **chhmcusr**, **chaccfg**, and **mkaccfg** commands.
- filter** The filter to apply to the HMC users to be listed. A filter is used to select which HMC users are to be listed. If a filter is not used, then all HMC users will be listed.  
  
The filter data consists of filter name/value pairs, which are in comma separated value (CSV) format. The filter data must be enclosed in double quotes.  
  
The format of the filter data is as follows:  
*"filter-name=value,filter-name=value,..."*  
  
Note that certain filters accept a comma separated list of values, as follows:



*""filter-name=value,value,...",..."*

When a list of values is specified, the filter name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a `'\'` character.

Multiple values can be specified for each filter.

Valid filter names for this command:

**names** Specify user name(s)

**resources**

Specify managed resource object(s)

**resourceroles**

Specify managed resource role name(s)

**taskroles**

Specify task role name(s)

**-F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each HMC user. If no attribute names are specified, then values for all of the attributes for each HMC user will be displayed.

When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.

This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.

**--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

---

## lshwinfo

List environmental information.

### Synopsis

**lshwinfo -r {frame | sys} -e managed-frame [-F [attribute-names] [--header]] [--help]**

### Description

**lshwinfo** lists environmental information, such as input power levels and ambient air temperatures, for the *managed-frame*.

### Options

- r** The type of resource for which to list environmental information. Valid values are **frame** for managed frame and **sys** for systems contained in a managed frame.
- e** The name of the managed frame for which to list environmental information. The name may either be the user-defined name for the managed frame, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the type, *mmm* is the model, and *sssssss* is the serial number of the managed frame. The *tttt-mmm\*sssssss* form must be used if there are multiple managed frames with the same user-defined name.

- F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each HMC user. If no attribute names are specified, then values for all of the attributes for each HMC user will be displayed.
- When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.
- This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.
- header** Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.
- help** Display the help text for this command and exit.
- 

## lshwres

List hardware resources.

### Synopsis

To list physical I/O resources:

```
lshwres -r io --rsubtype {unit | bus | slot | iopool | taggedio} -m managed-system [--level {pool | sys}] [-R] [--filter "filter-data"] [-F [attribute-names]] [--header]] [--help]
```

To list virtual I/O resources:

```
lshwres -r virtualio --rsubtype {eth | hsl | virtualopti | scsi | serial | slot} -m managed-system [--level {lpar | slot | sys}] [--filter "filter-data"] [-F [attribute-names]] [--header]] [--help]
```

To list memory resources:

```
lshwres -r mem -m managed-system --level {lpar | sys} [-R] [--maxmem quantity] [--filter "filter-data"] [-F [attribute-names]] [--header]] [--help]
```

To list processing resources:

```
lshwres -r proc -m managed-system --level {lpar | pool | sys} [-R] [--procunits quantity] [--filter "filter-data"] [-F [attribute-names]] [--header]] [--help]
```

To list Host Channel adapter (HCA) resources:

```
lshwres -r hca -m managed-system --level {lpar | sys} [--filter "filter-data"] [-F [attribute-names]] [--header]] [--help]
```

To list Host Ethernet adapter (HEA) resources (POWER6 servers only):

```
lshwres -r hea -m managed-system --rsubtype {logical | phys} --level {port | port_group | sys} [-R] [--stat] [--filter "filter-data"] [-F [attribute-names]] [--header]] [--help]
```

To list Switch Network Interface (SNI) adapter resources:

```
lshwres -r sni -m managed-system [--filter "filter-data"] [-F [attribute-names]] [--header]] [--help]
```

## Description

**lshwres** lists the hardware resources of the *managed-system*, including physical I/O, virtual I/O, memory, processing, Host Channel adapter (HCA), Host ethernet adapter (HEA) and Switch Network Interface (SNI) adapter resources.

## Options

**-r** The type of hardware resources to list. Valid values are **io** for physical I/O, **virtualio** for virtual I/O, **mem** for memory, **proc** for processing, **hca** for HCA, **hea** for HEA, and **sni** for SNI adapter resources.

HEA resources are only supported on POWER6 servers.

### --subtype

The subtype of hardware resources to list. Valid physical I/O resource subtypes are **unit** for I/O units, **bus** for I/O buses, **slot** for I/O slots, **iopool** for I/O pools, and **taggedio** for tagged I/O resources. Valid virtual I/O resource subtypes are **eth** for virtual ethernet, **hsl** for High Speed Link (HSL) OptiConnect, **virtualopti** for virtual OptiConnect, **scsi** for virtual SCSI, **serial** for virtual serial, and **slot** for virtual slot resources. Valid HEA resource subtypes are **logical** for logical HEA resources, and **phys** for physical HEA resources.

This option is required when listing physical I/O, virtual I/O resources, or HEA resources. This option is not valid when listing memory, processing, HCA, or SNI adapter resources.

**-m** The name of the managed system which has the hardware resources to list. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.

**--level** The level of information to list. Valid values are **lpar** for partition, **pool** for pool, **port** for port, **port\_group** for port group, **slot** for slot, and **sys** for system.

This option is required when listing I/O pool resources, virtual ethernet, serial, or slot resources, or memory, processing, HCA, or HEA resources.

Valid levels for I/O pool resources are **pool** or **sys**. Valid levels for virtual ethernet resources are **lpar** or **sys**. Valid levels for virtual serial resources are **lpar**. Valid levels for virtual slot resources are **lpar** or **slot**. Valid levels for memory resources are **lpar** or **sys**. Valid levels for processing resources are **lpar**, **pool**, or **sys**. Valid levels for HCA resources are **lpar** or **sys**. Valid levels for physical HEA resources are **port**, **port\_group**, or **sys**. Valid levels for logical HEA resources are **port** or **sys**.

**-R** Only list information for partitions with hardware resources that can be restored due to a dynamic logical partitioning (DLPAR) operation failure. The

**rsthwres** command can be used to restore those hardware resources.

This option is only valid for listing physical I/O slots, partition level memory or processing resources, or logical HEA resources.

### --maxmem

When this option is specified, the required minimum memory amount needed for partitions to support the maximum memory *quantity* specified is listed. All memory quantities are in megabytes, and are a multiple of the memory region size for the *managed-system*.

This information is useful for specifying memory amounts in partition profiles.

The required minimum memory amount listed is the minimum memory amount required for a partition by the managed system's system firmware. An operating system installed on the partition may require more memory than the amount listed.

This option is only valid when listing system level memory resources.

**--procunits**

When this option is specified, the range of optimal 5250 CPW percentages for partitions assigned the *quantity* of processing units specified is listed. The *quantity* of processing units specified can have up to 2 decimal places.

This information is useful when specifying the 5250 CPW percentages for partitions or partition profiles.

This option is only valid when listing system level processing resources. Also, this option is only valid when the *managed-system* supports the assignment of 5250 CPW percentages to partitions.

**--stat** When this option is specified, port counter statistics for HEA physical ports are listed.

This option is only valid when listing HEA physical port resources.

**--filter** The filter(s) to apply to the hardware resources to be listed. Filters are used to select which hardware resources of the specified type are to be listed. If no filters are used, then all of the hardware resources of the specified type will be listed. For example, all of the physical I/O slots on a specific I/O unit and bus can be listed by using a filter to specify the I/O unit and the bus which has the slots to list. Otherwise, if no filter is used, then all of the physical I/O slots in the managed system will be listed.

The filter data consists of filter name/value pairs, which are in comma separated value (CSV) format. The filter data must be enclosed in double quotes.

The format of the filter data is as follows:

`"filter-name=value,filter-name=value,..."`

Note that certain filters accept a comma separated list of values, as follows:

`""filter-name=value,value,...",..."`

When a list of values is specified, the filter name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a `'\'` character.

Unless otherwise indicated, multiple values can be specified for each filter.

Valid filter names for this command:

**adapter\_ids**

Specify HCA or HEA adapter ID(s)

**buses** Specify I/O bus ID(s)

**lpar\_ids**

Specify partition ID(s)

**lpar\_names**

Specify partition user-defined name(s)

**pools** Specify pool ID(s)

**port\_groups**

Specify HEA port group(s)

**slots** Specify physical I/O slot DRC index(ices) or virtual I/O slot number(s)

**sni\_device\_ids**

Specify SNI adapter device ID(s)

**units** Specify I/O unit physical location code(s)

**vlans** Specify virtual LAN ID(s)

Valid filters with **-r io --rsubtype unit**:

**units**

Valid filters with **-r io --rsubtype bus**:

**buses, units**

Valid filters with **-r io --rsubtype slot**:

**buses, lpar\_ids | lpar\_names, pools, slots, units**

Valid filters with **-r io --rsubtype iopool --level pool**:

**lpar\_ids | lpar\_names, pools**

Valid filters with **-r io --rsubtype taggedio**:

**lpar\_ids | lpar\_names**

Valid filters with **-r virtualio --rsubtype eth --level lpar**:

**lpar\_ids | lpar\_names, slots, vlans**

Valid filters with **-r virtualio --rsubtype hsl**:

**lpar\_ids | lpar\_names, pools**

Valid filters with **-r virtualio --rsubtype virtualopti**:

**lpar\_ids | lpar\_names, pools**

Valid filters with **-r virtualio --rsubtype scsi**:

**lpar\_ids | lpar\_names, slots**

Valid filters with **-r virtualio --rsubtype serial --level lpar**:

**lpar\_ids | lpar\_names, slots**

Valid filters with **-r virtualio --rsubtype slot --level lpar**:

**lpar\_ids | lpar\_names**

Valid filters with **-r virtualio --rsubtype slot --level slot**:

**lpar\_ids | lpar\_names, slots**

Valid filters with **-r mem --level lpar**:

**lpar\_ids | lpar\_names**

Valid filters with **-r proc --level lpar**:

**lpar\_ids | lpar\_names**

Valid filters with **-r hca --level sys**:

**adapter\_ids**

Valid filters with **-r hca --level lpar**:

**adapter\_ids, lpar\_ids | lpar\_names**

Valid filters with **-r hea --subtype logical --level sys:**

**adapter\_ids, lpar\_ids | lpar\_names**

Valid filters with **-r hea --subtype logical --level port:**

**adapter\_ids, lpar\_ids | lpar\_names, port\_groups**

Valid filters with **-r hea --subtype phys --level sys:**

**adapter\_ids**

Valid filters with **-r hea --subtype phys --level port:**

**adapter\_ids, port\_groups**

Valid filters with **-r hea --subtype phys --level port\_group:**

**adapter\_ids, port\_groups**

Valid filters with **-r sni:**

**lpar\_ids | lpar\_names, sni\_device\_ids**

**-F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each hardware resource. If no attribute names are specified, then values for all of the attributes for each hardware resource will be displayed.

When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.

This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.

**--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

---

## Isled

List LEDs.

## Synopsis

**Isled -r sa -t {phys | virtuallpar | virtualsys} -m *managed-system* [--filter "*filter-data*"] [-F [*attribute-names*] [--header]] [--help]**

## Description

**Isled** lists LED information for the *managed-system*.

## Options

- r** The type of LED resources to list. The only valid value is **sa** for System Attention (SA) LEDs.
- t** The type of System Attention (SA) LEDs to list. Valid values are **phys** for the physical SA LED for the *managed-system*, **virtualpar** for virtual partition SA LEDs, or **virtualsys** for the virtual SA LED for the *managed-system*.
- m** The name of the managed system which has the LEDs to list. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- filter** The filter to apply to the virtual partition SA LEDs to be listed. A filter is used to select which virtual partition SA LEDs are to be listed. If no filter is used, then all of the virtual partition SA LEDs for the managed-system will be listed.  
  
The filter data consists of filter name/value pairs, which are in comma separated value (CSV) format. The filter data must be enclosed in double quotes.  
  
The format of the filter data is as follows:  
*"filter-name=value,filter-name=value,..."*  
  
Note that certain filters accept a comma separated list of values, as follows:  
*""filter-name=value,value,...","..."*  
  
When a list of values is specified, the filter name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a `'\'` character.  
  
Valid filter names for this command are **lpar\_names** or **lpar\_ids**. Only one of these filters may be specified. Multiple partitions can be specified with the filter.  
  
This option is not valid when listing the physical SA LED or the virtual SA LED for the *managed-system*.
- F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each LIC level. If no attribute names are specified, then values for all of the attributes for each LIC level will be displayed.  
  
When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.  
  
This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.
- header** Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.
- help** Display the help text for this command and exit.

---

## Islic

List Licensed Internal Code levels.

### Synopsis

```
Islic {-m managed-system | -e managed-frame | -w} [-t {sys | power | syspower | powerfru}] [-r {ibmretain | ibmwebsite | ftp | dvd | disk | mountpoint}] [-h host-name] [-u user-ID] [--passwd password] [-d directory] [-F [attribute-names]] [--header]] [--help]
```



## Description

**lsled** lists Licensed Internal Code (LIC) levels installed, activated, and accepted. The LIC levels that are available to be retrieved from a repository can also be listed.

## Options

- m** The name of the managed system for which LIC levels are to be listed. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmmm\*ssssssss*, where *tttt* is the machine type, *mmm* is the model, and *ssssssss* is the serial number of the managed system. The *tttt-mmmm\*ssssssss* form must be used if there are multiple managed systems with the same user-defined name.
- e** The name of the managed frame for which LIC levels are to be listed. The name may either be the user-defined name for the managed frame, or be in the form *tttt-mmmm\*ssssssss*, where *tttt* is the machine type, *mmm* is the model, and *ssssssss* is the serial number of the managed frame. The *tttt-mmmm\*ssssssss* form must be used if there are multiple managed frames with the same user-defined name.
- w** List Licensed Internal Code levels on all High Performance Switches managed by the HMC.
- t** The type of LIC levels to list. Valid values are **sys** for Managed System LIC levels only, **power** for Power LIC levels only, **syspower** for both Managed System and Power LIC levels, or **powerfru** for Power FRU levels.
- r** The repository to query for LIC levels that are available to be retrieved for the *managed-system*. Valid values are **ibmretain** for the IBM support system, **ibmwebsite** for the IBM service Internet site, **ftp** for a remote FTP site, **dvd** for the DVD drive on the Hardware Management Console (HMC), **disk** for the internal hard disk drive on the HMC, or **mountpoint** for the specified mountpoint.
- h** The host name or IP address of the remote FTP server.  
  
This option is required when displaying LIC levels that are available to be retrieved from a remote FTP site. This option is not valid otherwise.
- u** The user ID to use to log in to the remote FTP site.  
  
This option is required when displaying LIC levels that are available to be retrieved from a remote FTP site. This option is not valid otherwise.
- passwd**  
The password to use to log in to the remote FTP site. If this option is omitted, you will be prompted to enter the password.  
  
This option is only valid when displaying LIC levels that are available to be retrieved from a remote FTP site.
- d** The mountpoint location or the directory to use on the remote FTP site. If this option is not specified for FTP, then the **/opt/ccfw/data** directory will be used.  
  
This option is only valid when displaying LIC levels that are available to be retrieved from a mountpoint or a remote FTP site.
- F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each LIC level. If no attribute names are specified, then values for all of the attributes for each LIC level will be displayed.  
  
When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.  
  
This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.



**--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

---

## Islock

List lock information.

## Synopsis

**Islock -e** *managed-frame* **[-F** *attribute-names*  **[--header]] [--help]**

## Description

**Islock** lists which Hardware Management Console (HMC) owns the lock on the *managed-frame*. If the *managed-frame* is not locked, then "No results were found." will be displayed.

## Options

- e** The name of the managed frame for which to list lock information. The name may either be the user-defined name for the managed frame, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the type, *mmm* is the model, and *sssssss* is the serial number of the managed frame. The *tttt-mmm\*sssssss* form must be used if there are multiple managed frames with the same user-defined name.
- F** A delimiter separated list of attribute names for the desired attribute values to be displayed. If no attribute names are specified, then values for all of the attributes will be displayed.  
  
When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.  
  
This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.

**--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

---

## Isiparutil

List utilization data.

## Synopsis

To list utilization data collected for a managed system:

**Isiparutil -r** {**hmc** | **lpar** | **pool** | **sys** | **all**} **-m** *managed-system* **[-d** *number-of-days*  **[-h** *number-of-hours*  **[--startyear** *year*  **[--startmonth** *month*  **[--startday** *day*  **[--starthour** *hour*  **[--endyear** *year*  **[--endmonth** *month*  **[--endday** *day*  **[--endhour** *hour*  **[-n** *number-of-events*  **[-s** *sample-rate*  **[--filter** *"filter-data"*  **[-F** *attribute-names*  **[--header]] [--help]**

To list HMC settings for utilization data collection:

**lslparutil -r config [-m *managed-system*] [-F [*attribute-names*] [--header]] [--help]**

## Description

**lslparutil** lists utilization data collected for a *managed-system*. This command also lists the Hardware Management Console (HMC) settings for utilization data collection.

The HMC collects the following types of utilization data: sampling events, state change events, configuration change events, and Utility Capacity on Demand (CoD) processor usage events.

Sampling events are collected for the managed system, for each partition in the managed system, and for the shared processor pool in the managed system. Sampling events are collected hourly, daily at midnight, and monthly at midnight on the first day of each month. Sampling events are also collected immediately following the collection of a Utility CoD processor usage event. Sampling events contain information about memory and processor utilization.

State change events are collected for the managed system, for each partition in the managed system, and for the HMC. State change events are collected when a state change occurs for the managed system, a partition, or when the HMC is started or shut down.

Configuration change events are collected for the managed system, for each partition in the managed system, and for the HMC. Configuration change events are collected when a configuration change affecting memory or processor resources occurs for the managed system or for a partition. Configuration change events are also collected when the local time is changed on the HMC.

Utility CoD processor usage events are collected for the managed system when a Utility CoD processor minute is used. All Utility CoD processor minutes used during a single minute are grouped into one event.

Hourly sampling events and all state change, configuration change, and Utility CoD processor usage events collected are only saved on the HMC for about 2 months. Daily sampling events are saved for about 2 years, and monthly sampling events are saved for about 10 years.

Utilization data collection for managed systems is not automatically enabled. The **chlparutil** command can be used to enable utilization data collection.

## Options

- r** The type of system resources for which events are to be listed. Valid values are **hmc** for HMC, **lpar** for partitions, **pool** for shared processor pools, **sys** for managed system, **all** for HMC, partitions, shared processor pools, and managed system, and **config** for HMC configuration settings for utilization data collection.
- m** The name of the managed system for which the collected utilization data or the HMC configuration settings is to be listed. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name, or if the HMC does not currently have a connection to the managed system.  
  
If this option is specified when listing HMC configuration settings, then the HMC configuration settings for the managed-system will be listed. Otherwise, the HMC configuration settings for all of the systems currently managed by this HMC, and for all of the systems for which utilization data has been previously collected by this HMC will be listed.
- d** The number of days prior to today for which events will be listed. Events that were collected today will be listed, along with events that were collected during the past *number-of-days* days.

- This option cannot be specified with the **-h**, **--startyear**, **--startmonth**, **--startday**, **--starthour**, **--endyear**, **--endmonth**, **--endday**, or **--endhour** options.
- h** The number of hours prior to the current hour for which events will be listed. Events that were collected during the current hour will be listed, along with events that were collected during the past *number-of-hours* hours.
- This option cannot be specified with the **-d**, **--startyear**, **--startmonth**, **--startday**, **--starthour**, **--endyear**, **--endmonth**, **--endday**, or **--endhour** options.
- startyear** The starting year for which events will be listed. The default value for this option is **1970**.
- This option cannot be specified with the **-d** or **-h** options.
- startmonth** The starting month for which events will be listed. Valid values are **1** for January through **12** for December. The default value for this option is **1** (January).
- This option cannot be specified with the **-d** or **-h** options.
- startday** The starting day for which events will be listed. Valid values are **1** through **31**. The default value for this option is **1**.
- This option cannot be specified with the **-d** or **-h** options.
- starthour** The starting hour for which events will be listed. Valid values are **0** for midnight through **23** for 11:00 pm. The default value for this option is **0** (midnight).
- This option cannot be specified with the **-d** or **-h** options.
- endyear** The ending year for which events will be listed. The default value for this option is now.
- This option cannot be specified with the **-d** or **-h** options.
- endmonth** The ending month for which events will be listed. Valid values are **1** for January through **12** for December. The default value for this option is now.
- This option cannot be specified with the **-d** or **-h** options.
- endday** The ending day for which events will be listed. Valid values are **1** through **31**. The default value for this option is now.
- This option cannot be specified with the **-d** or **-h** options.
- endhour** The ending hour for which events will be listed. Valid values are **0** for midnight through **23** for 11:00 pm. The default value for this option is now.
- This option cannot be specified with the **-d** or **-h** options.
- n** The maximum number of events to be listed, starting with the most recent event. The number specified must be greater than 0.
- If this option is not specified, and neither are any of the **-d**, **-h**, **--startyear**, **--startmonth**, **--startday**, **--starthour**, **--endyear**, **--endmonth**, **--endday**, or **--endhour** options, then only the most recent event will be listed.
- s** Use this option to specify which type of utilization data is to be listed. Valid values are **h** for hourly sampling events and all state change, configuration change, and Utility CoD processor usage events, **d** for daily sampling events, and **m** for monthly sampling events.

If this option is not specified, then hourly sampling events and all state change, configuration change, and Utility CoD processor usage events will be listed.

**--filter** The filter(s) to apply to the events to be listed. Filters are used to select which events for the specified resource type are to be listed.

The filter data consists of filter name/value pairs, which are in comma separated value (CSV) format. The filter data must be enclosed in double quotes.

The format of the filter data is as follows:

*"filter-name=value,filter-name=value,..."*

Note that certain filters accept a comma separated list of values, as follows:

*""filter-name=value,value,...",..."*

When a list of values is specified, the filter name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a '\ ' character.

Multiple values can be specified for each filter.

Valid filter names for this command:

**lpar\_ids**

Specify partition ID(s)

**lpar\_names**

Specify partition user-defined name(s)

**event\_types**

Specify one or more of the values:

**sample, state\_change, config\_change, utility\_cod\_proc\_usage**

Valid filters with **-r hmc**:

**event\_types**

Valid filters with **-r lpar**:

**event\_types, lpar\_ids | lpar\_names**

Valid filters with **-r pool**:

**event\_types**

Valid filters with **-r sys**:

**event\_types**

Valid filters with **-r all**:

**event\_types, lpar\_ids | lpar\_names**

The **lpar\_ids** and **lpar\_names** filter will only apply to partition events

**-F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each event. If no attribute names are specified, then values for all of the attributes for each event will be displayed.

When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.

This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.

Command attributes:

**borrowed\_pool\_proc\_units**

Processing units that are being borrowed from powered off partitions with dedicated processors.

**capped\_cycles**

The number of capped processing cycles utilized by this partition since the managed system was started.

**configurable\_pool\_proc\_units**

The number of configurable processing units in the shared processor pool.

**configurable\_sys\_mem**

The amount of configurable system memory (in megabytes).

**configurable\_sys\_proc\_units**

The number of configurable system processing units.

**curr\_5250\_cpw\_percent**

The 5250 CPW percent assigned to the partition.

**curr\_avail\_5250\_cpw\_percent**

The 5250 CPW percent available to be assigned to partitions.

**curr\_avail\_pool\_proc\_units**

The number of processing units available to be assigned to partitions.

**curr\_avail\_sys\_mem**

The amount of memory (in megabytes) available to be assigned to partitions.

**curr\_avail\_sys\_proc\_units**

The number of processing units available to be assigned to partitions.

**curr\_mem**

The amount of memory (in megabytes) assigned to the partition.

**curr\_proc\_mode**

The processing mode for the partition. Possible values are **ded** or **shared**.

**curr\_proc\_units**

The number of processing units assigned to the partition.

**curr\_procs**

The number of processors or virtual processors assigned to the partition.

**curr\_sharing\_mode**

The sharing mode of the partition. Possible values are **keep\_idle\_procs**, **share\_idle\_procs**, **share\_idle\_procs\_active**, **share\_idle\_procs\_always**, **cap**, or **uncap**.

**curr\_uncap\_weight**

The current weighted average of processing priority when in uncapped sharing mode. The smaller the value, the lower the weight. Possible values are 0 - 255.

**entitled\_cycles**

The number of processing cycles to which the partition has been entitled since the managed system was started. This value is based on the number of processing units assigned to the partition, and may be greater than or smaller than the number of cycles actually used.

**event\_type**  
The type of event. Possible values are **sample**, **state\_change**, **config\_change**, or **utility\_cod\_proc\_usage**.

**lpar\_id**  
The unique integer identifier for the partition.

**lpar\_name**  
The user-defined name of the partition at the time the event was collected.

**name** The user-defined name of the managed system.

**prev\_time**  
The time on the HMC when the HMC time was changed.

**proc\_cycles\_per\_second**  
Processing cycles per second on one physical processor. This value is static for a particular managed system.

**resource\_type**  
The type of system resource for which the event was collected. Possible values are **hmc**, **lpar**, **pool**, or **sys**.

**sample\_rate**  
The rate, in seconds, at which samples are obtained. This rate can be changed with the **chlpoutil** command.

**shared\_cycles\_while\_active**  
The number of dedicated processing cycles shared by this partition while it has been active since the managed system was started.

**shared\_proc\_pool\_id**  
The unique integer identifier for the shared processor pool.

**state** For system events, this is the state of the managed system at the time the event was collected. For partition events, this is the state of the partition at the time the event was collected.

**sys\_firmware\_mem**  
Amount of memory, in megabytes, on the managed system that is being used by system firmware.

**sys\_time**  
The time on the managed system that the sample was taken.

**time** The time on the HMC that the event was collected.

**time\_cycles**  
The number of time cycles since the managed system was started.

**time\_shut\_down**  
The time the HMC was shut down or rebooted.

**total\_pool\_cycles**  
The total number of processing cycles available in the shared processor pool since the managed system was started.

**type\_model\_serial\_num**  
The machine type, model, and serial number of the managed system.

**uncapped\_cycles**  
The number of uncapped processing cycles utilized by this partition since the managed system was started.

**unreported\_proc\_min**

The total number of Utility CoD processor minutes that have not been reported.

**used\_proc\_min**

The number of Utility CoD processor minutes that were used during the last minute.

**utilized\_pool\_cycles**

The number of processing cycles in the shared processor pool that have been utilized since the managed system was started.

**--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

## lsmediadev

List storage media devices.

### Synopsis

**lsmediadev** [-F *[attribute-names]*] [--header]] [--help]

### Description

**lsmediadev** lists the storage media devices that are available for use on the Hardware Management Console (HMC).

### Options

**-F** A delimiter separated list of attribute names for the desired attribute values to be displayed. If no attribute names are specified, then values for all of the attributes will be displayed.

When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.

This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.

**--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

## lsrefcode

List reference codes.

### Synopsis

**lsrefcode -r** {sys | lpar} **-m** *managed-system* [-s {p | s}] [-n *number*] [--filter "*filter-data*"] [-F *[attribute-names]*] [--header]] [--help]

### Description

**lsrefcode** lists reference codes for the *managed-system* or for partitions in the *managed-system*.

## Options

- r** The type of reference codes to list. Valid values are **sys** for managed system reference codes, and **lpar** for partition reference codes.
- m** The name of the managed system which has the reference codes to list. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- s** When listing managed system reference codes, use this option to specify the service processor for which reference codes are to be listed. Valid values are **p** for the primary service processor and **s** for the secondary service processor. If this option is not specified, reference codes for the primary service processor will be listed.

This option is only valid when listing managed system reference codes.
- n** The number of reference codes to list, starting with the current reference code, for the *managed-system* or for each partition. Reference codes are listed in order, with the most recent (current) reference code first.

The *number* specified must be greater than 0. If there are fewer reference codes available than *number*, only the available reference codes will be listed.

If this option is omitted, only the current reference code will be listed.
- filter** The filter to apply to the partition reference codes to be listed. A filter is used to select the partitions for which reference codes are to be listed. If no filter is specified, then reference codes for all partitions in the *managed-system* will be listed.

The filter data consists of filter name/value pairs, which are in comma separated value (CSV) format. The filter data must be enclosed in double quotes.

The format of the filter data is as follows:

```
filter-name=value,filter-name=value,...<LF>
```

Note that certain filters accept a comma separated list of values, as follows:

```
"filter-name=value,value,...",...<LF>
```

When a list of values is specified, the filter name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a `'\'` character.

Valid filter names for this command are **lpar\_names** or **lpar\_ids**. Only one of these filters may be specified. Multiple partitions can be specified with the filter.

This option is not valid when listing managed system reference codes.
- F** A delimiter separated list of attribute names for the desired attribute values to be displayed. If no attribute names are specified, then values for all of the attributes will be displayed.

When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.

This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.



#### **--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

---

## **Issacfg**

List Service Agent configuration information.

### **Synopsis**

**Issacfg -t {email | ftpfirewall | ftpoffload | snmp | snmptrapnames} [-F [attribute-names] [--header]] [--help]**

### **Description**

**Issacfg** lists Service Agent configuration information.

### **Options**

- t** The type of Service Agent configuration information to list. Valid values are **email** for customer email notification settings, **ftpfirewall** for FTP firewall settings, **ftpoffload** for FTP offload server settings, **snmp** for SNMP trap notification settings, and **snmptrapnames** to list all defined SNMP traps.
- F** A delimiter separated list of attribute names representing the desired attribute values to display. If this option is specified without any attribute names, then all of the attributes will be displayed.
- When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.
- This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.
- header** Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.
- help** Display the help text for this command and exit.

---

## **Issvcevents**

List console or serviceable events.

### **Synopsis**

**Issvcevents -t {console | hardware} [-d number-of-days | -i number-of-minutes] [-m managed-system] [--filter "filter-data"] [-F [attribute-names] [--header]] [--help]**

### **Description**

**Issvcevents** lists console events logged by the Hardware Management Console (HMC), or serviceable events.

### **Options**

- t** The type of events to list. Valid values are **console** for console events, or **hardware** for serviceable events.
  
- d** The number of days prior to today for which events will be listed. Events that occurred today will be listed, along with any events that occurred during the past *number-of-days* days.  
 If this option is omitted when listing console events, console events that occurred within the past 7 days will be listed.  
 If this option is omitted when listing serviceable events, all serviceable events will be listed.
  
- i** The number of minutes to go back and search for events. This search is based on the time that the event was initially created on the HMC, and is not affected by later updates to the event.
  
- m** The name of the managed system for which serviceable events are to be listed. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.  
 If this option is omitted, all serviceable events will be listed.  
 This option is only valid when listing serviceable events.
  
- filter** The filter to apply to the serviceable events to be listed. A filter is used to select which serviceable events are to be listed. For example, only open serviceable events can be listed by using a filter to specify the status (open) of the serviceable events to list. If a filter is not used, then all serviceable events will be listed.  
 The filter data consists of filter name/value pairs, which are in comma separated value (CSV) format. The filter data must be enclosed in double quotes.  
 The format of the filter data is as follows:  

```
"filter-name=value,filter-name=value,..."
```

 Note that certain filters accept a comma separated list of values, as follows:  

```
""filter-name=value,value,...",..."
```

 When a list of values is specified, the filter name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a `'\'` character.  
 Multiple values can be specified for each filter.  
 Valid filter names for serviceable events:  
**problem\_nums** Specify event problem number(s)  
**status** Specify event status. Valid values are **open** or **closed**.  
 This option is not valid when listing console events.
  
- F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each event. If no attribute names are specified, then values for all of the attributes for each event will be displayed.  
 When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.  
 This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.

### **--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

---

## **lssyscfg**

List system resources.

### **Synopsis**

```
lssyscfg -r {lpar | prof | sys | sysprof | cage | frame} [-m managed-system | -e managed-frame] [--filter "filter-data"] [-F [attribute-names]] [--header] [--help]
```

### **Description**

**lssyscfg** lists the attributes of partitions, partition profiles, or system profiles for the *managed-system*. It can also list the attributes of the *managed-system*, and of all of the systems managed by this Hardware Management Console (HMC).

**lssyscfg** can also list the attributes of cages in the *managed-frame*, the attributes of the *managed-frame*, or the attributes of all of the frames managed by this HMC.

### **Options**

**-r** The type of resources to list. Valid values are **lpar** for partitions, **prof** for partition profiles, **sys** for managed systems, **sysprof** for system profiles, **cage** for managed frame cages, and **frame** for managed frames.

**-m** The name of either the managed system to list, or the managed system which has the system resources to list. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.

This option is required when listing partitions, partition profiles, or system profiles. This option is optional when listing managed systems, and if it is omitted, then all of the systems managed by this HMC will be listed. This option is not valid when listing managed frame cages or managed frames.

**-e** The name of either the managed frame to list, or the managed frame which contains the cages to list. The name may either be the user-defined name for the managed frame, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the type, *mmm* is the model, and *sssssss* is the serial number of the managed frame. The *ttt-mmm\*sssssss* form must be used if there are multiple managed frames with the same user-defined name.

This option is required when listing managed frame cages. This option is optional when listing managed frames, and if it is omitted, then all of the frames managed by this HMC will be listed. This option is not valid when listing partitions, partition profiles, system profiles, or managed systems.

**--filter** The filter(s) to apply to the resources to be listed. Filters are used to select which resources of the specified resource type are to be listed. If no filters are used, then all of the resources of the specified resource type will be listed. For example, specific partitions can be listed by using a filter to specify the names or IDs of the partitions to list. Otherwise, if no filter is used, then all of the partitions in the managed system will be listed.

The filter data consists of filter name/value pairs, which are in comma separated value (CSV) format. The filter data must be enclosed in double quotes.

The format of the filter data is as follows:

*"filter-name=value,filter-name=value,..."*

Note that certain filters accept a comma separated list of values, as follows:

*"filter-name=value,value,...",..."*

When a list of values is specified, the filter name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a `'\'` character. Multiple values can be specified for each filter.

Valid filter names for partitions:

**lpar\_names | lpar\_ids | work\_groups**

Only one of these three filters may be specified.

Valid filter names for partition profiles:

**lpar\_names | lpar\_ids, profile\_names**

Valid filter names for system profiles:

**profile\_names**

This option is not valid when listing managed systems, managed frame cages, or managed frames.

**-F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each resource. If no attribute names are specified, then values for all of the attributes for the resource will be displayed.

When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.

This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.

**--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

---

## Issysconn

List system connections.

### Synopsis

**Issysconn -r all [-F *[attribute-names]*] [--header]] [--help]**

### Description

**lssysconn** lists connection information for all of the systems and frames managed by this Hardware Management Console (HMC). Connection information for all systems and frames to which this HMC is connected or attempting to connect is listed.

## Options

- r** The type of resources for which to list connection information. The only valid value is **all** for all managed systems and managed frames.
  - F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each resource. If no attribute names are specified, then values for all of the attributes for the resource will be displayed.  
  
When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.  
  
This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.
  - header** Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.
  - help** Display the help text for this command and exit.
- 

## lssysplan

List system plans.

## Synopsis

**lssysplan** [-F *[attribute-names]*] [--header] [--help]

## Description

**lssysplan** lists the system plan files in the system plan file directory on the Hardware Management Console (HMC).

## Options

- F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each file. If no attribute names are specified, then values for all of the attributes for each file will be displayed.  
  
When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.  
  
This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.  
  
The possible attributes that can be listed are: **name**, **description**, **source**, **version**, and **date**.
- header** Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.
- help** Display the help text for this command and exit.

---

## Issysplanres

List system plan resources.

### Synopsis

**Issysplanres -r osinstall [-F [attribute-names][--header]] [--help]**

### Description

**Issysplanres** lists the system plan resources that are defined on this Hardware Management Console (HMC). These resources can be used when deploying system plans from this HMC.

### Options

- r** The type of system plan resources to list. The only valid value is **osinstall** for operating system installation resources.
- F** A delimiter separated list of attribute names for the desired attribute values to be displayed for each system plan resource. If no attribute names are specified, then values for all of the attributes for each system plan resource will be displayed.  
  
When this option is specified, only those specified attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.  
  
This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.
- header** Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.
- help** Display the help text for this command and exit.

---

## Isvet

List Capacity on Demand advanced functions activation information.

### Synopsis

**Isvet -t {code | hist} -m managed-system [-F [attribute-names] [--header]] [--help]**

### Description

**Isvet** lists Capacity on Demand (CoD) advanced functions activation information for the *managed-system*. CoD advanced functions include Advanced POWER Virtualization and Enterprise Enablement.

CoD advanced functions are sometimes referred to as Virtualization Engine systems technologies.

### Options

- t** The type of information to list. Valid values are **code** for information used to generate CoD advanced functions activation codes, and **hist** for the CoD advanced functions activation history log.
- m** The name of the managed system for which information is to be listed. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmmm\*ssssssss*, where *tttt* is

the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.

**-F** A delimiter separated list of attribute names representing the desired attribute values to display. If this option is specified without any attribute names, then all of the attributes will be displayed.

When this option is specified, only attribute values will be displayed. No attribute names will be displayed. The attribute values displayed will be separated by the delimiter which was specified with this option.

This option is useful when only attribute values are desired to be displayed, or when the values of only selected attributes are desired to be displayed.

**--header**

Display a header record, which is a delimiter separated list of attribute names for the attribute values that will be displayed. This header record will be the first record displayed. This option is only valid when used with the **-F** option.

**--help** Display the help text for this command and exit.

---

## migrcfg

Migrate configuration.

### Synopsis

**migrcfg -m** *managed-system* **-t 1 -f** *file* [**--help**]

### Description

**migrcfg** migrates partition configuration data to a *managed-system*.

### Options

**-m** The name of the managed system to which to migrate the partition configuration data. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss* where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.

**-t** The migration data type. The only valid value is **1**.

**-f** The name of the file on floppy diskette that contains the partition configuration data to migrate.

**--help** Display the help text for this command and exit.

---

## mkaccfg

Create access control object.

### Synopsis

**mkaccfg -t** {**resourcerole** | **taskrole**} **-f** *configuration-file* | **-i** "*configuration-data*" [**--help**]

### Description

**mkaccfg** creates a new access control role.

### Options

**-t** The type of access control role to create. Valid values are **resourcerole** for managed resource role and **taskrole** for task role.

**-f** The name of the file containing the configuration data needed to create the access control role. The configuration data consists of attribute name/value pairs, which are in comma separated value (CSV) format. These attribute name/value pairs form a configuration record. A line feed marks the end of a configuration record. There can only be one configuration record in the file.

The format of a configuration record is as follows:

*attribute-name=value,attribute-name=value,...<LF>*

Note that certain attributes accept a comma separated list of values, as follows:

*"attribute-name=value,value,...",...<LF>*

When a list of values is specified, the attribute name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a `'\'` character.

Attribute names for managed resource roles (all attributes are required):

**name** name of the managed resource role to create

**resources**

comma separated list of managed resource objects

Attribute names for task roles (all attributes are required):

**name** name of the task role to create

**resources**

comma separated list of tasks

**parent** name of the parent task role on which to base this task role. Valid values are **hmcsuperadmin**, **hmcoperator**, **hmcviewer**, **hmcpe**, **hmcserVICerep**, or a user-defined task role.

The **-f** and the **-i** options are mutually exclusive.

**-i** This option allows you to enter configuration data on the command line, instead of using a file. Data entered on the command line must follow the same format as data in a file, and must be enclosed in double quotes.

The **-i** and the **-f** options are mutually exclusive.

**--help** Display the help text for this command and exit.

---

## mkhmcusr

Create a Hardware Management Console user.

### Synopsis

**mkhmcusr -u user-name -a task-role [-d description] [--passwd password] [-M number-of-days] [--help]**

### Description

**mkhmcusr** creates a Hardware Management Console (HMC) user.

### Options

**-u** The user name of the HMC user to create. The user name cannot be longer than 32 characters, and it must begin with a letter.



- a** The access control task role for this user. Valid values are **hmcsuperadmin**, **hmcoperator**, **hmcviewer**, **hmcpe**, **hmcserviceprep**, or a user-defined task role.
- d** The description for this user. *description* can be any string. If this option is not specified, then the description for this user will be set to "HMC User".
- passwd** The password for this user. If this option is omitted, you will be prompted to enter the password. The password must be at least 7 characters in length.
- M** The number of days until the password for this user expires. If this option is not specified, then this user's password will never expire.
- help** Display the help text for this command and exit.

---

## mksyscfg

Create system resources.

### Synopsis

```
mksyscfg -r {lpar | prof | sysprof} -m managed-system [{-f configuration-file | -i"configuration-data"}] [-o save {-p partition-name | --id partition-ID} [-n profile-name] [--help]
```

### Description

**mksyscfg** creates partitions, partition profiles, or system profiles for the *managed-system*.

**mksyscfg** can be used to save the current configuration of a partition to a new partition profile.

### Options

- r** The type of system resources to create. Valid values are **lpar** for partitions, **prof** for partition profiles, and **sysprof** for system profiles.  
When a partition is created, the default profile for the partition is also created.
- m** The name of the managed system for which the system resources are to be created. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- f** The name of the file containing the configuration data needed to create the system resources. The configuration data consists of attribute name/value pairs, which are in comma separated value (CSV) format. These attribute name/value pairs form a configuration record. A line feed marks the end of a configuration record. The file must contain one configuration record for each resource to be created, and each configuration record must be for the same resource type.  
The format of a configuration record is as follows:  
*attribute-name=value,attribute-name=value,...<LF>*  
Note that certain attributes accept a comma separated list of values, as follows:  
*"attribute-name=value,value,...",...<LF>*  
When a list of values is specified, the attribute name/value pair must be enclosed in double quotes. Depending on the shell being used, nested double quote characters may need to be preceded by an escape character, which is usually a `'\'` character.  
Attribute names for partitions (see below for attribute names that are common to both partitions and partition profiles):

**name** name of the partition to create

**[lpar\_id]**

**profile\_name**

name of the default profile to create

**lpar\_env**

Valid values are **aixlinux**, **os400**, or **vioserver**

**[shared\_proc\_pool\_util\_auth]**

Valid values are:

**0** - do not allow authority

**1** - allow authority

Attribute names for partition profiles (see below for attribute names that are common to both partition profiles and partitions):

**name** name of the partition profile to create

**lpar\_name | lpar\_id**

name or ID of the partition for which to create the profile

Attribute names for both partitions and partition profiles:

**[all\_resources]**

Valid values are:

**0** - do not use all the managed system resources

**1** - use all the managed system resources (this option is not valid for i5/OS partitions on IBM System p5 or eServer p5 servers)

**min\_mem**

megabytes

**desired\_mem**

megabytes

**max\_mem**

megabytes

**[min\_num\_huge\_pages]**

AIX and Linux only

**[desired\_num\_huge\_pages]**

AIX and Linux only

**[max\_num\_huge\_pages]**

AIX and Linux only

**[proc\_model]**

Valid values are:

**ded** - dedicated processors

**shared** - shared processors

**[min\_procs]**

**[desired\_procs]**

**max\_procs]**

**[min\_proc\_units]**

**[desired\_proc\_units]**

**[max\_proc\_units]**

**min\_520\_cpw\_percent**

Only valid for i5/OS partitions in managed systems that support the assignment of 5250 CPW percentages

**[desired\_5250\_cpw\_percent]**

Only valid for i5/OS partitions in managed systems that support the assignment of 5250 CPW percentages

**[max\_5250\_cpw\_percent]**

Only valid for i5/OS partitions in managed systems that support the assignment of 5250 CPW percentages

**[sharing\_mode]**

Valid values for partitions using dedicated processors are:

**keep\_idle\_procs**

nev er share processors

**share\_idle\_procs**

share processors only when partition is inactive

**share\_idle\_procs\_active**

share processors only when partition is active (POWER6 servers only)

**share\_idle\_procs\_always**

always share processors (POWER6 servers only)

Valid values for partitions using shared processors are:

**cap** - capped

**uncap** - uncapped

**[uncap\_weight]**

**[io\_slots]**

Comma separated list of I/O slots, with each I/O slot having the following format:

*slot-DRC-index/slot-IO-pool-ID/ is-required*

Both '/' characters must be present, but optional values may be omitted. Optional values are *slot-IO-pool-ID*.

Valid values for *is-required*:

0 - no

1 - yes

**[lpar\_io\_pool\_ids]**

comma separated

**[load\_source\_slot]**

i5/OS only, required on POWER5 servers DRC index of I/O slot, or virtual slot number

**[alt\_restart\_device\_slot]**

i5/OS only, DRC index of I/O slot, or virtual slot number

**console\_slot**

i5/OS only, DRC index of I/O slot, DRC index of HEA logical port (POWER6 servers only), virtual slot number, or the value **hmc**

**[alt\_console\_slot]**

i5/OS only, DRC index of I/O slot

**[op\_console\_slot]**

i5/OS only, DRC index of I/O slot

**[auto\_start]**

Valid values are:

0 - off

1 - on

**[boot\_mode]**

AIX, Linux, and virtual I/O server only

Valid values are:

**norm** - normal

**dd** - diagnostic with default boot list

**ds** - diagnostic with stored boot list

**of** - Open Firmware OK prompt

**sms** - System Management Services

**[power\_ctrl\_lpar\_ids | power\_ctrl\_lpar\_names]**

comma separated

**[conn\_monitoring]**

Valid values are:

0 - off

1 - on

**[hsl\_pool\_id]**

AIX, Linux, and virtual I/O server only

Valid values are:

0 - HSL OptiConnect is disabled

1 - HSL OptiConnect is enabled

**[virtual\_opti\_pool\_id]**

AIX, Linux, and virtual I/O server only

Valid values are:

0 - virtual OptiConnect is disabled

1 - virtual OptiConnect is enabled

**[max\_virtual\_slots]**

**[virtual\_eth\_adapters]**

Comma separated list of virtual ethernet adapters, with each adapter having the following format:

*virtual-slot-number/is-IEEE/ port-vlan-ID/additional-vlan-IDs/ trunk-priority/is-required*

All 5 '/' characters must be present, but optional values may be omitted. Optional values are *additional-vlan-IDs* and *trunk-priority*.

Valid values for *is-IEEE* and *is-required*:

0 - no

1 - yes

Valid values for *trunk priority*:

0 - this adapter is not a trunk adapter

1 - 15 - this adapter is a trunk adapter with the specified priority

**[virtual\_scsi\_adapters]**

Comma separated list of virtual SCSI adapters, with each adapter having the following format:

*virtual-slot-number/client-or-server/remote-lpar-ID/remote-lpar-name/remote-slot-number/is-required*

All 5 '/' characters must be present, but optional values may be omitted. Optional values for server adapters are *remote-lpar-ID*, *remote-lpar-name*, and *remote-slot-number*. Optional values for client adapters are *remote-lpar-ID* or *remote-lpar-name* (one of those values is required, but not both).

Valid values for *client-or-server*:

**client**

**server**

Valid values for *is-required*:

0 - no

1 - yes

**[virtual\_serial\_adapters]**

Comma separated list of virtual serial adapters, with each adapter having the following format:

*virtual-slot-number/client-or-server/supports-HMC/remote-lpar-ID/remote-lpar-name/remote-slot-number/is-required*

All 6 '/' characters must be present, but optional values may be omitted. Optional values for server adapters are *supports-HMC*, *remote-lpar-ID*, *remote-lpar-name*, and

*remote-slot-number*. Optional values for client adapters are *remote-lpar-ID* or *remote-lpar-name* (one of those values is required, but not both), and the *supports-HMC* value is not allowed.

Valid values for *client-or-server*:

- client**
- server**

Valid values for *supports-HMC*:

- 0** - no

Valid values for *is-required*:

- 0** - no
- 1** - yes

#### **[hca\_adapters]**

AIX, Linux, and virtual I/O server only

Comma separated list of Host Channel adapters (HCA), with each adapter having the following format:

*adapter-ID/GUID/capability*

All 3 values must be specified for each adapter.

Valid values for *capability*:

- 1** - low
- 2** - medium
- 3** - high
- 4** - dedicated

#### **[lhea\_logical\_ports]**

POWER6 servers only

Comma separated list of Logical Host Ethernet adapter (LHEA) logical ports, with each logical port having the following format:

*adapter-ID/port-group/physical-port-ID/ logical-port-ID/allowed-VLAN-IDs*

All 4 '/' characters must be present, but optional values may be omitted. Optional values are *allowed-VLAN-IDs*.

#### **[lhea\_capabilities]**

POWER6 servers only Comma separated list of LHEA capabilities, with each capability having one of the following formats:

*adapter-ID/capability*

or

*adapter-ID/5/ieq/nieq/qc/cq/mr*

where *ieq* (interruptible event queues), *niesq* (non-interruptible event queues), *qp* (queue pairs), *cq* (completion queues), and *mr* (memory regions) each specify the resource amount in addition to the base minimum.

Valid values for *capability*:

- 0** - base minimum
- 1** - low
- 2** - medium
- 3** - high
- 4** - dedicated

#### **[sni\_device\_ids]**

AIX, Linux, and virtual I/O server only

Comma separated list of Switch Network Interface (SNI) adapter device IDs

[**work\_group\_id**]

[**redundant\_err\_path\_reporting**]

Valid values are:

0 - disable

1 - enable

[**electronic\_err\_reporting**]

i5/OS only, POWER6 servers only

Valid values are:

0 - disable

1 - enable

[**lpar\_proc\_compat\_mode**]

POWER6 servers only

Valid values are:

**default** - default architected processor mode

**POWER6\_enhanced** - POWER6 enhanced processor mode

Attribute names for system profiles:

**name** name of the system profile to create

**lpar\_names** | **lpar\_ids**

comma separated

**profile\_names**

comma separated

Brackets around an attribute name indicate that the attribute is optional.

The **-f** and the **-i** options are mutually exclusive.

Configuration data is required to be specified with this option or the **-i** option except when **-o save** is specified to save the current configuration of a partition to a new partition profile. This option is not valid when **-o save** is specified.

- i** This option allows you to enter configuration data on the command line, instead of using a file. Data entered on the command line must follow the same format as data in a file, and must be enclosed in double quotes.

When this option is used, only a single system resource can be created.

The **-i** and the **-f** options are mutually exclusive.

Configuration data is required to be specified with this option or the **-f** option except when **-o save** is specified to save the current configuration of a partition to a new partition profile. This option is not valid when **-o save** is specified.

- o** The operation to perform. The only valid value is **save** to create a new partition profile by saving the current configuration of a partition.

If this option is not specified, then new system resources will be created using the configuration data specified with the **-f** or **-i** option.

- p** The name of the partition whose current configuration is to be saved to a new partition profile.

You can either use this option to specify the name of the partition whose current configuration is to be saved, or use the **--id** option to specify the partition's ID. The **-p** and the **--id** options are mutually exclusive.

A partition is required to be specified with this option or the **--id** option when **-o save** is specified to save the current configuration of a partition to a new partition profile. This option is not valid otherwise.

- id** The ID of the partition whose current configuration is to be saved to a new partition profile. You can either use this option to specify the ID of the partition whose current configuration is to be saved, or use the **-p** option to specify the partition's name. The **--id** and the **-p** options are mutually exclusive.
- A partition is required to be specified with this option or the **-p** option when **-o save** is specified to save the current configuration of a partition to a new partition profile. This option is not valid otherwise.
- n** The name of the new partition profile to which to save the partition configuration.
- This option is required when **-o save** is specified to save the current configuration of a partition to a new partition profile. This option is not valid otherwise.
- help** Display the help text for this command and exit.

---

## mksysconn

Create system connection.

### Synopsis

```
mksysconn --ip IP-address [-r {sys | frame}] [--passwd password] [--help]
```

### Description

**mksysconn** establishes a connection from the Hardware Management Console (HMC) to a system in the network and adds the system to the systems managed by the HMC. If a connection to the system cannot be established because the network is down, the service processor for the system is down, or too many other HMCs have already established a connection to the system, the system will be added as a managed system which is in the No Connection state.

**mksysconn** can also establish a connection from the HMC to a frame in the network and add the frame to the frames managed by the HMC. If a connection to the frame cannot be established because the network is down, the bulk power assembly (BPA) for the frame is down, or too many other HMCs have already established a connection to the frame, the frame will be added as a managed frame which is in the No Connection state.

**If your HMC is set up as a DHCP server on a private network, do not use this command to establish HMC connections to managed systems and frames that are DHCP clients. This command is intended for use on a public network only, where the systems are set to use static IP addresses. Using this command in a DHCP environment establishes a temporary connection that will not continue to work properly over network configuration changes, system power loss, and service repair actions.**

### Options

- ip** To connect to a system and add the system to the systems managed by the HMC, specify the IP address or host name of the service processor for the system.
- To connect to a frame and add the frame to the frames managed by the HMC, specify the IP address or host name of one side of the bulk power assembly (BPA) for the frame. Note that to properly connect to a frame, it is recommended that you issue this command twice, once for each side of the BPA, in order to connect to both sides of the BPA for the frame.
- r** The type of resource to which to connect and add to the HMC. Valid values are **sys** for system and **frame** for frame. If this option is omitted, then the resource to which to connect and add to the HMC is assumed to be a system.

**--passwd**

The HMC Access password for the system or the frame to which to connect. If this option is omitted, you will be prompted to enter the password.

**--help** Display the help text for this command and exit.

---

## mksysplan

Make system plan file.

### Synopsis

**mksysplan -f file-name -m managed-system [--check] [-d "description"] [-o noprobe] [-v] [--help]**

### Description

**mksysplan** creates a system plan file that represents the information known about a managed system's hardware, partitions, profiles, and partition provisioning information.

### Options

**-f** Specifies the file name that will contain the system plan created by this command. If the file does not exist, it will be created in the system plan file directory on the Hardware Management Console (HMC). If the file exists, its contents will be overwritten unless the **--check** option is specified.

The file name is restricted to the alphanumeric characters (upper and lower case) and a set of special characters (comma, period, hyphen, underscore, and space). The file name cannot begin with a period or hyphen.

The file name must end with the **.sysplan** suffix.

**-m** Specifies the managed system's name that will be used to get the information to create the system plan file.

The name may either be the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.

**--check**

Specifies that this command should check the system plan directory and fail with an error if the file with the name specified with the **-f** option already exists.

**-d** Specifies a description that will be added to the created file.

**-o** Specifies the options for inventory collection. The only valid value is **noprobe**. When **noprobe** is specified, the inventory gathered will be limited to that of just the PCI slot devices without any further inventory probes. Specify **noprobe** if just PCI devices are desired.

**-v** Display verbose output during command processing, in addition to the default messages.

**--help** Display the help text for this command and exit.



---

## mkvterm

Open a virtual terminal session.

### Synopsis

**mkvterm** **-m** *managed-system* **{-p** *partition-name* **| --id** *partition-ID***}** **[--help]**

### Description

**mkvterm** opens a virtual terminal session for an AIX, Linux, or virtual I/O server partition.

After establishing a virtual terminal session, the ~ character sequence can be entered in the terminal window to terminate it, or the **rmvterm** command can be used to force the session to be closed.

A partition can only have one open virtual terminal session at a time.

### Options

- m** The name of the managed system which has the partition for which to open the virtual terminal session. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- p** The name of the partition for which to open the virtual terminal session.  
You must either use this option to specify the name of the partition, or use the **--id** option to specify the partition's ID. The **-p** and the **--id** options are mutually exclusive.
- id** The ID of the partition for which to open the virtual terminal session.  
You must either use this option to specify the ID of the partition, or use the **-p** option to specify the partition's name. The **--id** and the **-p** options are mutually exclusive.
- help** Display the help text for this command and exit.

---

## monhmc

Monitor HMC subsystems and system resources.

### Synopsis

To monitor Hardware Management Console (HMC) subsystems:

**monhmc -s** **{hmcsvr | rmc}** **[-n** *<interval>***]** **[--help]**

To monitor HMC system resources:

**monhmc -r** **{disk | proc | mem | swap}** **[-n** *<interval>***]** **[--help]**

### Description

**monhmc** provides a dynamic real-time view of HMC related subsystems and system resources. The **top**, **watch**, and **df** commands are used to implement this command. Refer to documentation for those commands for additional information.

### Options

- s** The HMC subsystem to monitor. Valid values are **hmcsvr** for HMC server processes, and **rmc** for Resource Monitoring and Control (RMC) processes.  
Either this option or the **-r** option is required. The **-s** and the **-r** options are mutually exclusive.
  - r** The HMC system resource to monitor. Valid values are **disk** for filesystem disk space usage, **proc** for processor (CPU) usage, **mem** for memory usage, and **swap** for swap space usage.  
Either this option or the **-s** option is required. The **-r** and the **-s** options are mutually exclusive
  - n** The interval between updates in seconds. The default value for this option is 4 seconds.  
If an interval of 0 is specified, then statistics are displayed only once, and this command exits. If any other interval is specified, or if this option is omitted, then statistics are updated every interval seconds, and this command runs until interrupted with Ctrl-c.
  - help** Display the help text for this command and exit.
- 

## pedbg

Product Engineering debug tools.

### Synopsis

```
pedbg {-d {on | off} | -j {on | off} | -l {rmc | se} | -c | -s | -q {n} | -r} [--help]
```

### Description

**pedbg** provides debug tools for Product Engineer/Support Personnel. This command requires PE authority to run, i.e, only hscpe user can access this command.

### Options

- d** Turn on or off various debug tracing. This option will restart subsystems to start/stop internal tracing.
- j** Turn on or off Just in Time compiler. Turn off Just in Time compiler will result in loss of performance.
- l** List internal subsystem information. If **rmc** is specified, the list of RMC daemons will be displayed, along with its state. If **se** is specified, the IBM.ServiceEvent resource entries are displayed.
- c** Collect various logs and javacore. This option can copy the data collected onto DVD or leave a zip file in the /dump directory.
- s** Collect various managed system dumps that were sent to the HMC. This option can copy the data collected onto DVD or leave a zip file in the /dump directory.
- q** Collect logs or managed system dumps in quiet mode. Not prompted. Used with either the **-c** or the **-s** option.

Options for log collection:

- 1 = network info only
- 2 = network info + base logs
- 3 = network info + base logs + extended logs
- 4 = all logs - network info + base logs + extended logs + archives
- 5 = collect files in /home/hscpe/ibmsupt only
- 9 = run prompt to copy files to media

Options for managed system dumps:

- 1 collect all system dump types

- 2 collect FSPDUMP
- 3 collect SYSDUMP
- 4 collect LOGDUMP
- 5 collect SMADUMP
- 6 collect PWRDUMP
- 8 delete all system dumps
- 9 = run prompt to copy files to media

- r** Remove the log files collected that are put in /dump.
- help** Display the help text for this command and exit.

---

## pesh

Provides PE Shell access.

### Synopsis

**pesh** <serial number of machine>

### Description

**pesh** provides full shell access to Product Engineer/Support Personnel. **pesh** takes the serial number of the machine where full shell access is requested, then prompts the user for a 1 day password obtained from the support organization. If the password is valid, the user will be granted full shell access. Only user hscpe can access this command.

---

## rmaccfg

Remove access control object.

### Synopsis

**rmaccfg -t** {resource | resourcerole | taskrole} **-n** name **[--help]**

### Description

**rmaccfg** removes an access control role from the Hardware Management Console (HMC), or it removes inactive managed resource objects assigned to an HMC user.

### Options

- t** The type of access control objects to remove. Valid values are resource for inactive managed resource objects, **resourcerole** for a managed resource role, and **taskrole** for a task role.
- n** When removing inactive managed resource objects assigned to an HMC user, use this option to specify the user name of the HMC user from which to remove the inactive objects.  
  
When removing an access control role, use this option to specify the name of the role to remove. Note that the predefined task roles **hmcsuperadmin**, **hmcoperator**, **hmcviewer**, **hmcpe**, and **hmcservicerep** cannot be removed.  
  
If the specified access control role is currently assigned to one or more HMC users, you will be prompted to confirm that you want to remove the role.
- help** Display the help text for this command and exit.

---

## rmhmcusr

Remove a Hardware Management Console user.

### Synopsis

**rmhmcusr** **-u** *user-name* [**--help**]

### Description

**rmhmcusr** removes a Hardware Management Console (HMC) user.

### Options

- u**        The user name of the HMC user to remove. The HMC users **root** and **hscroot** cannot be removed.
- help**   Display the help text for this command and exit.

---

## rmlock

Remove lock.

### Synopsis

**rmlock** **-e** *managed-frame* [**--help**]

### Description

**rmlock** forces a Hardware Management Console (HMC) lock on the *managed-frame* to be released.

### Options

- e**        The name of the managed frame to unlock. The name may either be the user-defined name for the managed frame, or be in the form *tttt-mmmm\*sssssss*, where *tttt* is the type, *mmm* is the model, and *sssssss* is the serial number of the managed frame. The *tttt-mmmm\*sssssss* form must be used if there are multiple managed frames with the same user-defined name.
- help**   Display the help text for this command and exit.

---

## rmlparutil

Remove utilization data.

### Synopsis

**rmlparutil** **-m** *managed-system* [**--help**]

### Description

**rmlparutil** removes the utilization data collected for a managed system from the Hardware Management Console (HMC).

### Options

- m**        The name of the managed system for which collected utilization data is to be removed. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the

managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name, or if the HMC does not currently have a connection to the managed system.

Removing the utilization data for a managed system does not disable the collection of utilization data for that managed system. Use the **chlparutil** command to disable the collection of utilization data.

**--help** Display the help text for this command and exit.

---

## rmprofdata

Remove profile data.

### Synopsis

**rmprofdata -m** *managed-system* **-f** *file* [**--help**]

### Description

**rmprofdata** removes a profile data backup file for the *managed-system*.

### Options

**-m** The name of the managed system for which to remove the profile data backup file. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name, or if the HMC does not currently have a connection to the managed system.

**-f** The name of the profile data backup file to be removed. If *file* is not fully qualified, *file* will be removed from the **/var/hsc/profiles/serial-number** directory on the HMC (*serial-number* is the serial number of the managed system).

To remove profile data from removable media, the media must be present in the removable media device and the device must be mounted with the **mount** command before this command is issued. The **lsmediadev** command can be used to display all of the removable media devices on the HMC.

**--help** Display the help text for this command and exit.

---

## rmsyscfg

Remove a system resource.

### Synopsis

**rmsyscfg -r** {**lpar** | **prof** | **sysprof**} **-m** *managed-system* [**-n** *resource-name*] [**-p** *partition-name*] [**--id** *partition-ID*] [**--help**]

### Description

**rmsyscfg** removes a partition, a partition profile, or a system profile from the *managed-system*.

### Options

**-r** The type of system resource to remove. Valid values are **lpar** for a partition, **prof** for a partition profile, and **sysprof** for a system profile.

When a partition is removed, all of the partition profiles that are defined for that partition are also removed.

When a partition profile is removed, any system profiles that contain just that one partition profile are also removed.

- m** The name of the managed system from which the system resource is to be removed. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name, or if the HMC does not currently have a connection to the managed system.
- n** The name of the system resource to remove.  
  
To remove a partition, you must either use this option to specify the name of the partition to remove, or use the **--id** option to specify the partition's ID. The **-n** and the **--id** options are mutually exclusive when removing a partition.  
  
To remove a partition profile or a system profile, you must use this option to specify the name of the profile to remove.
- p** The name of the partition which has the partition profile to remove. This option is only valid when removing a partition profile.  
  
To remove a partition profile, you must either use this option to specify the name of the partition which has the partition profile to remove, or use the **--id** option to specify the partition's ID. The **-p** and the **--id** options are mutually exclusive.
- id** The partition's ID.  
  
To remove a partition, you must either use this option to specify the ID of the partition to remove, or use the **-n** option to specify the partition's name. The **--id** and the **-n** options are mutually exclusive when removing a partition.  
  
To remove a partition profile, you must either use this option to specify the ID of the partition that has the profile to remove, or use the **-p** option to specify the partition's name. The **--id** and the **-p** options are mutually exclusive when removing a partition profile.  
  
This option is not valid when removing a system profile.
- help** Display the help text for this command and exit.

---

## rmsysconn

Remove a system connection.

### Synopsis

```
rmsysconn -o {remove | reset} {-m managed-system | -e managed-frame | --ip IP-address} [--help]
```

### Description

**rmsysconn** removes or resets a connection from the Hardware Management Console (HMC) to a managed system or a managed frame.

If your HMC is set up as a DHCP server on a private network, do not use this command to remove HMC connections to managed systems and frames. The remove option of this command is intended for use on a public network only, where the HMC is not set up as a DHCP server. Using the remove option of this command prevents the HMC from managing any system or frame at that IP address, even though that address may still be assigned through DHCP.

## Options

- o** The operation to perform. Valid values are **remove** or **reset**. When **remove** is specified, the HMC disconnects from the specified managed system or the specified managed frame. If all connections to the managed system or managed frame are removed, then the managed system or managed frame is removed from the HMC.

When **reset** is specified, the HMC disconnects from the specified managed system or the specified managed frame then attempts to reconnect.

The **reset** operation is useful for retrying to establish a connection to a managed system or a managed frame that is in the "No Connection" state.

- m** The name of the managed system to remove or to reset the connection to. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.

If the managed system has a single service processor, the connection to the service processor is removed or reset. When the connection is removed, the managed system is removed from the HMC.

If the managed system has two service processors, the connections to both service processors for the managed system are removed or reset. When the connections to both service processors for the managed system are removed, the managed system is removed from the HMC. To remove or reset the connection to just one service processor for the managed system, use the **--ip** option.

Either this option, the **--ip** option, or the **-e** option is required. The **-m**, **--ip**, and the **-e** options are mutually exclusive.

- e** The name of the managed frame to remove or to reset the connection to. The name may either be the user-defined name for the managed frame, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the type, *mmm* is the model, and *sssssss* is the serial number of the managed frame. The *tttt-mmm\*sssssss* form must be used if there are multiple managed frames with the same user-defined name.

When this option is used to specify the managed frame to remove or to reset the connection to, the connections to both sides of the bulk power assembly (BPA) for the managed frame are removed or reset. When the connections to both sides of the BPA for the managed frame are removed, the managed frame is removed from the HMC.

To remove or reset the connection to just one side of the BPA for the managed frame, use the **--ip** option.

Either this option, the **--ip** option, or the **-m** option is required. The **-e**, **--ip**, and the **-m** options are mutually exclusive.

- ip** To remove or reset the connection to a managed system with a single service processor, you can use this option to specify the IP address or host name of the service processor for the managed system to remove or to reset the connection to. Alternatively, you can use the **-m** option to specify the name of the managed system to remove or to reset the connection to.

To remove or reset the connection to just one service processor for a managed system with two service processors, you can use this option to specify the IP address or host name of the service processor to remove or to reset the connection to. To remove or reset the connection to both service processors for a managed system, use the **-m** option. Note that a managed system with two service processors will not be removed from the HMC until the connections to both service processors for the managed system are removed.

To remove or reset the connection to just one side of the BPA for a managed frame, you can use this option to specify the IP address or host name of the BPA side to remove or to reset the connection to. To remove or reset the connection to both sides of the BPA for a managed frame,

use the **-e** option. Note that a managed frame will not be removed from the HMC until the connections to both sides of the BPA for the managed frame are removed.

Either this option, the **-m** option, or the **-e** option is required. The **--ip**, **-m**, and the **-e** options are mutually exclusive.

**--help** Display the help text for this command and exit.

---

## rmsysplan

Remove system plan.

### Synopsis

**rmsysplan -f *file-name* [--help]**

### Description

**rmsysplan** removes a system plan file from the system plan file directory on the Hardware Management Console (HMC).

### Options

**-f** Specifies the name of the file that will be removed. Only files in the system plan file directory on the HMC will be removed.

**--help** Display the help text for this command and exit.

---

## rmsysplanres

Remove system plan resource.

### Synopsis

**rmsysplanres -r *osinstall* -n *resource-name* [--help]**

### Description

**rmsysplanres** removes a system plan resource that is defined on this Hardware Management Console (HMC). These resources can be used when deploying system plans from this HMC.

### Options

**-r** Specifies the type of system plan resource to remove. The only valid value is **osinstall** for an operating system installation resource.

**-n** Specifies the name of the system plan resource to remove.

**--help** Display the help text for this command and exit.

---

## rmvterm

Close a virtual terminal session.

### Synopsis

**rmvterm -m *managed-system* {-p *partition-name* | --id *partition-ID*} [--help]**

### Description



**rmvterm** forces the closure of a virtual terminal session for an AIX, Linux, or virtual I/O server partition.

To close the virtual terminal session normally, enter the `~.` character sequence in the terminal window.

## Options

- m** The name of the managed system which has the partition for which to close the virtual terminal session. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- p** The name of the partition for which to close the virtual terminal session.  
You must either use this option to specify the name of the partition, or use the **--id** option to specify the partition's ID. The **-p** and the **--id** options are mutually exclusive.
- id** The ID of the partition for which to close the virtual terminal session.  
You must either use this option to specify the ID of the partition, or use the **-p** option to specify the partition's name. The **--id** and the **-p** options are mutually exclusive.
- help** Display the help text for this command and exit.

---

## rsthwres

Restore hardware resources.

## Synopsis

To restore memory or processing resources:

```
rsthwres -r {mem | proc} -m managed-system [{-p partition-name | --id partition-ID}]
```

To restore physical I/O slots:

```
rsthwres -r io -m managed-system [{-p partition-name | --id partition-ID}] [-l slot-DRC-index]
```

To restore Host Ethernet Adapter (HEA) resources (POWER6 servers only):

```
rsthwres -r hea -m managed-system [{-p partition-name | --id partition-ID}] [-l HEA-adapter-ID] [-g port-group --logport logical-port-ID]
```

## Description

**rsthwres** restores the hardware resource configuration of partitions in the *managed-system*. This operation may need to be performed after a dynamic logical partitioning (DLPAR) operation fails.

## Options

- r** The type of hardware resources to restore. Valid values are *mem* for memory, *proc* for processing resources, *io* for physical I/O slots, and *hea* for Host Ethernet Adapter (HEA) resources.  
HEA resources are only supported on POWER6 servers.
- m** The name of the managed system which has the partitions for which to restore the hardware resources. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.

- p**      The name of the partition for which to restore the hardware resources.  
 To restore hardware resources for a single partition, you must either use this option to specify the name of the partition, or use the **--id** option to specify the partition's ID. Otherwise, hardware resources for all partitions in the *managed-system* will be restored.  
 The **-p** and the **--id** options are mutually exclusive.
- id**    The ID of the partition for which to restore the hardware resources.  
 To restore hardware resources for a single partition, you must either use this option to specify the ID of the partition, or use the **-p** option to specify the partition's name. Otherwise, hardware resources for all partitions in the *managed-system* will be restored.  
 The **--id** and the **-p** options are mutually exclusive.
- l**      When restoring physical I/O slots, specify the DRC index of the physical I/O slot to restore. If this option is omitted and a partition is specified with the **-p** or **--id** option, then all physical I/O slots assigned to the specified partition will be restored. If this option is omitted and a partition is not specified, then all physical I/O slots in the *managed-system* will be restored.  
 When restoring HEA resources, specify the adapter ID of the HEA to restore. If this option is omitted and a partition is specified with the **-p** or **--id** option, then all HEA resources, including Logical Host Ethernet Adapters and logical ports, assigned to the specified partition will be restored. If this option is omitted and a partition is not specified, then all HEA resources in the *managed-system* will be restored. This option is required when the **-g** and **--logport** options are specified to restore a specific logical port.  
 This option is only valid when restoring physical I/O slots or HEA resources.
- g**      The port group containing the HEA logical port to restore. This option is required when the **--logport** option is specified to restore a specific logical port.
- logport**  
 The ID of the HEA logical port to restore.
- help**   Display the help text for this command and exit.

---

## rstprofdata

Restore profile data.

### Synopsis

```
rstprofdata -m managed-system -l restore-type [-f file] [--help]
```

### Description

**rstprofdata** restores profile data for the *managed-system* from a backup file. **rstprofdata** can also be used to initialize the profile data for the *managed-system*.

The **bkprofdata** command can be used to back up profile data for the *managed-system*.

### Options

- m**      The name of the managed system for which to restore or initialize profile data. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- l**      The type of restore to perform. Valid values are:

- 1 - full restore from the backup file.
  - 2 - merge the current profile data and profile data from the backup file, giving priority to the backup data. If the profile data conflicts, the backup data is restored over the current data.
  - 3 - merge the current profile data and profile data from the backup file, giving priority to the current data. If the profile data conflicts, the backup data is not restored over the current data.
  - 4 - initialize the profile data. All partitions, partition profiles, and system profiles for the managed system will be deleted.
- f** The name of the backup file that contains the profile data to be restored. If *file* is not fully qualified, *file* must exist in the `/var/hsc/profiles/serial-number` directory on the HMC (*serial-number* is the serial number of the managed system).
- To restore the profile data from removable media, the media must be present in the removable media device and the device must be mounted with the **mount** command before this command is issued. The **lsmediadev** command can be used to display all of the removable media devices on the HMC.
- This option is required for all restore types except **4** (initialize).
- help** Display the help text for this command and exit.

---

## rstupgdata

Restore upgrade data.

### Synopsis

**rstupgdata -r dvd [--help]**

### Description

**rstupgdata** copies the current partition profile data, Hardware Management Console (HMC) user data, and HMC configuration data previously saved on DVD-RAM into a portion of the HMC hard drive that the HMC upgrade process cannot erase. After this command has been executed, reboot the HMC to automatically recover the data.

The DVD-RAM media must be present in the drive, and mounted with the **mount** command, before running this command.

**Note:** Time on the HMC will need to be set after the data has been recovered.

### Options

- r** If **dvd** is specified, upgrade data will only be read from the DVD-RAM media.
- help** Display the help text for this command and exit.

---

## saveupgdata

Save upgrade data.

### Synopsis

**saveupgdata -r {disk | diskdvd} [--help]**

### Description

**saveupgdata** stores the current partition profile data, Hardware Management Console (HMC) user data, and HMC configuration data in a portion of the HMC hard drive that the HMC upgrade process cannot erase. The HMC automatically recovers the data after the upgrade process completes.

This command should be run immediately prior to performing an HMC upgrade. If the HMC is rebooted without performing an upgrade after running this command, this command needs to be run again.

## Options

- r** If **disk** is specified, upgrade data will only be saved on the HMC hard drive.  
If **diskdvd** is specified, then in addition to storing the upgrade data on the HMC hard drive, this command will copy the same upgrade data onto DVD-RAM media. You must ensure that the media is present in the DVD drive and that the DVD drive is mounted with the **mount** command before issuing this command.
- help** Display the help text for this command and exit.

---

## sendfile

Transfer file from the HMC to a remote system.

## Synopsis

```
sendfile -f filename -h remote-system -d remote-directory -u user [--passwd password] [-s] [-k keyfile] [--help]
```

## Description

**sendfile** transfer a file from the HMC to a remote system using File Transfer Protocol. Optionally allows Secure FTP over an encrypted ssh transport to be used. When selecting the secure ftp option, user have the option to specify an identity key file, generated by the ssh-keygen command for public key authentication. If the matching public key file resides on the remote system, and the passphrase is empty, no password will be prompted.

## Options

- f** The file name to transfer.
- h** The remote system name. An IP address can also be specified.
- d** The directory on the remote system to put the file.
- u** The user name on the remote system.
- passwd** The user's password on the remote system. If not specified, the password will be prompted.
- s** Specify the option to use Secure File Transfer Protocol.
- k** Specify the identity key file for public key authentication. This is the key file generated by the ssh-keygen command. If the public key file is deployed on the remote system, and the passphrase is empty, the password will not be prompted during secure file transfer.
- help** Prints help message.

---

## startdump

Start dump.

### Synopsis

```
startdump {-m managed-system | -e managed-frame} -t {pss | sp | sys} [-s {a | b | p | s}] [--help]
```

### Description

**startdump** initiates a dump on the *managed-system* or the *managed-frame*.

The **lsdump** command can be used to determine when the dump has completed and is available. The **getdump** command can then be used to offload the dump from the *managed-system* or the *managed-frame* to the Hardware Management Console (HMC).

### Options

- m**     The name of the managed system on which to initiate the dump. The name may either be the user-defined name for the managed system, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *ttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.

This option is required when initiating a service processor dump or a platform dump. This option is not valid otherwise.
- e**     The name of the managed frame on which to initiate the dump. The name may either be the user-defined name for the managed frame, or be in the form *ttt-mmm\*sssssss*, where *ttt* is the type, *mmm* is the model, and *sssssss* is the serial number of the managed frame. The *ttt-mmm\*sssssss* form must be used if there are multiple managed frames with the same user-defined name.

This option is required when initiating a power subsystem dump. This option is not valid otherwise.
- t**     The dump to initiate. Valid values are **pss** for a power subsystem dump, **sp** for a service processor dump, or **sys** for a platform dump.

When a service processor dump is started on the primary service processor, all communications between the HMC and the *managed-system* will be halted. When the dump has completed, communications will be resumed.

When a platform dump is started, the *managed-system* will be halted. When the dump has completed, the *managed-system* will be restarted.
- s**     When initiating a power subsystem dump, use this option to specify the side of the managed frame's bulk power assembly (BPA) on which to initiate the dump. Valid values are **a** for side A and **b** for side B.

When initiating a service processor dump, use this option to specify the service processor on which to initiate the dump. Valid values are **p** for the primary service processor and **s** for the secondary service processor. If this option is not specified, the service processor dump will be initiated on the primary service processor.
- help**   Display the help text for this command and exit.

---

## updhmc

Update code on the Hardware Management Console.

### Synopsis

```
updhmc -t {m | s | l} [-h ftp-server -u user-id [-p password | -i]] [-f patch-file] [-r] [-c] [--help]
```

### Description

**updhmc** updates code on the Hardware Management Console (HMC). This command performs the equivalent of the Install Corrective Service task under Licensed Internal Code Maintenance/HMC Code Update on the console.

### Options

- t** The source type to update from. Valid values are:
  - m** - media
  - s** - server
  - l** - local file system. This is only valid when specifying **-f** and the file is on the local file system.
- h** Host name or IP address of the FTP server where the patch file is located. Only valid when **s** is specified on the **-t** flag.
- u** User ID to use on the FTP server.
- p** Password to use on the FTP server. The password will be in clear text. When running the command interactively, use the **-i** parameter for entering a password without echo.
- i** Prompts for password. Password will be hidden.
- f** File on the FTP server to obtain, or locally.
- r** Reboot HMC after applying the update.
- c** Remove the file from the local file system after the installation.
- help** Display the help text for this command and exit.

---

## updlc

Update Licensed Internal Code (LIC).

### Synopsis

To retrieve, install, and activate LIC updates on a managed system:

```
updlc -o a -m managed-system -t {sys | power | syspower | io | all} -r {ibmretain | ibmwebsite | ftp | dvd | disk | mountpoint} -l {latest | latestconcurrent | sss | ccc,ppp} [-h host-name] [-u user-ID] [--passwd password] [-d directory] [-q]
```

To retrieve and install, but not activate LIC updates on a managed system:

```
updlc -o i -m managed-system -t {sys | power | syspower | io | all} -r {ibmretain | ibmwebsite | ftp | dvd | disk | mountpoint} -l {latest | latestconcurrent | sss | ccc,ppp} [-h host-name] [-u user-ID] [--passwd password] [-d directory] [-q]
```

To remove the most recently installed LIC updates and activate the previously accepted level on a managed system:

**updlc -o r -m *managed-system* -t syspower [-q]**

To change a managed system's LIC update control to the Hardware Management Console (HMC):

**updlc -o h -m *managed-system***

To change a managed system's LIC update control to Operating System:

**updlc -o o -m *managed-system***

To disruptively activate LIC updates on a managed system:

**updlc -o d -m *managed-system* [-q]**

To accept currently activated LIC updates on a managed system:

**updlc -o c -m *managed-system***

To reject installed LIC updates on a managed system:

**updlc -o j -m *managed-system***

To upgrade Licensed Internal Code to a new release on a managed system:

**updlc -o u -m *managed-system* -r {ibmretain | ibmwebsite | ftp | dvd | mountpoint} [-h *host-name*] [-u *user-ID*] [--passwd *password*] [-d *directory*] [-q]**

To check system readiness on a managed system:

**updlc -o k -m *managed-system***

To retrieve, install, and activate LIC updates on all High Performance Switches managed by the HMC:

**updlc -o a -w -r {ibmretain | ibmwebsite | ftp | dvd | disk | mountpoint} -l {latest | latestconcurrent | sss | ccc,ppp} [-h *host-name*] [-u *user-ID*] [--passwd *password*] [-d *directory*] [-q]**

To retrieve and install, but not activate LIC updates on all High Performance Switches managed by the HMC:

**updlc -o i -w -r {ibmretain | ibmwebsite | ftp | dvd | disk | mountpoint} -l {latest | latestconcurrent | sss | ccc,ppp} [-h *host-name*] [-u *user-ID*] [--passwd *password*] [-d *directory*] [-q]**

To remove the most recently installed LIC updates and activate the previously accepted level on all High Performance Switches managed by the HMC:

**updlc -o r -w [-q]**

To disruptively activate LIC updates on all High Performance Switches managed by the HMC:

**updlc -o d -w [-q]**

To accept currently activated LIC updates on all High Performance Switches managed by the HMC:

**updlc -o c -w**

To reject installed LIC updates on all High Performance Switches managed by the HMC:

**updlc -o j -w**

To upgrade Licensed Internal Code to a new release on all High Performance Switches managed by the HMC:

**updlc -o u -w -r {ibmretain | ibmwebsite | ftp | dvd | mountpoint} [-h *host-name*] [-u *user-ID*] [--passwd *password*] [-d *directory*] [-q]**

To check system readiness on all High Performance Switches managed by the HMC:

**updlc -o k -w**

## Description

**updlc** updates Licensed Internal Code (LIC) on the *managed-system* or on all High Performance Switches managed by this Hardware Management Console (HMC).

## Options

- o** The operation to perform. Valid values are **a**, **i**, **r**, **h**, **o**, **d**, **c**, **j**, **u**, and **k**.
  - Use the **a** operation to retrieve, install, and activate LIC updates. Previously activated updates will be automatically accepted.
  - Use the **i** operation to retrieve and install, but not activate, LIC updates.
  - Use the **r** operation to remove the most recently installed LIC updates and activate the previously accepted level. This operation is only valid when the LIC type is both Managed System and Power.
  - Use the **h** operation to change LIC update control to the Hardware Management Console (HMC). This option is only valid for a managed system.
  - Use the **o** operation to change LIC update control to Operating System. This option is only valid for a managed system.
  - Use the **d** operation to disruptively activate LIC updates.
  - Use the **c** operation to accept currently activated LIC updates (copy T to P).
  - Use the **j** operation to reject installed LIC updates (copy P to T).
  - Use the **u** operation to upgrade Licensed Internal Code to a new release.
  - Use the **k** operation to check system readiness for LIC operations.
- m** The name of the managed system on which to update LIC. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- w** Update LIC on all High Performance Switches managed by the HMC.
- t** The type(s) of LIC updates to install. Valid values are **sys** for Managed System LIC updates only, **power** for Power LIC updates only, **syspower** for both Managed System and Power LIC updates, **io** for I/O LIC updates only, or **all** for Managed System, Power, and I/O LIC updates. This option is only valid for a managed system.
  - This option is required for **a** and **i** operations, and is optional for the **r** operation. This option is not valid otherwise.
- l** The LIC level to retrieve. Valid values are **latest**, **latestconcurrent**, *sss*, or *ccc.ppp*.



This option is required for **a** and **i** operations. This option is not valid otherwise.

Specify **latest** to retrieve the latest LIC updates, even if disruptive.

Specify **latestconcurrent** to retrieve the latest concurrent LIC updates.

Specify **sss** to retrieve a specific level of Managed System or Power LIC updates, even if disruptive. **sss** is the three character identifier of the specific level to retrieve. This is only valid when the LIC type is either Managed System only or Power only.

Specify **ccc,ppp** to retrieve a specific level of Managed System and Power LIC updates, even if disruptive. **ccc** is the three character identifier of the specific level of Managed System LIC updates to retrieve. **ppp** is the three character identifier of the specific level of Power LIC updates to retrieve. This is only valid when the LIC type is both Managed System and Power.

- r** The repository from which to retrieve the LIC updates. Valid values are **ibmretain** for the IBM support system, **ibmwebsite** for the IBM service Internet site, **ftp** for a remote FTP site, **dvd** for the DVD drive on the Hardware Management Console (HMC), **disk** for the internal hard disk drive on the HMC, or **mountpoint** for the specified mountpoint.

This option is required for **a**, **i**, and **u** operations. This option is not valid otherwise.

- h** The host name or IP address of the remote FTP server.

This option is required when retrieving LIC updates from a remote FTP site. This option is not valid otherwise.

- u** The user ID to use to log in to the remote FTP site.

This option is required when retrieving LIC updates from a remote FTP site. This option is not valid otherwise.

#### **--passwd**

The password to use to log in to the remote FTP site. If this option is omitted, you will be prompted to enter the password.

This option is only valid when retrieving LIC updates from a remote FTP site.

- d** The mountpoint location or the directory to use on the remote FTP site. If this option is not specified for FTP, then the **/opt/ccfw/data** directory will be used.

This option is only valid when retrieving LIC updates from a mountpoint or a remote FTP site.

- q** Use this option to query the concurrency status of the specified update. The update is not performed when this option is specified.

This option allows you to determine if the specified update is disruptive. If so, you can shut down operating systems or configure I/O devices offline prior to performing the specified update.

When this option is used with **-m**, one of the following return codes will be returned:

- 0 - no updates are available.
- 1 - all updates are concurrent.
- 2 - Managed System and Power updates are concurrent. I/O updates are disruptive.
- 3 - Managed System and Power updates are disruptive. I/O updates are concurrent.
- 4 - all updates are disruptive.

Any other return code value indicates that an error occurred.

When this option is used with **-w**, one of the following return codes will be returned:

- 0 - no updates are available
- 1 - all updates are concurrent
- 4 - all updates are disruptive

Any other return code value indicates that an error occurred.

When this option is not used, a return code value of zero indicates success. Any other value indicates that an error occurred.

**--help** Display the help text for this command and exit.

---

## viosvr cmd

Issue virtual I/O server command.

### Synopsis

**viosvr cmd** **-m** *managed-system* **{-p** *partition-name* **|** **--id** *partition-ID* **}** **-c** "*command*" **[--help]**

### Description

**viosvr cmd** issues an I/O server command line interface (ioscli) command to a virtual I/O server partition.

The ioscli commands are passed from the Hardware Management Console (HMC) to the virtual I/O server partition over an RMC session. RMC does not allow interactive execution of ioscli commands.

### Options

- m** The name of the managed system which has the virtual I/O server partition to which to issue the command. The name may either be the user-defined name for the managed system, or be in the form *tttt-mmm\*sssssss*, where *tttt* is the machine type, *mmm* is the model, and *sssssss* is the serial number of the managed system. The *tttt-mmm\*sssssss* form must be used if there are multiple managed systems with the same user-defined name.
- p** The name of the virtual I/O server partition to which to issue the command.  
You must either use this option to specify the name of the partition, or use the **--id** option to specify the partition's ID. The **-p** and the **--id** options are mutually exclusive.
- id** The ID of the virtual I/O server partition to which to issue the command.  
You must either use this option to specify the ID of the partition, or use the **-p** option to specify the partition's name. The **--id** and the **-p** options are mutually exclusive.
- c** The I/O server command line interface (ioscli) command to issue to the virtual I/O server partition.  
*command* must be enclosed in double quotes. Also, *command* cannot contain the semicolon (;), greater than (>), or vertical bar (|) characters.
- help** Display the help text for this command and exit.

---

## Appendix E. Advanced Systems Management Interface (ASMI)

Some repair procedures require connection to the Advanced Systems Management Interface (ASMI).

---

### Connecting to a terminal

Connect your server to an ASCII terminal or a graphics terminal to interface with the system management services (SMS) menus. Connect your server to an ASCII terminal to interface with the Advanced System Management Interface (ASMI).

#### ASCII terminal

The ASCII terminal is connected to the server through a serial link. The ASCII interface to the ASMI provides a subset of the ASMI functions that are available using the Web interface, and the ASCII interface is available only when the server is in the platform standby state. The ASCII interface to the ASMI is not available during initial program load or run time. See “Accessing the ASMI using an ASCII terminal” on page 250 to set up the ASCII terminal for direct or remote access to the ASMI.

This connection also allows you to access the SMS menus. Use the menus to view information about your system and to perform tasks such as changing the boot list and setting the network parameters. See “Starting the system management services” on page 296 to get started.

#### Graphics terminal

The graphics terminal is available to users who want to use a graphical user interface (GUI) to their AIX® or Linux® servers. To use the graphics terminal, plug the graphics adapter into a PCI slot in the back of the server. You can connect a standard monitor, keyboard, and mouse to the adapter to use the terminal.

This connection allows you to access the SMS menus. For instructions, see “Starting the system management services” on page 296.

---

### Controlling the system power

Learn how to control the system power using the power button on the control panel and the ASMI.

#### Controlling the system power using the ASMI

Use the Advanced System Management Interface (ASMI) to manually and automatically control the system power.

#### Powering the system on and off

View and customize various initial program load (IPL) parameters.

You can start and shut down the system in addition to setting IPL options.

To perform these operations, your authority level must be one of the following:

- Administrator
- Authorized service provider

Several IPL options that you can set pertain to the server firmware. Firmware is an integral part of the server that is stored in *flash memory*, whose contents are preserved when the system is powered off. The firmware is code that automatically starts when the server is turned on. Its main purpose is to bring the server to a state where it is ready to operate, which means the server is ready to install or boot an

operating system. Firmware also enables the handling of exception conditions in the hardware and provides extensions to the functions of the server hardware platform. You can view the server's current firmware level on the Advanced System Management Interface (ASMI) Welcome pane.

This server has a permanent firmware boot side, or P side, and a temporary firmware boot side, or T side. When updating the firmware, install new levels of firmware on the temporary side first to test the compatibility with your applications. When the new level of firmware has been approved, copy it to the permanent side.

To view and change IPL settings, perform the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Power/Restart Control** and select **Power On/Off System**.
3. Set the following desired boot settings.

#### **System boot speed**

Select the speed for the next boot: **Fast** or **Slow**. Fast boot results in some diagnostic tests being skipped, and shorter memory tests being run during the boot.

#### **Firmware boot side for next boot**

Select the side from which the firmware boots the next time: **Permanent** or **Temporary**. Test firmware updates by booting from the temporary side before being copied into the permanent side.

#### **System operating mode**

Select the operating mode: **Manual** or **Normal**. Manual mode overrides various automatic power-on functions, such as auto-power restart, and enables the power button.

#### **Boot to server firmware**

Select the state for the server firmware: **Standby** or **Running**. When the server is in the server firmware standby state, partitions can be set up and activated.

#### **System power off policy**

Select the system power off policy. The system power off policy is a system parameter that controls the system's behavior when the last partition (or the only partition in the case of a system that is not managed by an HMC) is powered off.

#### **Current hyperboot mode state:**

This setting is displayed if the hyperboot feature is activated for the system. The hyperboot mode states are: **capable** and **enabled**. When the hyperboot feature is activated by entering the activation code, the mode state initializes in the ASMI and displays **capable** until the system is restarted. After the system has restarted the state changes to **enabled**. Any time you restart the system in the enabled state, it starts in hyperboot mode.

4. Perform one of the following steps:
  - Click **Save settings** to save the selected options. The power state does not change.
  - Click **Save settings and power on/off**. All selected options are saved and the system turns on or off. The power-on option is available only if the system is powered off. The power-off option is available only if the system is powered on.
  - Click **Save settings and continue server firmware boot** to save the selected options, and turn the server firmware on or off. This option is available only if the server firmware is in *standby* mode.

## **Setting auto-power restart**

Enable or disable the function that automatically restarts the system.

You can set your system to automatically restart. This function is useful when power has been restored and any backup power supply has recharged after a temporary power failure or after an unexpected power line disturbance that caused the system to shut down. Auto-power restart works only if the system

operating mode is set to **normal** in the Power On/Off System settings. For information about setting the system operating mode, see “Powering the system on and off” on page 243.

When the system restarts, it returns to the state it was in at the time of the power loss. If the system is not managed by a Hardware Management Console (HMC), the system reboots the operating system. If the system is managed by an HMC, all of the partitions that were running before the power loss are reactivated.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To set the auto-power restart function, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Power/Restart Control** and select **Auto Power Restart**.
3. Select either **Enable** or **Disable** from the selection list. By default, the state for auto-power restart is *Disable*.
4. Click **Save settings** to save the selected options.

## Performing an immediate power off

You can power off your system faster by using the **immediate power off** option. Typically, this option is used when an emergency power off is needed. The operating system is *not* notified before the system is powered off.

**Attention:** To avoid experiencing data loss and a longer IPL the next time the system or logical partitions are booted, shut down the operating system prior to performing an immediate power off.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To perform an immediate power off, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Power/Restart Control** and select **Immediate Power Off**.
3. Click **Continue** to perform the operation.

## Performing a system reboot

You can reboot your system without a complete system shutdown.

**Important:** Rebooting the system immediately shuts down all partitions.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To perform a system reboot, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Power/Restart Control** and select **System Reboot**.
3. Click **Continue** to perform the operation.

---

## Managing the Advanced System Management Interface (ASMI)

Understand how to manage the Advanced System Management Interface (ASMI).

The Advanced System Management Interface (ASMI) is the interface to the service processor that is required to perform general and administrator-level service tasks, such as reading service processor error logs, reading vital product data, setting up the service processor, and controlling the system power. The ASMI might also be referred to as the service processor menus.

### ASMI requirements

Learn about ASMI setup and functionality requirements.

To successfully access and use the ASMI, note the following requirements:

- The ASMI requires password authentication.
- The ASMI provides a Secure Sockets Layer (SSL) Web connection to the service processor. To establish an SSL connection, open your browser using `https://`.
- Supported browsers are Netscape (version 7.1), Microsoft® Internet Explorer (version 6.0), and Opera (version 7.23). Later versions of these browsers cannot be used to access ASMI. JavaScript™ and cookies must be enabled.
- Clicking **Back** in the browser might display outdated data. To display the most up-to-date data, select the desired item from the navigation pane.
- The browser-based ASMI is available during all phases of the system operation, including initial program load (IPL) and run time. Some menu options are not available during the system IPL or run time to prevent usage or ownership conflicts if corresponding resources are in use during that phase.
- The ASMI that is accessed on a terminal is available only if the system is at platform standby.
- All requested input must be provided in English-language characters regardless of the language selected to view the interface.

### ASMI Authority Levels

There are several authority levels for accessing the service processor menus using the ASMI. The following levels of access are supported:

#### General user

The menu options presented to the general user are a subset of the options available to the administrator and authorized service provider. Users with general authority can view settings in the ASMI menus. The login ID is **general** and the default password is *general*.

#### Administrator

The menu options presented to the administrator are a subset of the options available to the authorized service provider. Users with administrator authority can write to persistent storage, and view and change settings that affect the server's behavior. The first time a user logs into the ASMI after the server is installed, a new password must be selected. The login ID is **admin** and the default password is *admin*.

#### Authorized service provider

This login gives the authorized service provider access to all functions that could be used to gather additional debug information from a failing system, such as viewing persistent storage, and clearing all deconfiguration errors.

There are three authorized service provider login IDs: **celogin0**, **celogin1**, and **celogin2**.

- **celogin0** is the primary service provider account. It is enabled by default, and it can enable or disable the other two service provider IDs, **celogin1** and **celogin2**. The login ID is **celogin0**; the password is generated dynamically and must be obtained by calling IBM technical support. **celogin0** can be disabled by the **admin** user.



- **celogin1** and **celogin2** are disabled by default. If the IDs are enabled, a static password must be set for them. The default password for both IDs is *celogin*. The default password must be changed the first time the ID is enabled. The **admin** user can also disable and enable these login IDs.
- To reset the password for **celogin1** or **celogin2**, the **admin** user can disable, then re-enable the ID. As soon as the ID is re-enabled, the password will have to be changed.
- If enabled, **celogin0**, **celogin1**, or **celogin2** can be used to reset the **admin** password, if necessary.

### Development

This login is used by support personnel to analyze a system that is failing at a detailed level. It is enabled by default, and can be disabled by the admin user. The userid is **dev**, and the password is generated dynamically and must be obtained by calling IBM technical support. This ID has the highest authority. Once a password for the ID is obtained, the ID can be used to reset the admin password, if necessary.

During the initial administrator and general user logins, the only menu option available is **Change Password**. In order to gain access to additional ASMI menus, you must change the administrator and general user default passwords. If you are an authorized service provider, you cannot change your password. For information about how to change your password, see “Changing ASMI passwords” on page 251.

## ASMI login restrictions

Learn about ASMI login restrictions, including the maximum number of user logins allowed.

Only three users can log in at the same time. For example, if three people are logged in to the ASMI and a person with a higher authority level than one of the current logged in users attempts to log in, the ASMI forces one of the lowest privileged users to log out. In addition, if you are logged in and not active for 15 minutes, your session expires. You receive no immediate notification when your session expires. However, when you select anything on the current page, you are returned to the ASMI Welcome pane.

To see who is logged in to the ASMI, view **Current users** on the ASMI Welcome pane after you log in.

If you make five login attempts that are not valid, your user account is locked out for five minutes and none of the other accounts are affected. For example, if the administrator account is locked, the general user can still log in using the correct password. This login restriction applies to the general user, administrator, and authorized service provider IDs.

## Accessing the ASMI

You can access the ASMI through a Web browser or an ASCII terminal.

### Accessing the ASMI using a Web browser

Connect a PC or mobile computer to the server to access the ASMI. The Web interface to the ASMI is available during all phases of system operation including the initial program load (IPL) and run time.

The Web interface to the Advanced System Management Interface (ASMI) is accessible through Microsoft Internet Explorer 6.0, Netscape 7.1, or Opera 7.23 running on a PC or mobile computer connected to the service processor. The Web interface is available during all phases of system operation including the initial program load (IPL) and run time. However, some of the menu options in the Web interface are unavailable during IPL or run time to prevent usage or ownership conflicts if the system resources are in use during that phase.

The following instructions apply to systems that are not connected to an HMC. If you are managing the server using an HMC, see the *Operations Guide for the Hardware Management Console and Managed Systems*,

To set up the Web browser for direct or remote access to the ASMI, complete the following tasks:

1. Connect the power cord from the server to a power source, and wait for the control panel to display 01.
2. Select a PC or mobile computer that has Microsoft Internet Explorer 6.0, Netscape 7.1, or Opera 7.23 to connect to your server.

If you do not plan to connect your server to your network, this PC or mobile computer will be your ASMI console.

If you plan to connect your server to your network, this PC or mobile computer will be temporarily connected directly to the server for setup purposes only. After setup, you can use any PC or mobile computer on your network that is running Microsoft Internet Explorer 6.0, Netscape 7.1, or Opera 7.23 as your ASMI console.

3. Connect an Ethernet cable from the PC or mobile computer to the Ethernet port labeled HMC1 on the back of the managed system. If HMC1 is occupied, connect an Ethernet cable from the PC or mobile computer to the Ethernet port labeled HMC2 on the back of the managed system.
4. Configure the Ethernet interface on the PC or mobile computer to an IP address and subnet mask within the same subnet as the server so that your PC or mobile computer can communicate with the server. For instructions, see “Setting the IP address on your PC or mobile computer” on page 249. Use the following table to help you determine these values:

Table 14. PC or mobile computer network configuration information

Server connector	Subnet mask	IP address
HMC1	255.255.255.0	169.254.2.146
HMC2	255.255.255.0	169.254.3.146

For example, if you connected your PC or mobile computer to HMC1, the IP address for your PC or mobile computer could be 169.254.2.146 and the subnet mask would be 255.255.255.0. Set the gateway IP address to the same IP address as the PC or mobile computer.

5. Use Table 14 to determine the IP address of the Ethernet port that your PC or mobile computer is connected to, and type the IP address in the Address field of your PC's or mobile computer's Web browser. For example, if you connected your PC or mobile computer to HMC1, type <https://169.254.2.146> in your PC's or mobile computer's Web browser.
6. When the login display appears, enter one of the following default user IDs and passwords:

Table 15. Default user IDs and passwords for the Web interface

User ID	Password
general	general
admin	admin

7. Change the default password when prompted. For information, see “ASMI Authority Levels” on page 246.
8. If you plan to connect your PC or mobile computer to your network, complete the following steps:
  - a. From the navigation area, expand **Network Services**.
  - b. Click **Network Configuration**.
  - c. If your PC or mobile computer is connected to HMC1, fill in the section labeled Network interface eth0.  
If your PC or mobile computer is connected to HMC2, fill in the section labeled Network interface eth1.



Ensure that the following fields are filled in correctly.

Table 16. Fields and values for network configuration

Field	Value
Configure this interface?	Selected
Type of IP address	Static
IP address	This is a set IP address obtained from the network administrator
Subnet mask	This is a set subnet mask obtained from the network administrator

**Note:** For information about the other fields and values, refer to “Configuring network interfaces” on page 268.

- d. Click **Continue**.
  - e. Click **Save Settings**.
  - f. Disconnect your PC or mobile computer from the server.
  - g. Connect the server to your company network.
  - h. Go to any PC or mobile computer on your company network that is running Microsoft Internet Explorer 6.0, Netscape 7.1, or Opera 7.23, and type the following in the Address field of your browser:  
`https://host name.domain name`  
  
where *host name* and *domain name* are the host name and domain name you entered when completing step 8c on page 248.
  - i. Log in to the ASMI.
9. “Changing the time of day” on page 256 on the server.

#### Setting the IP address on your PC or mobile computer:

To access the ASMI through a Web browser you first need to set the IP address on your PC or mobile computer. The following procedures describe setting the IP address on PC and mobile computers running Microsoft Windows® and Linux.

#### Setting the IP address in Windows XP and Windows 2000

To set the IP address within Windows XP and Windows 2000, complete these steps.

1. Click **Start >Settings >Control Panel**.
2. On the control panel, double-click **Network Connections**.
3. Right-click **Local Area Connection**.
4. Click **Properties**.

**Attention:** Record the current settings before making any changes. This will allow you to restore these settings if you disconnect the PC or mobile computer after setting up the ASMI Web interface.

**Note:** If Internet Protocol (TCP/IP) does not appear in the list, do the following:

- a. Click **Install**.
  - b. Select **Protocol**, and then click **Add**.
  - c. Select **Internet Protocol (TCP/IP)**.
  - d. Click **OK** to return to the Local Area Connection Properties window.
5. Select **Internet Protocol (TCP/IP)**, and then click **Properties**.

6. Select **Use the Following IP Address**.
7. Complete the **IP address**, **Subnet mask**, and **Default gateway** fields by using the values in step 4 on page 248 from Accessing the ASMI using a Web Browser.
8. Click **OK** on the Local Area Connection Properties window. It is not necessary to restart your PC.

### Setting the IP address in Linux

To set the IP address in Linux, complete these steps. You will need the information from step 4 on page 248 in Accessing the ASMI using a Web Browser to complete step 4 in the following procedure.

1. Make sure you are logged on as a root user.
2. Start a terminal session.
3. Type `ifconfig` at the command prompt.  
**Attention:** Record or print the current settings before making any changes. This allows you to restore these settings if you disconnect the PC or mobile computer after setting up the ASMI Web interface.
4. Type `ifconfig eth0 xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx`, where the `xxx.xxx.xxx.xxx` values are the values from step 4 on page 248 for IP address and Subnet mask.
5. Press Enter.

### Accessing the ASMI using an ASCII terminal

Connect the ASCII terminal to the server to access the ASMI.

The ASCII interface to the ASMI provides a subset of the Web interface functions. The ASCII terminal is available only when the system is in the platform standby state. It is not available during the initial program load (IPL) or run time. The ASMI on an ASCII terminal is not available during the other phases of system operation, including the initial program load (IPL) and run time.

To set up the ASCII terminal for direct or remote access to the ASMI, complete the following tasks:

1. Using a cable equipped with a null modem, connect the ASCII terminal to system connector S1 on the back of the server or to system port S1 on the control panel using an RJ-45 connector.

**Note:** Both system port 1 connections are not available simultaneously; when one is connected, the other is deactivated.

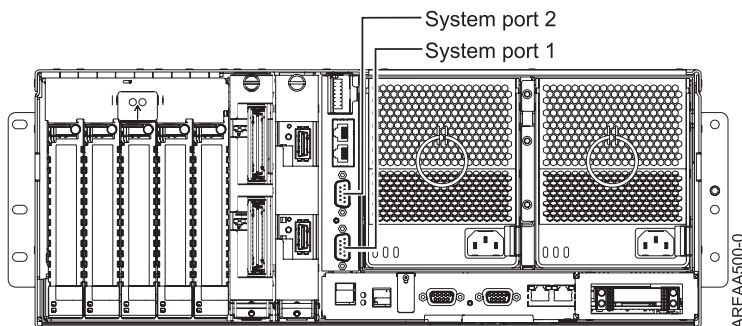


Figure 21. Connection for model 570

2. Connect the power cord from the server to a power source.
3. Wait for the control panel to display 01.
4. Ensure that your ASCII terminal is set to the following general attributes.  
These attributes are the default settings for the diagnostic programs. Be sure your terminal is set according to these attributes before proceeding to the next step.

Table 17. Default settings for the diagnostic programs

General setup attributes	3151 /11/31/41 settings	3151 /51/61 settings	3161 /64 settings	Description
Line speed	19,200	19,200	19,200	Uses the 19,200 (bits per second) line speed to communicate with the system unit.
Word length (bits)	8	8	8	Selects eight bits as a data word length (byte).
Parity	No	No	No	Does not add a parity bit and is used together with the word length attribute to form the 8-bit data word (byte).
Stop bit	1	1	1	Places a bit after a data word (byte).

- Press a key on the ASCII terminal to allow the service processor to confirm the presence of the ASCII terminal.
- When the login display appears, enter one of the following default user IDs and passwords:

Table 18. Default user IDs and passwords for the Web interface

User ID	Password
general	general
admin	admin

- Change the default password when you are prompted. For information see “ASMI Authority Levels” on page 246.
- “Changing the time of day” on page 256 on the server.

## Setting up an ASMI login profile

Learn how to change passwords, view login audits, change the default language, and update the installed languages.

### Changing ASMI passwords

Change the general user, administrator, and HMC access passwords.

You can change the general user, administrator, and HMC access passwords. If you are a general user, you can change only your own password. If you are an administrator, you can change your password and the passwords for general user accounts. If you are an authorized service provider, you can change your password, the passwords for general and administrator user accounts, and the HMC access password.

Passwords can be any combination of up to 64 alphanumeric characters. The default password for the general user ID is `general`, and the default password for the administrator ID is `admin`. After your initial login to the ASMI and after the reset toggle jumpers are moved, the general user and administrator passwords must be changed.

The HMC access password is usually set from the HMC during initial login. If you change this password using the ASMI, the change takes effect immediately.

To change a password, follow these steps:

**Note:** As a security measure, you are required to enter the current user’s password into the **Current password for current user** field. This password is not the password for the user ID you want to change.

- On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.

2. In the navigation area, expand **Login Profile**.
3. Select **Change Password**.
4. Specify the required information, and click **Continue**.

## Retrieving ASMI login audits

View the login history.

You can view the login history for the ASMI to see the last 20 successful logins and the last 20 logins that failed.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To retrieve login audits, follow these steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Login Profile**.
3. Select **Retrieve Login Audits**. The right pane displays the login history.

## Changing the default language for the ASMI

Select the language that will be used to display the ASMI Web and TTY menus.

You can select the language that is displayed on the ASMI welcome screen prior to login and during your ASMI session if you do not choose an alternative language at the time of login. You must provide all requested input in English-language characters regardless of the language selected to view the interface.

**Note:** You can change the language for each ASMI session by selecting the desired language from the menu found on the ASMI Welcome pane prior to logging in to the ASMI.

To perform this operation, your authority level must be one of the following:

- General
- Administrator
- Authorized service provider

To change the default language, follow these steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Login Profile**.
3. Select **Change Default Language**.
4. In the right pane, select the desired default language and click **Save setting**.

## Updating installed languages

Select additional languages to install on the service processor.

A maximum of five languages can be supported on the service processor at any given time. By default, English is always installed. Languages installation changes take effect when the firmware is updated.

**Note:** You must provide all requested input in English-language characters regardless of the language selected to view the interface.

To perform this operation, your authority level must be one of the following:

- General
- Administrator

- Authorized service provider

To update the installed language, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Login Profile**.
3. Select **Update Installed Languages**.
4. In the right pane, select the desired languages and click **Save setting**.

## Viewing system information

View vital product data (VPD), persistent storage, system power control network (SPCN) trace data, and progress indicator data.

**Important:** Clicking **Back** in the browser might display outdated data. To display the most up-to-date data, select the desired item from the navigation pane.

## Viewing vital product data

View selected or all manufacturer's VPD, such as serial numbers and part numbers.

You can view manufacturer's vital product data (VPD) stored from the system boot prior to the one in progress now.

To perform this operation, your authority level must be one of the following:

- General
- Administrator
- Authorized service provider

To view the VPD, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information** and select **Vital Product Data**.
3. A list of field replaceable units (FRUs) that exist on the system and their descriptions are displayed. Select a single FRU or multiple FRUs from this list that you would like to view.
4. Click **Display Details** to display the details for selected FRUs, or click **Display all details** to display details for all VPD entries.

## Viewing persistent storage

Learn how to display the contents of the registry.

You can gather additional debug information from a failing system by viewing the contents of the registry. The term *registry key* can refer to either the key part of a registry entry or the entire registry entry, depending on the context. The registry key hierarchy and the contents of any key can be viewed in both ASCII and hexadecimal formats.

Each registry entry is identified by a two-part key. The first part is the component name, and the second part is the name of the key. For example, the `TerminalSize` key of the `esw_menu` component is identified as `menu/TerminalSize`. Each registry key also has a value, which is up to 255 bytes of binary data.

To view persistent storage, your authority level must be authorized service provider.

To view the component names of the contents of the registry, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information** and select **Persistent Storage**.
3. Click the component names to view a list of registry entries.

4. Click the desired registry entry to view the contents of a registry entry.

## Viewing file systems

You can view the files systems that currently display on the control panel.

To perform this operation, your authority level must be authorized service provider.

To view the file systems, perform the following task:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information**.
3. Select **File System** to display a list of directories on the FSP.
4. Select the file or directory you want to view.

## Viewing system power control network trace

View SPCN trace data that was dumped from the processor subsystem or server drawer.

You can dump the system power control network (SPCN) trace data from the processor subsystem, or server drawer, to gather additional debug information. Producing a trace may take an extended period of time based on your system type and configuration. This delay is due to the amount of time the system requires to query the data.

**Important:** Due to the amount of time required to produce a trace, select this option only if it is recommended by an authorized service provider.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To view this trace data, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information** and select **Power Control Network Trace**. Trace data is displayed as single contiguous data in two columns.
3. View the raw binary data in the left column and an ASCII translation in the right column.

## Viewing progress indicator from previous boot

Learn how to display the boot progress indicator from the previous system boot.

You can view the progress indicator that displayed in the control panel during the previous failed boot. During a successful boot, the previous progress indicator is cleared. If this option is selected after a successful boot, nothing is displayed.

To perform this operation, your authority level must be one of the following:

- General
- Administrator
- Authorized service provider

The progress indicator information is stored in nonvolatile memory. If the system is powered off using the power-on button on the control panel, this information is retained. If the ac power is disconnected from the system, this information is lost.

To view the progress indicator from the previous boot, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information**.

3. Select **Previous Boot Progress Indicator**. The results are displayed in the right pane.

### Viewing progress indicator history

You can view progress codes that appeared in the control panel display during the last boot. The codes display in reverse chronological order.

To perform this operation, your authority level must be one of the following:

- General
- Administrator
- Authorized service provider

To view the progress indicator history, perform the following task:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information**.
3. Select **Progress Indicator History**.
4. Select the desired progress indicator to view additional details and click **Show Details**. The progress indicator codes are listed from top (latest) to bottom (earliest).

### Viewing real-time progress indicator

You can view the progress and error codes that currently display on the control panel. Viewing progress and error codes is useful when diagnosing boot-related issues.

To perform this operation, your authority level must be one of the following:

- General
- Administrator
- Authorized service provider

To view the progress indicator, perform the following task:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Information**.
3. Select **Real-time Progress Indicator** to display a small box that contains the current progress and error codes. If no value is currently on the control panel, the small box is displayed but remains empty.

## Changing system configuration

View and perform custom system configurations, such as enabling PCI (Peripheral Component Interconnect) error injection policies, viewing system identification information, and changing memory configuration.

### Changing system name

You can change the name that is used to identify the system. This name helps your support team (for example, your system administrator, network administrator, or authorized service provider) to more quickly identify the location, configuration, and history of your server.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

The system name is initialized to the 31-character value `Server-tttt-mmm-SN0000000`, where the substitution characters mean the following:

Characters	Description
tttt	Machine type



Characters	Description
mmm	Model number
oooooooo	Serial number

The system name can be changed to any valid ASCII string. It does not have to follow the initialized format.

To change the system name, do the following:

1. In the navigation area, expand **System Configuration**.
2. Select **System Name**.
3. Enter the desired system name using the previous naming convention.
4. Click **Save settings** to update the system name to the new value.

The new system name is displayed in the status frame, the area where the logout button is located. If another method, such as the HMC, is used to change the system name, the status frame does not reflect the change.

## Configuring I/O enclosures

View and change various enclosure attributes.

After the server firmware has reached the *standby* state, you can configure I/O enclosure attributes as follows:

- List the status, location code, rack address, unit address, power control network identifier, and the machine type and model of each enclosure in the system.
- Change the identification indicator state on each enclosure to *identify* or *off*.
- Update the power control network identifier, enclosure serial number, and the machine type and model of each enclosure.
- Change the identification indicator state of the SPCN firmware in a enclosure to *Enable* or *Disable*.
- Remove rack and unit addresses for all inactive enclosures in the system.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure I/O enclosures, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and select **Configure I/O Enclosures**.
3. Select the enclosure and the desired operation. If you select **Change settings**, click **Save setting** to complete the operation.

## Changing the time of day

Display and change the time and date stored by the system.

You can display and change the system's current date and time. The date and time can only be changed when the system is powered off. The time is stored as UTC (Coordinated Universal Time), formerly expressed as Greenwich mean time (GMT).

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider



**Note:** You can change the time of day only when the system is powered off.

To change the time of day, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Time of Day**. If the system is powered off, the right pane displays a form that shows the current date (month, day, and year) and time (hours, minutes, seconds).
4. Change either the date value or the time value or both, and click **Save settings**.

## Changing firmware update policy

Configure your system to only allow firmware updates from the selected source.

**Note:** These options are only valid if your server is managed by an HMC, otherwise the default source for installing firmware updates is the operating system and setting the source using this method is ignored by the server.

You can change the source for firmware updates. For example, if you choose the Hardware Management Console (HMC) as the source for a firmware update, the HMC must be used to perform the update. The HMC performs all tasks to update the server firmware.

### Updating firmware on IBM System p servers:

If your server has an HMC attached, the firmware update can only be performed from the HMC. The firmware update must be initiated from the HMC concurrently (while the system is running), but the update will not be applied until the server is rebooted. .

For information about performing a firmware update, see “Managed System Updates” on page 116.

## Enabling PCI error injection policy

Change the PCI error injection policy that forces errors to be injected to PCI cards.

You can enable or disable the injection of errors on the PCI bus. For example, independent software vendors who develop device drivers can inject errors to test the error handling code in the device driver.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

**Note:** To inject errors, you must have special hardware in addition to having advanced PCI bus knowledge.

To enable or disable the PCI error injection policy, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **PCI Error Injection Policy**.
4. In the right pane, select **Enabled** or **Disabled**.
5. Click **Save settings**.

## Configuring monitoring

Configure the server firmware and HMC monitoring.

To configure monitoring, your authority level must be an authorized service provider.

Monitoring is accomplished by periodic samplings called *heartbeats*, which can detect an HMC or server firmware connection failure.

To configure monitoring, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Monitoring**.
4. Select **Enabled** or **Disabled** for the server firmware and HMC. All connection monitoring fields are enabled by default.
5. Click **Save settings**. Monitoring does not take effect until the next time the operating system is started.

## Removing HMC connection data

Display and remove disconnected HMC data.

By default, HMC connection data expires on the managed system after 14 days of disconnection from the HMC. If you want to perform a task that requires all HMCs to be disconnected from the managed system, you can remove the HMC connection data prior to the 14-day period.

To disconnect an HMC, your authority level must be an authorized service provider.

To disconnect an HMC, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Hardware Management Consoles**.
4. Select the desired HMC.
5. Click **Remove connection**.

## Changing the interposer plug count

View and change the multiple chip module (MCM) interposer plug count.

You can track the number of times that a multiple chip module (MCM) has been replaced or reseated on a given interposer. This interposer plug count provides you with information needed to prevent field problems due to damaged or overused interposers. You can use the ASMI to view and alter the interposer plug count for all MCMs in the system. Whenever a service action is performed on a system that requires the replacement or reseating of an MCM, service personnel are responsible for updating the plug count for that interposer.

**Note:** The **Interposer Plug Count** option is supported only on certain system types and models. If your server does not support this option and you select this option from the menu, the firmware returns a message indicating that this option is not applicable to your system.

To perform this operation, your authority level must be authorized service provider.

To view and modify the interposer plug count, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Interposer Plug Count**. The current plug count is displayed in the text edit field for each MCM interposer. Each interposer is identified by location code.
4. Type a new value into the text field to change the plug count.
5. Click **Save settings**. A report page displays the new value.

## Enabling I/O adapter memory allocation

Increase the amount of PCI memory space allocated to specified PCI slots.

You can increase the amount of I/O adapter memory for specified PCI slots. When the **I/O Adapter Enlarged Capacity** option is enabled, specific PCI slots receive the largest memory-mapped address spaces that are available.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To enable or disable I/O adapter memory allocation, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **I/O Adapter Enlarged Capacity**.
4. In the right pane, select **Enabled** or **Disabled**.
5. Click **Save settings**.

## Deconfiguring hardware

Set deconfiguration policies, change processor configuration, change memory configuration, view deconfigured resources, and clear all deconfiguration errors.

### Setting deconfiguration policies:

Set various processor and memory configuration and deconfiguration policies.

You can set various policies to deconfigure processors and memory in certain situations. You can enable policies that will deconfigure the processor when failures occur, such as a predictive failure (for example, correctable errors generated by a processor exceeding the threshold), floating point failure, functional failure, or system bus failure. You can also enable the firmware to power off a processing unit (node) for concurrent maintenance when any of the resources in that node are deconfigured.

To set the deconfiguration policies, your authority level must be one of the following (any user can view the deconfiguration policies):

- Administrator
- Authorized service provider

To set deconfiguration policies, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Hardware Deconfiguration**.
3. Select **Deconfiguration Policies**.
4. In the right pane, select **Enabled** or **Disabled** for each policy.
5. Click **Save settings**.

### Changing processor configuration:

Learn how to display data and change the state for each processor.

All processor failures that stop the system, even if intermittent, are reported to the authorized service provider as a diagnostic call out for service repair. To prevent the recurrence of intermittent problems and improve the availability of the system until a scheduled maintenance window, processors with a failure history are marked *deconfigured* to prevent them from being configured on subsequent boots.

A processor is marked *deconfigured* under the following circumstances:

- A processor fails a built-in self-test or power-on self-test testing during boot (as determined by the service processor).
- A processor causes a machine check or check stop during run time, and the failure can be isolated specifically to that processor (as determined by the processor run-time diagnostics in the service processor firmware).
- A processor reaches a threshold of recovered failures that results in a predictive call to service (as determined by the processor run-time diagnostics in the service processor firmware).

During system start time, the service processor does not configure processors that are marked *deconfigured*. The deconfigured processors are omitted from the hardware configuration. The processor remains offline for subsequent reboots until it is replaced or the deconfiguration policy is disabled. The deconfiguration policy also provides the user with the option of manually deconfiguring a processor or re-enabling a previously manually deconfigured processor. This state is displayed as *deconfigured by user*.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

**Note:** The state of the processor can be changed only if the system is powered off. At run time, users can view but not change the state of each processor. If the deconfiguration policy is disabled, the states of the processors cannot be changed.

To view or change the processor configuration, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Hardware Deconfiguration**.
3. Select **Processor Deconfiguration**.
4. In the right pane, select a node from the list of nodes displayed.
5. Click **Continue** to change the state of each processor to configured, or deconfigured if it is not already deconfigured by the system.
6. Reboot the system for the changes to take effect.

### Changing memory configuration:

Display data for each memory unit and bank. You can change the state of each bank.

Each memory bank contains two DIMMs (dual inline memory module). If the firmware detects a failure, or predictive failure, of a DIMM, it deconfigures the DIMM with the failure, as well as the other DIMM, in the memory bank. If memory DIMMs are being monitored for errors, each memory bank will be in one of the following states:

- Configured by system (cs)
- Manually configured (mc)
- Deconfigured by system (ds)
- Manually deconfigured (md)

With ASMI, you can change the state of the memory bank from *cs* to *md*, from *mc* to *md*, and from *md* to *mc* for one or more DIMMs. If one DIMM is deconfigured, the other DIMM in the memory bank automatically becomes deconfigured.

**Note:** You can change the state of the memory bank only if the deconfiguration policy is enabled for the memory domain. If this policy is not enabled and you try to change the state, an error message is displayed.

The error type is the cause of memory deconfiguration and applies to the bank in the *ds* state. The error type is displayed only when the bank is in the *ds* state.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To view or change the memory configuration, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Hardware Deconfiguration**.
3. Select **Memory Deconfiguration**.
4. In the right pane, select a node from the list of nodes displayed.
5. Click **Continue** to change the state of memory to configured or deconfigured, if it is not already deconfigured by the system.

**Note:** The state of the memory can be changed only if the system is powered off. At run time, users can view, but not change, the state of each processor. If the deconfiguration policy function is disabled, the state of the memory cannot be changed.

6. Click **Submit**. A report page is displayed, which indicates success or failure when the state of the memory bank has been changed.

#### Viewing deconfigured resources:

View the resources deconfigured by the system.

To view the deconfigured resources, your authority level must be authorized service provider.

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Hardware Deconfiguration**.
3. Select the deconfigured resource that you want to view.

#### Clearing all deconfiguration errors:

Clear error records for specific or all resources in the system.

The ASMI allows you to clear error records for all or individual system hardware resources that include the processor, memory, L2 and L3 cache, I/O hubs, service processor card, and clock card.

To clear all deconfiguration errors, your authority level must be an authorized service provider.

**Note:** Before performing this operation, record error messages or ensure that the error record data is no longer needed; otherwise, you will lose all error data from the hardware resources.

To clear all deconfiguration errors, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Hardware Deconfiguration**.
3. Select **Clear All Deconfiguration Errors**.
4. In the right pane, select the desired hardware resource from the menu. You can select **All hardware resources** or an individual resource.
5. Click **Clear errors for selected hardware resource**.

#### Configuring virtual Ethernet environment settings

Specify settings to control your virtual Ethernet environment.

You can configure system firmware settings that enable you to restrict virtual input/output (I/O) connectivity between partitions, control the number of virtual Ethernet switches allocated by the firmware, and control when to run the floating point unit computation test.

### Managing virtual I/O connectivity:

Use the ASMI to set the policy for virtual input/output connectivity.

**Important:** Before you change the policy setting, power off the system.

Specifying this configuration setting enables you to control virtual input/output activity between partitions. The policy is set to *enabled* by default, which allows all virtual input/output connectivity between partitions. If this setting is disabled, only virtual TTY sessions to the Hardware Management Console (HMC) are allowed.

**Note:** Your authority level must be an authorized service provider.

To set the policy for virtual I/O connections, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log in**.
2. In the navigation area, expand **System Configuration**, and then click **Virtual I/O Connections**.
3. Select either **enable** or **disable** to change the setting.
4. Click **Save Settings**.

### Setting the maximum number of virtual Ethernet switches:

Control the number of virtual Ethernet switches allocated by the system server firmware.

You can set a configuration value that enables you to specify the number of virtual Ethernet switches that can be allocated by the system server firmware. This value is set to 0 by default. A value of 0 enables the Hardware Management Console (HMC) to control the number of virtual Ethernet switches allocated by the system server firmware. You can change this value to specify up to 16 allowable virtual switches.

The default value is generally used for most configurations. However, in a more complex environment where you might want the system server firmware to create a larger number of virtual Ethernet switches during platform power on, you can set this number higher and override the HMC's control.

After setting this value, when a virtual Ethernet adapter is created using the HMC, the adapter will be connected to a particular virtual switch depending on the virtual slot number chosen during creation. The adapter's virtual slot number will be divided by the number of virtual Ethernet switches, and the remainder of this division operation will be used to determine with which switch the adapter will be associated. Each virtual Ethernet adapter will be able to communicate only with other virtual Ethernet adapters on the same virtual switch.

**Important:** Before you change the value for the number of virtual Ethernet switches, power off the system.

To configure the value for virtual Ethernet switches, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log in**.
2. In the navigation area, expand **System Configuration**, and then click **Virtual Ethernet Switches**.
3. Enter a value for the Number of Virtual Ethernet Switches. The value can be a whole number from 0 to 16.
4. Click **Save Settings** to save the configuration.

For example, if you set the number of virtual Ethernet switches to 3, virtual Ethernet adapters in virtual slot 3, 6, and 9 are assigned to the same switch. A virtual Ethernet adapter in virtual slot 4 would be assigned to another switch, and would not be able to communicate with the adapters in slots 3, 6, and 9.

### Accepting firmware license agreement:

Learn how to accept the firmware license agreement.

To perform this operation, your authority level must be authorized service provider.

**Important:** Only perform this operation when directed to do so by service and support.

To accept the firmware license agreement, perform the following task:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration**.
3. Select **Firmware License Agreement**.
4. Select **Accept** or **Decline**, and then click **Save settings**.

### Running the floating point unit computation test:

Control the policy of when to run the floating point unit computation test.

Specifying this configuration setting allows you to control when you want to run this test. You can set it to run immediately or to run at various times.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To specify when to run this test, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log in**.
2. In the navigation area, expand **System Configuration**, and then click **Floating point unit computation test**.
3. In the right pane, select the settings that you want.
4. Click **Save Settings**.

### Programming vital product data

The ASMI allows you to program the system vital product data (VPD) such as system brand, system identifiers, and system enclosure type. To access any of the VPD-related panels, your authority level must be administrator or authorized service provider.

**Note:** You cannot boot the system until valid values are entered for the system brand, system identifiers, and system enclosure type.

### Setting the system brand:

Set and view the system brand.

The system brand identifies your system using a 2-character system brand as shown in the following table.



Table 19. System brand values

System brand	Description
D0	IBM Storage
P0	IBM System p

Changing the system brand is only allowed if the value has not been set, or if the current value is **P0** and the new value will be **D0**. Additionally, for IBM Storage, each of the systems that constitutes the storage facility must be set to D0 for storage to be accessible online.

**Note:** You cannot boot the system until valid values are entered for all fields. Use this procedure only under the direction of service and support.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To change the system brand, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Program Vital Product Data**.
3. Select **System Brand**. In the right pane, the current system brand is displayed. If the system brand has not been set, you will be prompted to enter the system brand. Enter the values as specified by service and support.
4. Click **Continue**. Your system brand setting and the following notice are displayed:  
Attention: Once set, this value cannot be changed unless it is 'P0', and then only to 'D0'.
5. Click **Save settings** to update the system brand and save it to the VPD.

#### Setting the system identifiers:

Set the system-unique ID, system serial number, machine type, and machine model.

You can set the system-unique ID, serial number, machine type, and machine model. If you do not know the system-unique ID, contact your next level of support.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

**Note:** You cannot boot the system until valid values are entered for all fields. You can change these entries only once.

To set the system keywords, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Program Vital Product Data**.
3. Select **System Keywords**.
4. In the right pane, enter the desired values for the system serial number, machine type, and machine model using the naming convention shown in the ASMI help. Set the **Reserved** field to blank spaces unless directed otherwise by service and support.
5. Click **Continue**. The data validation panel is displayed, which includes your entered settings.
6. Click **Save settings** to update the system keywords and save them to the VPD.



### Setting the system enclosure type:

Set values that uniquely identify the type of enclosures attached to the system.

When setting the system enclosure type, ensure that the enclosure serial number field matches the original value, which can be found on a label affixed to the unit. Updating the enclosure serial field keeps the configuration and error information synchronized, and this information is used by the system when creating the location codes. This task must be done using the ASMI, not with the control panel. However, if you do not have access to the ASMI, the system will still operate without updating this information.

For example, when replacing the I/O backplane, you must re-enter the original enclosure serial number into the enclosure serial number field to overwrite the serial number that is recorded for the new I/O backplane. Failure to enter the correct enclosure serial number will result in logical partition mappings being incorrect.

**Note:** You cannot boot the system until valid values are entered for all fields in the enclosure-type information.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To change the system enclosure type, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** → **Program Vital Product Data**.
3. Select **System Enclosures**. In the right pane, the current system enclosures are displayed.
4. Enter the desired settings for the **Enclosure location**, **Feature Code/Sequence Number**, and **Enclosure serial number** fields using the naming convention described in the ASMI help.  
The value of the **Enclosure serial number** field is different than the serial number of the system. Set the **Reserved** field to blank spaces unless directed otherwise by service and support.
5. Click **Save settings** to update the system enclosure type information and save it to the VPD.

### Changing service indicators

Turn off system attention indicator, enable enclosure indicators, change indicators by location code, and perform an LED test on the control panel.

The service indicators alert you that the system requires attention or service. It also provides a method for identifying a field-replaceable unit (FRU) or a specific enclosure within the system.

A hierarchical relationship exists between FRU indicators and enclosure indicators. If any FRU indicator is in an *identify* state, then the corresponding enclosure indicator will change to an *identify* state automatically. You cannot turn off the enclosure indicator until all FRU indicators within that enclosure are in an *off* state.

### Turning off system attention indicator:

Learn how to turn off the system attention indicator.

The system attention indicator provides a visual signal that the system as a whole requires attention or service. Each system has a single system attention indicator. When an event occurs that either needs your intervention or that of service and support, the system attention indicator lights continuously. The system attention indicator is turned on when an entry is made in the service processor error log. The error entry is transmitted to the system level and operating system error logs.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To turn off the system attention indicator, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Service Indicators**.
3. Select **System Attention Indicator**.
4. In the right pane, click **Turn off system attention indicator**. If the attempt is unsuccessful, an error message is displayed.

### Enabling enclosure indicators:

Find out how to display and change FRU indicators within each enclosure.

You can turn on or off the *identify* indicators in each enclosure. An *enclosure* is a group of indicators. For example, a processing unit enclosure represents all of the indicators within the processing unit and an I/O enclosure represents all of the indicators within that I/O enclosure. Enclosures are listed by their location code.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To enable the enclosure indicator states, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Service Indicators**.
3. Select **Enclosure Indicators**.
4. Select the enclosure of choice and click **Continue**.
5. Make the necessary changes to the selection list located next to each location code.
6. To save the changes made to the state of one or more FRU indicators, click **Save settings**.  
To turn off all of the indicators for this enclosure, click **Turn off all**. A report page is displayed indicating success or failure.

### Changing indicators by location code:

You can specify the location code of any indicator to view or modify its current state. If you provide the wrong location code, the advanced system manager attempts to go to the next higher level of the location code.

The next level is the base-level location code for that field replaceable unit (FRU). For example, a user types the location code for the FRU located on the second I/O slot of the third enclosure in the system. If the location code for the second I/O slot is incorrect (the FRU does not exist at this location), an attempt to set the indicator for the third enclosure is initiated. This process continues until a FRU is located or no other level is available.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To change the current state of an indicator, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.

2. In the navigation area, expand **System Configuration** and **Service Indicators**.
3. Select **Indicators by Location code**.
4. In the right pane, enter the location code of the FRU and click **Continue**.
5. Select the preferred state from the list.
6. Click **Save settings**.

#### Performing an LED test on the control panel:

You can perform an LED test on the control panel to determine if one of the LEDs is not functioning properly.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To perform an LED test on the control panel, perform the following task:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Configuration** and **Service Indicators**.
3. Select **Lamp Test**.
4. On the Lamp Test pane, click **Continue** to perform the lamp test. The test changes all indicators to the *identify* state for a short time (approximately 4 minutes).

## Setting performance options

You might enhance the performance of your managed system by changing the logical memory block size and increasing the system memory page size.

### Changing the logical memory block size

You might enhance the managed system performance by manually or automatically changing the logical memory block size.

The system kernel uses the memory block size to read and write files. By default, the logical memory block size is set to **Automatic**. This setting allows the system to set the logical block memory size based on the physical memory available. You can also manually change the logical memory block size.

To select a reasonable logical block size for your system, consider both the performance desired and the physical memory size. Use the following guidelines when selecting logical block sizes:

- On systems with a small amount of memory installed (2 GB or less), a large logical memory block size results in the firmware consuming an excessive amount of memory. Firmware must consume at least 1 logical memory block. As a general rule, select the logical memory block size to be no greater than 1/8th the size of the system's physical memory.
- On systems with a large amount of memory installed, small logical memory block sizes result in a large number of logical memory blocks. Because each logical memory block must be managed during boot, a large number of logical memory blocks can cause boot performance problems. As a general rule, limit the number of logical memory blocks to 8 K or less.

**Note:** The logical memory block size can be changed at run time, but the change does not take effect until the system is restarted.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure logical memory block size, perform the following task:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Performance Setup**.
3. Select **Logical Memory Block Size**.
4. In the right pane, select the logical memory block size and click **Save settings**.

## Increasing the system memory page size

Improve your system performance by setting up the system with larger memory pages.

You can improve your system performance by setting up the system with larger memory pages. Performance improvements vary depending on the applications running on your system. Only change this setting if advised by service and support.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To set up your system with larger memory pages, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Performance Setup**.
3. Select **System Memory Page Setup**.
4. In the right pane, select the settings that you want.
5. Click **Save settings**.

## Configuring network services

Use ASMI to configure network interfaces, configure network access, and debug the virtual TTY.

### Configuring network interfaces

Configure the number and type of network interfaces according to the needs of your system.

You can configure network interfaces on the system. The number and type of interfaces vary according to the specific needs of your system.

**Attention:** This operation can be performed when the system is powered on as well as powered off. Because network configuration changes occur immediately, existing network sessions, such as HMC connections, are stopped. If a firmware update is in progress, do not perform this operation. The new settings must be used to re-establish any network connections. Additional errors might also be logged if the system is powered on.

You can change the network configurations when the system is in any state.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure network interfaces, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Network Services**.
3. Select **Network Configuration**.

**Important:** If you are attempting to configure a network connection on a multi-drawer system, you must select the primary or secondary service processor, and then click **Continue**.

4. In the right pane, locate the interface that you want to change. Select the box corresponding to the **Configure this interface?** field of the identified interface. If this box is not selected, the corresponding field changes are ignored.
5. Select the **Type of IP address** from the following options:
  - Static** The IP address, subnet mask, broadcast address, default gateway and first DNS server address must be entered. The second and third DNS server addresses are optional.
  - Dynamic**  
No additional input is required.
6. Click **Continue**. The next screen allows you to verify the IP settings that have been entered.

**Attention:** If incorrect network configuration information is entered, you may not be able to use the ASMI after the changes are made. To remedy this situation, you must reset the service processor to the default settings by removing the service processor assembly from the server and moving the reset jumpers. Resetting the service processor also resets all user IDs and passwords to their default values.

**Note:** Click **Reset Network Configuration** to reset Network Configuration settings to their default factory settings.
7. Click **Save settings** to make the changes.

## Configuring network access

Specify which IP addresses will be allowed to access the server.

When you configure network access, you specify which IP addresses can access the service processor. You can specify a list of allowed IP addresses and a list of denied IP addresses.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure network access, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Network Services**.
3. Select **Network Access**. In the right pane, the **IP address** field displays the IP address of the server that your browser is running on and that connects to the ASMI.
4. Specify up to 16 addresses each for the list of allowed addresses and the list of denied addresses. ALL is a valid IP address.

If a login is received from an IP address that matches a complete or partial IP address in the allowed list, access to the service processor is granted. Access to the service processor is not allowed if a login is received from an IP address that matches a complete or partial IP address from the denied list.

**Note:** The allowed list takes priority over the denied list, and an empty denied list is ignored. ALL is not allowed in the denied list if the allowed list is empty.

5. Click **Save settings** to validate the data.

## Debugging the virtual TTY

Debug the virtual TTY from the master service processor.

You can gather additional debug information from a failing system by using the debug virtual server (DVS). The DVS enables communication with the server firmware and partition firmware. DVS allows a maximum of eight open connections. External interfaces such as the ASMI and service processor remote application can communicate with the server firmware and partition firmware through DVS. This communication is bidirectional. External interfaces can send a message to the server firmware and partition firmware through DVS.

DVS uses the partition ID and session ID to distinguish between the server firmware and partition firmware. The range for both the partition ID and session ID is 0 to 255. Clients, such as the ASMI, interact with DVS using a TCP/IP socket. Port 30002 on the service processor is used for this communication.

The partition ID and the session ID parameters must be specified to start communicating. After specifying both parameters, a telnet session must be opened to send messages. The telnet session must be started and messages must be sent within the time-out period of 15 minutes. If both actions are not taken within the time-out period, the connection is closed.

To perform this operation, your authority level must be authorized service provider.

To debug the virtual TTY, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **Network Services**.
3. Select **Debug Virtual TTY**.
4. In the right pane, enter the partition and session IDs.
5. Click **Save settings**.

## Troubleshooting

Troubleshoot common problems associated with setting up access to the ASMI, and learn how to view and customize troubleshooting information using various service aids.

### Troubleshooting problems in accessing the ASMI

Troubleshoot common problems associated with setting up access to the ASMI.

The following table contains information about common problems that might occur while you are trying to access the Advanced System Management Interface (ASMI) through a Web browser. The table also provides common resolutions to those problems.

*Table 20. Troubleshooting problems when trying to access the ASMI through a Web browser*

Problem	Resolution
After you enter the server's IP address in the Web browser, you receive a security alert.	Usually this means that your PC or mobile computer does not accept the server as a secure site. To resolve this problem, complete the following steps: <ol style="list-style-type: none"><li>1. In the Client Authentication window, select the certificate you want to use when connecting and click <b>OK</b>.</li><li>2. If you receive the error that this page cannot be found, your PC or mobile computer does not trust the server as a secure site. If you have a firewall on your PC or mobile computer, modify the firewall settings to trust the server's IP address. Then, type the IP address in the Address field of your PC's or mobile computer's Web browser.</li><li>3. On the Security Alert window, click <b>Yes</b>.</li></ol>

Table 20. Troubleshooting problems when trying to access the ASMI through a Web browser (continued)

Problem	Resolution
After you enter the server's IP address in the Web browser, the browser displays an error message stating that it cannot find the IP address that you entered.	<ol style="list-style-type: none"> <li>1. Ensure that you entered <code>https://&lt;IP address of server&gt;</code> in the Address field of your Web browser.</li> <li>2. Ensure that you entered the correct IP address for the server. See Table 14 on page 248 for a list of IP addresses for the server.</li> <li>3. Add a routing entry to the PC or mobile computer so that the PC or mobile computer can locate the server on the network. For example, if you are using a PC installed with Windows, open a command line prompt and type <code>route add &lt;server IP address&gt; mask 255.255.255.0 &lt;PC or mobile computer IP address&gt; metric 1</code>.</li> </ol>
You are using Microsoft Internet Explorer 6.0 running on Windows XP, you have correctly cabled the PC or mobile computer to the server, and you cannot access the ASMI.	<p>Usually this means that the Use TLS 1.0 option in Microsoft Internet Explorer is enabled. To connect to the ASMI, this option must be disabled. To resolve this problem, complete the following steps:</p> <ol style="list-style-type: none"> <li>1. From the <b>Tools</b> menu in Microsoft Internet Explorer, select <b>Internet Options</b>.</li> <li>2. From the Internet Options window, click the <b>Advanced</b> tab.</li> <li>3. Clear the <b>Use TLS 1.0</b> check box (in the Security category) and click <b>OK</b>.</li> </ol>
You are locked out of the ASMI after you enter the default user ID and password either incorrectly or more than five times.	<p>Reset the default password and network settings to the default settings using one of the following methods:</p> <ul style="list-style-type: none"> <li>• Ask your authorized service provider to obtain a new login password.</li> <li>• Use the service processor reset toggle switches to reset the default password and network settings; refer to Table 18 on page 251. This task requires removing the service processor card from the server. For instructions, see the <i>Customer-Installable Features for the IBM System p 570 (9117-MMA)</i>, SA76-0104.</li> </ul>

## Troubleshooting the server using service aids

View and customize troubleshooting information with various service aids (such as viewing error logs and initiating service processor dumps).

**Note:** Each system port is disabled when a Hardware Management Console (HMC) is attached to the server, and the server is booted beyond the service processor standby state.

### Displaying error and event logs:

Display a list of all of the error and event logs in the service processor.

You can view error and event logs that are generated by various service processor firmware components. The content of these logs can be useful in solving hardware or server firmware problems.

To perform this operation, your authority level must be one of the following:

- General
- Administrator
- Authorized service provider



Informational, error, and miscellaneous logs can be viewed by all authority levels. Hidden error logs can be viewed by authorized service providers.

The following table shows error log types that might be displayed, the conditions that make an error log specific to that error log type, and the user authority level that will allow you to view specific types of error logs:

Table 21. Error log types

Error log type	Conditions		User availability
	Severity	Action	
Informational logs	Informational	Report to operating system (OS) but not hidden	Available to all users
Error logs	Not informational	Report to OS but not hidden	Available to all users
Hidden logs	Not informational and informational	Report to OS, hidden, or both	Available only to the authorized service provider and users with higher authority.
Miscellaneous	Informational	Not reported to OS	Available to all users

To view error and event logs in summary or full detailed format, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** and click **Error/Event Logs**. If log entries exist, a list of error and event log entries is displayed in a summary view.
3. To view the full detail format of any of the logs listed, select the log's corresponding check box and click **Show details**. When multiple logs are selected, any action applies to each selected log. The full detail information might span several pages. The contents and layout of the full detail output is defined by the event or error logging component.
4. Click **Mark as reported** to mark platform error entries whose underlying causes have been resolved. By doing so, these entries are not reported to the operating system again when the system reboots. After they are marked, these errors can be overwritten by other errors logged in the service processor history log.

**Note:** The **Mark as reported** button is available only when your authority level is an authorized service provider.

### Enabling serial port snoop:

Specify parameters (including the snoop string) for enabling a serial port (system port) snoop.

You can disable or enable a snoop operation on a system port. When enabled, data received on the selected port is examined, or *snooped*, as it arrives. You can also specify the snoop string, a particular sequence of bytes that resets the service processor if detected. The system port S1 serves as a "catchall" reset device.

**Note:** Each system port is disabled when a Hardware Management Console (HMC) is attached to the server, and the server is booted beyond the service processor standby state.

To perform this operation, your authority level must be one of the following:

- General
- Administrator



- Authorized service provider

To view and change the current Serial Port Snoop settings, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** and select **Serial Port Snoop**.
3. Disable or enable snooping on system port S1. The default is *Disabled*.
4. Enter the desired snoop string, up to 32 bytes, into the **Snoop string** field. The current value displayed is the default. Ensure that the string is not a commonly used string. A mixed-case string is recommended.
5. Click **Update snoop parameters** to update the service processor with the selected values.

**Note:** After the snoop operation is correctly configured, at any point after the system is booted to AIX, the system uses the service processor reboot policy to restart whenever the reset string is typed on an ASCII terminal attached to system port S1.

### Initiating a system dump:

Control how frequently a system dump is performed and the amount of data collected from the hardware and server firmware.

You can initiate a system dump in order to capture overall system information, system processor state, hardware scan rings, caches, and other information. This information can be used to resolve a hardware or server firmware problem. A *system dump* can also be automatically initiated after a system malfunction, such as a checkstop or hang. It is typically 34 MB.

**Note:** Use this procedure only under the direction of your service provider.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure and initiate a system dump, do the following:

1. Perform a controlled shutdown of the operating system if possible.
2. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
3. In the navigation area, expand **System Service Aids** and click **System dump**.
4. From the selection list labeled **Dump policy**, select the policy to determine when an automatic system dump is collected.

The dump policy is used whenever a system error condition is automatically detected by the system. In addition to the dump policy, the platform firmware determines whether a dump is recommended, based on the type of error that has occurred. This recommendation is combined with the dump policy to determine if a system dump will be initiated.

The dump policy options are the following:

#### As needed

Collects the dump data only for specific reasons. This is the default setting for the dump policy.

#### Always

Collects the dump data after the system locks up or after a checkstop. This setting overrides the firmware recommendation and forces a system dump, even when it is not recommended.

**Note:** The dump policy only defines when a system dump is performed. It does not define what to dump nor the size of the information to be dumped. Those parameters are controlled by the **Hardware content** settings.

5. Select the policy to determine how much data to dump from the selection list labeled **Hardware content**.

The system firmware makes a recommendation for the dump content based on the type of error that has occurred. This recommendation is combined with the hardware content to determine how much dump data is actually collected.

The dump policy options available are the following:

- **Automatic** Collects dump data automatically. The firmware decides which dump content is best, depending on the type of failure. This is the default setting for the hardware content.
- **Minimum** Collects the minimum amount of dump data. Collection of hardware dump data can be time-consuming. This selection allows the user to minimize the content of the hardware portion of the system dump. It also allows the system to reboot as quickly as possible.

**Note:** If this option is selected, the debug data collected for some errors may be insufficient. The capturing of relevant error data for some errors may be sacrificed for less system downtime.

- **Medium** Collects a moderate amount of hardware error data. More data is captured with this setting than the minimum setting, and less time is needed for dump data collection in comparison to the maximum setting.
- **Maximum** Collects the maximum amount of hardware error data. This setting gives the most complete error coverage but requires more system downtime in relation to the other policies. It is expected to be used in rare cases by authorized service providers if you are willing to sacrifice reboot speed for error capture on a first failure, or if difficult problems are being analyzed.

**Note:** If this option is selected, the collection of hardware dump data can be time-consuming, especially for systems with a large number of processors.

6. In the **Server firmware content** field, select the content level that indicates the amount of data to dump for the server firmware portion of the system dump.
7. Click **Save settings** to save the setting changes.

To save the setting changes and instruct the system to immediately process a dump with the current settings, click **Save settings and initiate dump**.

For information about copying, reporting, and deleting the dump using the HMC, see “Manage Dumps” on page 60.

### Initiating a service processor dump:

Enable or disable the service processor dump in addition to immediately initiating a service processor dump.

Use this procedure only under the direction of your hardware service provider. With this function, you can preserve error data after a service processor application failure, external reset, or user request for a service processor dump. The existing service processor dump is considered valid if neither the server firmware nor Hardware Management Console (HMC) has collected the previous failure data.

To perform this operation, your authority level must be authorized service provider.

To enable or disable the service processor dump and view the status of the existing service processor dump, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** and click **Service Processor Dump**.
3. Select either **Enable** or **Disable** from the selection list. By default, the state is *Enable*. The current setting is displayed and the status of an existing service processor dump is displayed as valid or invalid.

**Note:** You cannot perform a user-requested service processor dump when this setting is disabled.

4. Click **Save settings** to save the setting changes.

To save the setting changes and instruct the system to immediately process a service processor dump with the current settings, click **Save settings and initiate dump**.

For information about copying, reporting, and deleting dumps on the HMC, see “Manage Dumps” on page 60.

### Initiating a partition dump:

Enable or disable the partition dump in addition to immediately initiating a partition dump.

Use this procedure only under the direction of your hardware service provider. By initiating a partition dump, you can preserve error data that can be used to diagnose server firmware or operating system problems. The state of the operating system is saved on the hard disk and the partition restarts. This function can be used when the operating system is in an abnormal wait state or endless loop.

**Attention:** You might experience data loss when using this operation. This feature is only available on non-HMC managed systems that have the system server firmware in the *Running* state.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To perform a partition dump, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids** and click **Partition Dump**.
3. Select **Partition Dump**.

### Configuring a system port for call options:

Configure a system port for use with the call-home and call-in options.

You can configure a system port used with the call-home and call-in features. You can also set the baud rate for a system port.

**Note:** Each system port is disabled when a Hardware Management Console (HMC) is attached to the server, and the server is booted beyond the service processor standby state. Therefore, these menus are not present if the system is managed by an HMC, or if the system has no ports.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure a system port, complete the following steps:

1. In the navigation area, expand **System Service Aids** and click **Serial Port Setup**. Two sections are displayed. The first section is labeled **S1**, which is the system port that is used with the call-home feature. The second section is labeled **S2**, which is the system port that is used with the call-in feature.
2. Modify the appropriate fields in the **S1** and **S2** sections.

#### Baud rate

Select the baud rate for this system port. If a terminal is attached to this port, the settings must match. The speeds available are 50, 300, 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bps.

**Character size**

Select the character size for this system port. If a terminal is attached to this port, the settings must match.

**Stop bits**

Select the number of stop bits for this system port. If a terminal is attached to this port, the settings must match.

**Parity** Select the parity for this system port. If a terminal is attached to this port, the settings must match.

3. Click **Save settings** to save the setting changes.

**Configuring your modem:**

Configure your modem that is connected to the system port.

**Note:** Each system port is disabled when a Hardware Management Console (HMC) is attached to the server, and the server is booted beyond the service processor standby state.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure the modem, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Modem Configuration**. Two sections are displayed. The first section is labeled **S1**, which is the system port that is used with the call-home feature. The second section is labeled **S2**, which is the system port that is used with the call-in feature.
4. Modify the fields in the **S1** and **S2** sections.
  - **Modem type** Select the supported modem type from the selection list.
  - **Modem reset command** Enter the command to use to reset the modem to the power-on defaults.
  - **Modem initialization command** This command configures the modem for the required behavior. To ensure proper operation, result codes should be returned (ATQ0), echo should be disabled (ATE0), and result codes should be strings (ATV1). This setting is ignored if the modem type is not Custom.
  - **Modem dial command** This command is used for dialing a number. For example, ATDT for tone dialing. This setting is ignored if the modem type is not Custom.
  - **Modem auto-answer command** This command enables the modem to answer incoming calls. For example, ATS0=1. This setting is ignored if the modem type is not Custom.
  - **Modem pager dial command** Enter the modem pager dial command. This command is used to dial a pager. For example: ATDT%s,,,%s;ATH0.

**Note:** Both %s strings are required. This setting is ignored if the modem type is not Custom.

- **Modem disconnect command** Enter the modem disconnection command. This command is used to disconnect the call. For example, +++ATH0. This setting is ignored if the modem type is not Custom.
5. Click **Save settings** to save the modem configuration changes.

**Configuring the call-home and call-in policy:**

Configure your system to call home and call in.

You can select which system port is used to call home and to call in, set various telephone numbers, and add customer information.

**Note:**

- The modem is required to be configured on each call-in and call-home enabled system port.
- Each system port is disabled when a Hardware Management Console (HMC) is attached to the server, and the server is booted beyond the service processor standby state.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To configure the call-in and call-home policies, complete the following steps:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Call-in/Call-home**.
4. Enter the desired text into the specified fields.
  - **Call-home policy**
    - **Call-home serial port** Select a system port for call-home or select **Disabled** to disable call-home.
    - **Call-in serial port** Select a system port for call-in or select **Disabled** to disable call-in.
    - **Call-home dialing policy** Select the dialing policy for call-home. Select **First** to call the telephone numbers in sequence and to stop at the first successful call-home, or select **All** to call all of the telephone numbers.
    - **Number of retries** This setting is the number of times the server should retry calls that were unsuccessful.
  - **Telephone numbers**
    - **Service center telephone number** This is the number of the service center computer. The service center usually includes a computer that takes calls from servers with call-out capability. This computer is referred to as the **catcher**. The **catcher** expects messages in a specific format to which the service processor conforms. For more information about the format and **catcher** computers, refer to the readme file in the AIX `/usr/samples/syscatch` directory. Contact your authorized service provider for the correct service center telephone number to enter. Until you have that number, leave this field unassigned.
    - **Customer administration center telephone number** This is the number of the system administration center computer (catcher) that receives problem calls from servers. Contact your system administrator for the correct telephone number to enter here. Until you have that number, leave this field unassigned.
    - **Digital pager telephone number** This is the number for a numeric pager carried by someone who responds to problem calls from your server. Contact your administration center representative for the correct telephone number to enter.
    - **Pager numeric data** Enter the numeric data to be sent during a pager call.
  - **Customer account**
    - **Customer RETAIN<sup>®</sup> account number** This is the number assigned by your RETAIN service provider for record keeping and billing. Enter your account number.
    - **Customer RETAIN login user ID** Enter the RETAIN login user ID. Leave this field unassigned if your service provider does not use RETAIN.
    - **Customer RETAIN login password** Enter the RETAIN account password. Leave this field unassigned if your service provider does not use RETAIN.
    - **Primary RETAIN server IP address** Enter the IP address of the primary RETAIN server.
    - **Secondary RETAIN server IP address** Enter the IP address of the secondary RETAIN server.

- **Customer site user ID** Enter the user ID for your problem reporting center.
- **Customer site password** Enter the password for your problem reporting center.
- **Customer company information**

5. Click **Save settings** to save changes.

### Testing the call-home policy:

You can test the call-home policy configuration after the modem is installed and configured correctly.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To test your call-home policy configuration, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Call-Home Test**.
4. Click **Initiate call-home test**. A test of the call-home system is performed as specified by the current port and modem selections.

### Rebooting the service processor:

Reboot the service processor.

In critical system situations, such as during system hangs, you can reboot the service processor. Perform this task only when directed by your service provider.

To perform this operation, your authority level must be one of the following:

- Administrator
- Authorized service provider

To reboot your service processor, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Reset Service Processor**.
4. Click **Continue** to perform the reboot.

### Restoring your server to factory settings:

Restore firmware settings, network configuration, and passwords to their factory defaults.

You can reset all the factory settings on your server to the factory default settings, or you can choose to reset specific settings by using the following options:

- Reset all settings
- Reset the service processor settings
- Reset the server firmware settings
- Reset the PCI bus configuration

If you choose to reset all settings, all three of these actions are performed resulting in the service processor settings, the server firmware settings, and the PCI bus configuration being reset in one operation.



**Note:** If redundant service processors are installed and enabled, whichever type of reset operation that you perform on the primary service processor will also be performed on the secondary service processor.

**Attention:** Reset your server settings to the factory default only when directed by your service provider. Before you reset all settings, make sure you have manually recorded all settings that need to be preserved. This operation can be performed only if the identical level of firmware exists on both the permanent firmware boot side, also known as the P side, and the temporary firmware boot side, also known as the T side.

Resetting the service processor settings results in the loss of all system settings (such as the HMC access and ASMI passwords, time of day, network configuration, and hardware deconfiguration policies) that you may have set through user interfaces.

**Attention:** Resetting the server firmware settings results in the loss of all of the partition data that is stored on the service processor.

Resetting the PCI bus configuration results in the following sequence of events:

- The service processor instructs the server firmware to power on and enter into a standby state.
- When the server firmware has entered into the standby state, the PCI bus configuration settings are cleared.
- The server firmware then powers off and the service processor is in the standby state.

**Attention:** Resetting all settings results in the loss of system settings as described for each option in the preceding paragraphs. Also, you will lose the system error logs and partition-related information.

To restore factory default settings, your authority level must be one of the following:

- Administrator
- Authorized service provider

To restore factory default settings, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Factory Configuration**.
4. Select the options that you want to restore to factory settings.
5. Click **Continue**. The service processor reboots after all settings have been reset.

#### **Entering service processor commands:**

Enter commands to perform on the service processor.

You can enter commands to perform on the service processor. Currently, no syntactical validation is performed on the command string that is entered. As a result, ensure that the command is entered correctly before initiating the action.

To perform this operation, your authority level must be an authorized service provider.

To enter service processor commands, do the following:

1. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
2. In the navigation area, expand **System Service Aids**.
3. Select **Service Processor Command Line**.
4. Enter a valid command that does not exceed 80 characters.

**Note:** Entering a command that is not valid might hang the system. If this condition occurs, reset the service processor.

5. Click **Execute** to perform the command on the service processor.

---

## Managing the control panel functions

The control panel functions allow you to interface with the server. Control panel functions range in complexity from functions that display status (such as IPL speed) to low-level service functions that only service representatives must access.

### Physical control panel

The physical control panel is your initial interface with the server. You can use the physical control panel to perform functions such as IPL, power on, and power off.

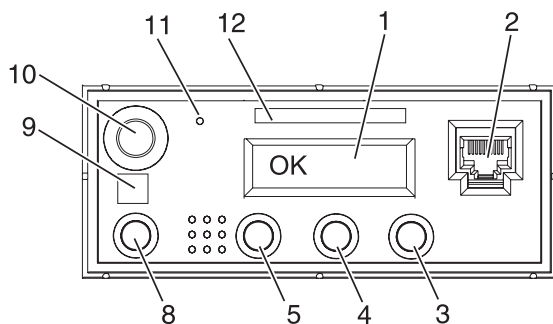


Figure 22. 570 control panel

- |    |   |
|----|---|
| 1  | Function/Data display   |
| 2  | Serial port   |
| 3  | Increment button  |
| 4  | Enter button  |
| 5  | Decrement button  |
| 8  | System reset button   |
| 9  | Power LED   |
|    | <ul style="list-style-type: none"><li>• A blinking light indicates standby power to the unit.</li><li>• A constant light indicates full system power to the unit.</li></ul> |
| 10 | Power-on button   |
| 11 | Service processor reset switch (pinhole)  |
| 12 | Serial number label   |

**Note:** There is approximately a 30-second transition period from the time the power-on button is pressed to when the power LED goes from blinking to solid. During the transition period, you might observe the blinking intervals speed up.

The system attention light is located along the upper right edge of the first drawer.



## Accessing the control panel functions using the physical control panel

Activating a control panel function with the physical control panel is a two-step procedure.

To activate a control panel function, do the following:

1. Select a function number by pressing the Increment (↑) or Decrement (↓) button on the control panel.
2. To activate the function, press Enter on the control panel.

## Putting the physical control panel in manual operating mode

You must first put the physical control panel in manual operating mode before you can select or activate certain functions.

To put the physical control panel in manual operating mode, do the following:

1. Use the Increment button to scroll to function 02.

```
0 2 _ _ _ _ _ _ _ _ _ _  
_ _ _ _ _ _ _ _ _ _
```

2. Press Enter to start function 02.

3. Press Enter again to move to the second character on the function 02 menu. The current system operating mode is displayed with a pointer, as shown in the following example:

```
0 2 _ _ B _ _ N < _ _ _ _  
_ _ _ _ _ _ _ _ _ _ P _ _ _
```

4. Use the Increment button to scroll through the system operating modes, and select M for manual, as shown in the following example:

```
0 2 _ _ B _ _ M < _ _ _ _  
_ _ _ _ _ _ _ _ _ _ P _ _ _
```

5. Press Enter to select the system operating mode.
6. Press Enter again to exit function 02.

The control panel is in manual operating mode. For information about other options in function 02, see “Function 02: Select IPL type, IPL speed override, system operating mode, and firmware mode” on page 283.

## Control panel function codes

Learn about function codes that are displayed on the control panel to indicate status and function options.

To display all functions, put the control panel in manual operating mode. See “Putting the physical control panel in manual operating mode.”

The following table includes descriptions of the primary and customer-extended control panel function codes.

Table 22. Primary and customer-extended control panel (32-character) function codes

Function code	Function selected
01	Displays the current IPL parameters. This function is available in both normal and manual operating mode.
02	Used to select the IPL type, system operating mode, IPL speed, and firmware IPL mode. This function is available in both normal and manual operating mode.
03	Restarts an IPL of the system using the selected IPL parameters. This function is available only in manual operating mode and when the system power is on.
04	Performs a lamp test; all displays and indicators are lit. This function is available in both normal and manual operating mode.

Table 22. Primary and customer-extended control panel (32-character) function codes (continued)

Function code	Function selected
05 and 06	Reserved.
07	Allows you to perform SPCN service functions. This function is available only in the manual operating mode and from power on standby.
08	Causes a fast power off. This function is available only when the system is in manual operating mode and the system power is on.
09 and 10	Reserved.
11	Displays a system reference code (SRC) on the control panel using up to 32 ASCII characters, including non-hexadecimal characters. This function is available in both normal and manual operating mode when an SRC is available.
12	Displays an SRC on the control panel using up to four extended SRC data words. This function is available in both normal and manual operating mode when an SRC is available.
13	Displays an SRC on the control panel using up to eight extended SRC data words. This function is available in both normal and manual operating mode when an SRC is available.
14 through 19	Displays an SRC on the control panel using callout data. These functions are available in both normal and manual operating mode when an SRC is available.
20	Displays the machine type and model, VPD card CCIN, and IPL types. This function is available in both normal and manual operating mode.
21	Not applicable.
22	Forces a partition dump. This function is available only in the manual operating mode and when activated by the operating system.
23 and 24	Reserved.
25 and 26	Use service switches 1 and 2 to enable or disable functions 50 through 99. These functions are available only in the manual operating mode.
27 through 29	Reserved.
30	Displays the service processor IP address and port location. This function is available only in the manual operating mode and from power on standby.
31 through 33	Reserved.
34	Not applicable.
35 through 41	Reserved.
42	Performs a platform dump. This function is available only in the manual operating mode and when activated by the operating system or the service processor.
43	Performs a service processor dump. This function is available only in the manual operating mode.
44 through 54	Reserved.
55	Displays or changes the platform dump collection policy, platform dump hardware content, and platform dump firmware content settings. This function is available only in the manual operating mode.
56 through 62	Reserved.
63	Displays up to the last 25 system status SRCs. This function is available only in the manual operation mode.
64	Displays up to the last 25 diagnostic status SRCs. This function is available only in the manual operation mode.
65 through 70	Not applicable.

Table 22. Primary and customer-extended control panel (32-character) function codes (continued)

Function code	Function selected
71 through 99	Reserved.

If you cannot find the function code in this chart, added features or devices might not have been available when this information was produced. Look on the control panel for supplemental unit function code information for the function code that you displayed.

## Primary control panel functions

Learn about the primary control panel functions that are available.

### Function 01: Display selected IPL type, system operating mode, and IPL speed

This function allows you to display the current system operating mode, the IPL speed for the next IPL, the firmware mode for the next IPL, and the operating system IPL mode (when enabled).

This function is available in both normal and manual operating mode.

This function displays the following information:

- The operating system (OS) IPL types (A, B, C, or D).
- The valid logical key modes (M or N).
- The IPL speed (F, V=F, S, V=S, H, V=H, X, or V=X).
- The firmware mode (P or T).

Table 23. Function 01 on systems without OS IPL enabled

Function/Data	Action or description
0 1 _	Use the Increment or Decrement buttons to scroll to function 01.
0 1 _ _ A _ _ M _ _ V = F _ _ _ _ _ _ _ _ _ _ _ _ _ P _ _ _	Valid OS IPL types are A, B, C, and D.  Valid system operating modes are M and N.  Valid IPL speed displays are F, V=F, S, V=S, H, V=H, X, and V=X.  Valid firmware IPL modes are P and T.
0 1 _	Use the Increment or Decrement buttons to scroll through the control panel functions.

### Function 02: Select IPL type, IPL speed override, system operating mode, and firmware mode

This function allows you to select the IPL type and logical key mode when the system is either powered on or off.

This function is available in both normal and manual operating mode.

Before you can select the IPL speed, the system must be at power on standby.

For powered-on systems, function 02 is used to select the operating system (OS) IPL type, system operation mode, or firmware IPL mode. The following table shows an example of the function 02 IPL type, system operating mode, and firmware IPL mode selection sequence for a powered-on system.

Table 24. Function 02: Select IPL type, system operating mode, and firmware IPL mode on powered-on systems

Function/Data	Action or description
0 2 _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to scroll to function 02.
0 2 _ _ A < _ M _ _ _ _ _ _ _ _ _ P _ _ _ _	Press Enter to start function 02. <ul style="list-style-type: none"> <li>The current OS IPL type is displayed with a pointer.</li> <li>The current system operating mode is displayed.</li> <li>The current firmware mode is displayed.</li> </ul>
0 2 _ _ B < _ M _ _ _ _ _ _ _ _ _ P _ _ _ _	Use the Increment or Decrement buttons to scroll through the OS IPL types.
0 2 _ _ B _ _ M < _ _ _ _ _ _ _ _ _ P _ _ _ _	Press Enter to select the OS IPL type. <ul style="list-style-type: none"> <li>The current OS IPL type is displayed.</li> <li>The current system operating mode is displayed with a pointer.</li> <li>The current firmware mode is displayed.</li> </ul>
0 2 _ _ B _ _ N < _ _ _ _ _ _ _ _ _ P _ _ _ _	Use the Increment or Decrement buttons to scroll through the system operating modes.
0 2 _ _ B _ _ N _ _ _ _ _ _ _ _ _ P < _ _ _ _	Press Enter to select the system operating mode. <ul style="list-style-type: none"> <li>The current OS IPL type is displayed.</li> <li>The current system operating mode is displayed.</li> <li>The current firmware mode is displayed with a pointer.</li> </ul>
0 2 _ _ B _ _ N _ _ _ _ _ _ _ _ _ T < _ _ _ _	Use the Increment or Decrement buttons to scroll through the firmware IPL modes.
0 2 _ _ _ _ _ _ _ _ _ _	Press Enter to select the firmware IPL mode and exit function 02.
0 1 _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to scroll through the control panel functions.

For powered-off systems, function 02 is used to select the OS IPL type, system operating mode, system IPL speed, and firmware IPL mode. The following table shows an example of the function 02 OS IPL type, system operating mode, system IPL speed, and firmware IPL mode selection sequence for a powered-off system.

Table 25. Function 02: Select IPL type, system operating mode, system IPL speed, and firmware IPL mode on powered-off systems

Function/Data	Action or description
0 2 _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to scroll to function 02.
0 2 _ _ A < _ M _ _ _ _ _ _ _ _ _ T _ _ _ _	Press Enter to start function 02. <ul style="list-style-type: none"> <li>The current OS IPL type is displayed with a pointer.</li> <li>The current system operating mode is displayed.</li> <li>The current IPL speed is displayed.</li> <li>The current firmware IPL mode is displayed.</li> </ul>
0 2 _ _ B < _ M _ _ _ _ _ _ _ _ _ T _ _ _ _	Use the Increment or Decrement buttons to scroll through the OS IPL types.

Table 25. Function 02: Select IPL type, system operating mode, system IPL speed, and firmware IPL mode on powered-off systems (continued)

Function/Data	Action or description
0 2 _ _ B _ _ M < _ _ _ V _ _ _ _ _ _ _ _ _ _ _ _ T _ _ _	Press Enter to select the IPL type. <ul style="list-style-type: none"> <li>The current IPL type is displayed.</li> <li>The current system operating mode is displayed with a pointer.</li> <li>The current IPL speed is displayed.</li> <li>The current firmware IPL mode is displayed.</li> </ul>
0 2 _ _ B _ _ N < _ _ _ V _ _ _ _ _ _ _ _ _ _ _ _ T _ _ _	Use the Increment or Decrement buttons to scroll through the system operating modes.
0 2 _ _ B _ _ N _ _ _ _ V < _ _ _ _ _ _ _ _ _ _ _ T _ _ _	Press Enter to select the system operating mode. <ul style="list-style-type: none"> <li>The current IPL type is displayed.</li> <li>The current system operation mode is displayed.</li> <li>The current IPL speed is displayed with a pointer.</li> <li>The current firmware IPL mode is displayed.</li> </ul>
0 2 _ _ B _ _ N _ _ _ _ S < _ _ _ _ _ _ _ _ _ _ _ T _ _ _	Use the Increment or Decrement buttons to scroll through the IPL speeds.
0 2 _ _ B _ _ N _ _ _ _ S _ _ _ _ _ _ _ _ _ _ _ _ T < _ _	Press Enter to select the IPL speed. <ul style="list-style-type: none"> <li>The current IPL type is displayed.</li> <li>The current system operation mode is displayed.</li> <li>The current IPL speed is displayed.</li> <li>The current firmware IPL mode is displayed with a pointer.</li> </ul>
0 2 _ _ B _ _ N _ _ _ _ S _ _ _ _ _ _ _ _ _ _ _ _ P < _ _	Use the Increment or Decrement buttons to scroll through the firmware IPL modes.
0 2 _	Press Enter to select the firmware IPL mode and exit function 02.
0 1 _	Use the Increment or Decrement buttons to scroll through the control panel functions.

### Function 03: Restart IPL

This function restarts an IPL of the system using the selected IPL parameters.

This function is available only in manual operating mode and when the system power is on.

When you select function 03 and press Enter, a restart IPL debounce is performed. The restart IPL debounce SRC (A1008003) is displayed.

Notifications are not required prior to restarting the IPL.

### Function 04: Lamp test

This function shows whether any control panel indicators are burned out and whether characters that are displayed in the Function/Data display on the control panel are valid.

This function is available in both normal and manual operating mode.

When you activate the lamp test, all of the control panel lights and indicators are lit. The lamp test continues on the system control panel for four minutes.

Use the following procedure to verify that the lights on the system control panel are working correctly. If you cannot complete these steps, see the *Problem Analysis*, SA76-0111, guide.

1. Power on the system.
2. Press the Increment (↑) or Decrement (↓) buttons on the control panel to display function 04.  
Press Enter on the control panel.
3. Do all of the lights and indicators on the system control panel come on?

Yes	No
↓	Exchange the control panel or the replaceable unit that contains the control panel function [system unit backplane (MB1) or tower card (CB1)]. See <i>Customer-Installable Features for the IBM System p 570 (9117-MMA)</i> , SA76-0104.

4. Do the expansion unit control panel lights all come on?

**Note:** The expansion unit control panel lights will be lit for only about 25 seconds after function 04 is entered.

Yes	No
↓	Exchange the control panel on the expansion unit. See <i>Customer-Installable Features for the IBM System p 570 (9117-MMA)</i> , SA76-0104.

The lights on the system control panel are working correctly.

## Function 05 to 06: Reserved

This function is reserved.

## Function 07: SPCN functions

This function allows you to perform a System Power Control Network (SPCN) operation.

This function is available only in the manual operating mode and from power on standby.

### Notes:

- The system that will display the ID must be powered off with ac power applied.
- If you have just restored power to the system, the service processor must return to standby mode before the control panel functions will work correctly. Returning the service processor to standby mode takes a few minutes *after* the panel appears to be operational.
- The control panel must be in manual operating mode to access function 07 options.

To perform an SPCN operation that is controlled by function 07, do the following:

1. Select function 07, and then press Enter. 07\*\* is displayed.
2. Select the function that you want to perform (see Table 26). Use the Increment or Decrement buttons (↑↓) to scroll to the appropriate function. Press Enter to display 07nn00, where *nn* is the function that you selected.

Table 26. SPCN functions in function 07

Function	Description	For more information
A1	Broadcasts a power-on command.	Go to step 5.
A6	Displays frame address on all I/O enclosures.	Go to step 5.


Table 26. SPCN functions in function 07 (continued)

Function	Description	For more information
A8	Displays the SPCN configuration ID number for a selected frame.	07A8 is displayed. Go to step 3.
A9	Sets the SPCN configuration ID for a selected frame.	07A9 is displayed. Go to step 4.

3. If you selected function A8 in step 2, complete the following steps to display the configuration of the I/O enclosure:
  - a. Use the Increment (↑) or Decrement (↓) buttons to select the first two characters of the frame address of the I/O enclosure, and then press Enter. 07nn00 is displayed, where nn is the first byte of the frame address.
  - b. Use the Increment (↑) or Decrement (↓) buttons to select the second two characters of the frame address of the I/O enclosure, and then press Enter. 07nn00 is displayed on the selected I/O enclosure, where nn is the second byte of the frame address.

**Notes:**

- The display on the addressed I/O enclosure is blinking on and off .
- The configuration ID is the last two characters of the bottom line.

4. If you selected function A9 in step 2, complete the following steps to set the configuration of the selected I/O enclosure:
  - a. Ensure that the system power of the selected I/O enclosure is in standby mode. If the system power of the selected I/O enclosure is not in standby mode, power it off. For instructions, go to the appropriate Service Guide on the Resource Link Web site at <http://www.ibm.com/servers/resourcelink>  . Then return to step 1.
  - b. Use the (↑) or Decrement (↓) buttons to select the first two characters of the frame address of the I/O enclosure to configure, and then press Enter. 07nn00 is displayed, where nn is the first byte of the unit address.
  - c. Use the Increment (↑) or Decrement (↓) buttons to select the second two characters of the frame address of the I/O enclosure, and then press Enter. 07nn00 is displayed, where nn is the second byte of the frame address.

**Note:** The display on the addressed I/O enclosure is blinking on and off.

- d. Use the Increment (↑) or Decrement (↓) buttons to select the correct configuration ID. 07nn is displayed, where nn is the configuration ID.
  - e. Press Enter. 07nn00 is displayed. After 20 to 30 seconds, the display on the addressed I/O enclosure stops blinking and returns to the normal display format.
5. Scroll to 07\*\* using the Increment (↑) or Decrement (↓) buttons, and then press Enter. This returns the control panel to the normal display.

## Function 08: Fast power off

This function allows you to power off the system when it is suspended.

This function is available only when the system is in manual operating mode and the system power is on.

The first time that you select function 08 and press Enter, a fast power off (FPO) debounce is performed and the system displays SRC A1008008. The second time that you select function 08 and press Enter, an FPO is performed and the system returns to its default display.

**Attention:** Because of the potential for causing a loss of data, do not use this function if you can shut down the system from the operating system.



**Note:** If you changed the system password at the most recent IPL, performing a fast power off might cause that new password information to be lost.

## Functions 09 to 10: Reserved

These functions are reserved.


### Function 11: SRC display (ASCII string)

This function displays a system reference code (SRC) on the control panel using up to 32 ASCII characters, including non-hexadecimal characters, and can be displayed in all display positions. This function serves as a diagnostic aid that helps you determine the source of a hardware or operating system problem.

This function is the default SRC display and is available in both normal and manual operating mode when an SRC is available.

Function 11, if enabled, represents the words of the SRC.

Record SRC information for error reporting. For more information, see “Collecting reference codes and system information” on page 309.

For more information about interpreting SRCs, go to the appropriate System Reference Codes guide on the Resource Link Web site at <http://www.ibm.com/servers/resourcelink> .

To use an SRC for problem analysis, see the *Problem Analysis*, SA76-0111, guide.


### Function 12: SRC display (hex words 2-5)

This function displays a system reference code (SRC) on the control panel using up to four extended SRC data words to serve as a diagnostic aid that helps you determine the source of a hardware or operating system problem.

This function is available in both normal and manual operating mode when an SRC is available.

The extended SRC data words are displayed depending on the number in the SRC. Extended SRC data words are displayed four words at a time. If any extended SRC data words exist, function 12 is scrollable. Unused words are presented as blanks in the required display.

Record SRC information for error reporting. For more information, see “Collecting reference codes and system information” on page 309.

For more information about interpreting SRCs, go to the appropriate System Reference Codes guide on the Resource Link Web site at <http://www.ibm.com/servers/resourcelink> .

To use an SRC for problem analysis, see the *Problem Analysis*, SA76-0111, guide.

### Function 13: SRC display (hex words 6-9)


This function displays a system reference code (SRC) on the control panel using up to eight extended SRC data words to serve as a diagnostic aid that helps you determine the source of a hardware or operating system problem.

This function is available in both normal and manual operating mode when an SRC is available.

The extended SRC data words are displayed depending on the number in the SRC. Extended SRC data words are displayed four words at a time. If there are only one to four extended SRC data words, function 13 is not scrollable. If there are five to eight extended SRC data words, function 13 is scrollable. Unused words are presented as blanks in the required display.



Record SRC information for error reporting. For more information, see “Collecting reference codes and system information” on page 309.

For more information about interpreting SRCs, go to the appropriate System Reference Codes guide on the Resource Link Web site at <http://www.ibm.com/servers/resourceLink> .

To use an SRC for problem analysis, see the *Problem Analysis*, SA76-0111, guide.

## Functions 14 to 19: SRC display (callouts)

These functions display a system reference code (SRC) on the control panel using callout data to serve as a diagnostic aid to help you determine the source of a hardware or operating system problem.

These functions are available in both normal and manual operating mode when an SRC is available.

Functions 14 through 19, if enabled, display field replaceable unit (FRU) and procedure callout data. This data is displayed following any present extended SRC data words. Multiple FRU and procedure callout data entries can be included with each SRC. One FRU or procedure callout data entry is displayed for each function number. Up to six different FRU or procedure callout data entries can be presented at the control panel using functions 14 through 19.

The following table shows an example of a function 14 FRU callout display selection sequence.

Table 27. Function 14: FRU callout display selection sequence


Function/Data	Action or description
1 4 _	Use the Increment or Decrement buttons to scroll to function 14.
H _ -PARTNUM CCIN _ _ U970305010ABCDE- _ _ _	Press Enter to select function 14. The FRU callout data is displayed.
1 4 _	Pressing Enter toggles between function and data display.

The following table shows an example of a function 15 procedure callout display selection sequence.

Table 28. Function 15: Procedure callout display selection sequence

Function/Data	Action or description
1 5 _	Use the Increment or Decrement buttons to scroll to function 15.
M _ -FSPSP04 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to select function 15. The procedure callout data is displayed.
1 5 _	Pressing Enter toggles between function and data display.

Record SRC information for error reporting. For more information, see “Collecting reference codes and system information” on page 309.

For more information about interpreting SRCs, go to the appropriate System Reference Codes guide on the Resource Link Web site at <http://www.ibm.com/servers/resourceLink> .

To use an SRC for problem analysis, see the *Problem Analysis*, SA76-0111, guide.

## Function 20: System type, model, feature code, and IPL type

This function displays the machine type and model, VPD card CCIN, and IPL types.

This function is available in both normal and manual operating mode.

The machine type, model, VPD card CCIN, and IPL type are displayed in the following format:

```
p p p p - m m m _ _ _ c c c c
T T T T T T T t t t t t t t
```

The values are indicated as follows:

- Values for *p* indicate the machine type.
- Values for *m* indicate the machine model.
- Values for *c* indicate the system VPD card CCIN.
- Values for *T* indicate the CEC IPL type.
- Values for *t* indicate the FSP IPL type.

Record this information with the system reference code (SRC).

If you select this function and it has not been activated, the command is rejected.

## Customer-extended panel functions

Learn about the customer-extended panel functions that are available.

### Function 21: Service tool initiation

Not applicable.

### Function 22: Partition dump

This function initiates a dump of a partition's operating system data.

This function is available only in the manual operating mode and when activated by the operating system.

You must perform two consecutive function 22 selections to initiate a partition dump. The following table shows an example of function 22.

Table 29. Function 22: Initiate a partition dump

Function/Data	Action or description
2 2 _	Use the Increment or Decrement buttons to scroll to function 22.
2 2 _ _ _ _ 0 0 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to start function 22.
A 1 0 0 3 0 2 2 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Displays the partition dump verification system reference code (SRC).
2 2 _	Use the Increment or Decrement buttons to scroll to function 22.
2 2 _ _ _ _ 0 0 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to start function 22.

## Functions 23 to 24: Reserved

These functions are reserved.

## Functions 25 and 26: Service switches 1 and 2

These functions are used to set the service function range (50 to 99).

These functions are available only in the manual operating mode.

To set the service function range (50 to 99), use function 25 to set the service representative switch 1, and then use function 26 to set the service representative switch 2.

## Functions 27 to 29: Reserved

These functions are reserved.

## Function 30: Service processor IP address and port location

This function displays the service processor IP address and port location.

This function is available only in the manual operating mode and from power on standby.

The following table shows an example of function 30.

*Table 30. Function 30: Service processor IP address and port location*

Function/Data	Action or description
3 0 _	Use the Increment or Decrement buttons to scroll to function 30.
3 0 * * _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to enter sub-function mode.
3 0 0 0 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to select an IP address 00 = SP A: ETH0 (primary enclosure) 01 = SP A: ETH1 (primary enclosure) 02 = SP B: ETH0 (secondary enclosure) 03 = SP B: ETH1 (secondary enclosure)
S P _ A : _ E T H 0 : _ _ _ T 5 9 . 5 . 1 0 5 . 2 4 3 _ _ _ _ _	Press Enter to display the selected IP address.
3 0 * * _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to select sub-function exit.
3 0 _	Press Enter to exit sub-function mode.

## Functions 31 to 33: Reserved

These functions are reserved.

## Function 34: Retry partition dump

Not applicable.

## Functions 35 to 41: Reserved

These functions are reserved.

## Function 42: Platform dump

This function initiates a platform dump.

This function is available only in the manual operating mode and when activated by the operating system or the service processor.

You can use function 42 to dump IBM POWER™ hypervisor main storage and hardware data. You must perform two consecutive function 42 selections to initiate a platform dump. The following table shows an example of function 42:

*Table 31. Function 42: Initiate a platform dump*

Function/Data	Action or description
4 2 _	Use the Increment or Decrement buttons to scroll to function 42.
4 2 _ _ _ _ 0 0 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to start function 42.
A 1 0 0 3 0 4 2 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Displays the confirmation SRC.
4 2 _	Use the Increment or Decrement buttons to scroll to function 42.
4 2 _ _ _ _ 0 0 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to start function 42.

### Function 43: Service processor dump

This function initiates a service processor dump.

This function is available only in the manual operating mode.

You must perform two consecutive function 43 selections to initiate a service processor dump. The following table shows an example of function 43.

*Table 32. Function 43: Initiate a service processor dump*

Function/Data	Action or description
4 3 _	Use the Increment or Decrement buttons to scroll to function 43.
4 3 0 0 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to confirm.
A 1 0 0 3 0 4 3 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Displays the confirmation system reference code (SRC).
4 3 _	Use the Increment or Decrement buttons to scroll to function 43.
4 3 0 0 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to confirm.

### Functions 44 to 54: Reserved

These functions are reserved.

### Function 55: View and change platform dump data

This function allows you to view and change the platform dump data.

This function is available only in the manual operating mode.

When you select function 55 and press Enter, you can view and change the platform dump collection policy, platform dump hardware content, and platform dump firmware content settings

The following table shows an example of how to view the platform dump data.

Table 33. Function 55: View the platform dump data

Function/Data	Action or description
5 5 _	Use the Increment or Decrement buttons to scroll to function 55.
5 5 * * _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to enter sub-function mode.
5 5 0 0 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to select to view the platform dump variables.
5 5 0 0 _ xxyyzz _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to execute selected sub-function. xx = Collection policy yy = Hardware content zz = Firmware content
5 5 * * _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to select sub-function exit.
5 5 _	Press Enter to exit sub-function mode.

The following table shows an example of how to change the platform dump data.

Table 34. Function 55: Change the platform dump data

Function/Data	Action or description
5 5 _	Use the Increment or Decrement buttons to scroll to function 55.
5 5 * * _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to enter sub-function mode.
5 5 0 2 _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to select to change the platform dump variable. 01 = Set platform dump collection policy to <i>disable</i> 02 = Set platform dump collection policy to <i>enable</i> 03 = N/A - will always display FF in Line 1 when selected 04 = Set platform dump hardware content to <i>maximum</i> 05 = Set platform dump hardware content to <i>automatic</i> 06 = N/A - will always display FF in Line 1 when selected 07 = N/A - will always display FF in Line 1 when selected 08 = Set platform dump firmware content to <i>minimum</i> 09 = Set platform dump firmware content to <i>maximum</i> 0A = Set platform dump firmware content to <i>physical I/O</i> 0B = Set platform dump firmware content to <i>virtual I/O</i> 0C = Set platform dump firmware content to <i>HPS cluster</i> 0D = Set platform dump firmware content to <i>InfiniBand I/O</i>
5 5 0 2 _ 0 0 _ _ _ _ _ _ _ _ _ _ _ _ _ _	Press Enter to execute selected sub-function. 00 = Accept FF = Reject

Table 34. Function 55: Change the platform dump data (continued)

Function/Data	Action or description
5 5 * _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to select sub-function exit.
5 5 _ _ _ _ _ _ _ _ _ _	Press Enter to exit sub-function mode.

## Functions 56 to 62: Reserved

These functions are reserved.

## Function 63: Display system status SRCs

This function displays system status SRCs.

This function is available only in the manual operating mode.

When you select function 63 and press Enter, you can display up to the last 25 system status SRCs.

Table 35. Function 63: Display system status SRCs

Function/Data	Action or description
6 3 _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to scroll to function 63.
6 3 * _ _ _ _ _ _ _ _ _	Press Enter to enter sub-function mode.
6 3 1 8 _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to select the address offset. <b>Note:</b> Enter a sub-function between 00 and 18 to view the SRCs in sequential order. The most recent SRC displays at the highest possible sub-function number (18). If no system status SRCs exist, then only sub-function 00 is available and it will not display an SRC when selected.
C 1 0 0 1 0 3 4 _ _ _ _ _ _ _ _ _ _	Press Enter to read the SRC data.
6 3 * _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to select sub-function exit.
6 3 _ _ _ _ _ _ _ _ _ _	Press Enter to exit sub-function mode.

## Function 64: Display diagnostic status SRCs

This function displays diagnostic status SRCs.

This function is available only in the manual operating mode.

When you select function 64 and press Enter, you can display up to the last 25 diagnostic status SRCs.

Table 36. Function 63: Display diagnostic status SRCs

Function/Data	Action or description
6 4 _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to scroll to function 64.
6 4 * _ _ _ _ _ _ _ _ _	Press Enter to enter sub-function mode.

Table 36. Function 63: Display diagnostic status SRCs (continued)

Function/Data	Action or description
6 4 0 2 _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to select the address offset. <b>Note:</b> Enter a sub-function between 00 and 18 to view the SRCs in sequential order. The most recent SRC displays at the highest possible sub-function number (18). If no diagnostic status SRCs exist, then only sub-function 00 is available and it will not display an SRC when selected.
D 1 2 3 4 5 6 7 _ _ _ _ _ _ _ _ _ _	Press Enter to read the SRC data.
6 4 * * _ _ _ _ _ _ _ _ _ _	Use the Increment or Decrement buttons to select sub-function exit.
6 4 _ _ _ _ _ _ _ _ _ _	Press Enter to exit sub-function mode.

## Functions 65 to 70: Not applicable

These functions are not applicable.

## Functions 71 to 99: Reserved

These functions are reserved.

## Values for IPL types, system operating modes, and speeds

Learn about the valid initial program load (IPL) types, system operating modes, speeds, and firmware IPL modes that are used in control panel functions.

Refer to the following tables:

- Operating system IPL types
- System operating mode values
- IPL speeds
- Firmware IPL types

**Note:** Operating system IPL types are displayed only when the operating system IPL mode has been enabled from the operating system.

Table 37. Operating system IPL types

Initial program load (IPL) type	Action or description
A	IPL from disk using copy A of the system Licensed Internal Code.
B	IPL from disk using copy B of the system Licensed Internal Code.
C	Reserved for hardware service use only.  <b>Attention:</b> Incorrect use of this function can cause severe data loss.
D	IPL from media other than load-source disk. Alternate IPL for code installation support.

Table 38. System operating mode values

System operating mode	Action or description
Manual (M)	Allows you to perform an attended IPL and provides access to restricted control panel functions.

Table 38. System operating mode values (continued)

System operating mode	Action or description
Normal (N)	Allows you to perform an unattended IPL.

Table 39. IPL speeds

IPL speed	Action or description	Details
F	Fast override for one IPL.	Fast IPL runs. Some hardware diagnostics are passed over.
S	Slow override for one IPL.	Full hardware diagnostics runs. Use this speed whenever hardware is changed, for intermittent hardware failure, or on the first installation IPL. The following diagnostics are run: <ul style="list-style-type: none"> <li>• Main storage tests.</li> <li>• Service processor inter-chip interface tests (wire test).</li> <li>• Extended logical built-in self tests.</li> </ul>
V=F	Use system-defined speed.	Fast IPL set by the system value (displayed at function 01).
V=S	Use system-defined speed.	Slow IPL set by the system value (displayed at function 01).
V	Fast IPL or slow IPL set by the system value (selected at function 02).	Function 02 selection, or the system default at each IPL.
H	Hyperboot override for one IPL.	Hyperboot IPL runs. Most hardware diagnostics are skipped and the system's cached data is used unless new VPD is discovered.
X	Extreme override for one IPL.	Extreme IPL runs. All hardware diagnostics are skipped and the system's cached data is used. There are no checks for new hardware.
V=H	Use system-defined speed.	Hyperboot IPL is set by the system value (displayed at function 01).
V=X	Use system-defined speed.	Extreme IPL is set by the system value (displayed at function 01).

Table 40. Firmware IPL types

IPL type	Action or description
P	IPL from disk using copy P of the system Licensed Internal Code.
T	IPL from disk using copy T of the system Licensed Internal Code.

## Managing the system management services

Use the menus within system management services (SMS) to view information about your system and to perform tasks such as changing the boot list and setting the network parameters. These menus can be used for AIX or Linux partitions.

## Starting the system management services

Learn how to start the system management services (SMS) from a partitioned or nonpartitioned server.



To start the SMS, select one of the options below, depending on whether the system is partitioned or nonpartitioned.

- If you have a partitioned system, complete one of the following tasks:

**Requirement:** The logical partition must be shut down.

- Use the Hardware Management Console (HMC) to activate the logical partition. (If a VTERM on the HMC is the firmware console for the partition that is being restarted, open the VTERM.)
- Use the HMC to change your partition profile properties.
  1. In the navigation area, open **Server and Partition**.
  2. Select **Server Management**.
  3. In the contents area, open the server on which the partition profile is located.
  4. Open **Partitions**.
  5. Open the logical partition for the partition profile.
  6. Right-click the partition profile and select **Properties**.
  7. Click the **Settings** tab and change the boot mode to System Management Services (SMS).
  8. Click **OK**.
  9. Activate the logical partition.

The system will reboot into the SMS menus.

- If you have a nonpartitioned system, complete one of the following tasks:
  - If the ASMI is available on a network-attached console and the system is in standby, complete the following steps:
    1. On the ASMI Welcome window, specify your user ID and password, and click **Log In**.
    2. In the navigation area, expand **Power/Restart Control** and select **Power On/Off System**.
    3. Click **Save settings** and continue system server firmware boot.
    4. Look for the POST indicators **memory**, **keyboard**, **network**, **scsi**, **speaker**, which display across the bottom of the firmware console.
    5. Press the numeric 1 key after the word **keyboard** is displayed and before the word **speaker** is displayed.
  - If the ASMI is not available and the system is in standby, complete the following steps:
    1. Press the power button on the control panel.
    2. Look for the POST indicators **memory**, **keyboard**, **network**, **scsi**, **speaker**, which display across the bottom of the firmware console.
    3. Press the numeric 1 key after the word **keyboard** is displayed and before the word **speaker** is displayed.
  - If the ASMI is not available and the system has already booted the operating system, complete the following steps:
    1. Reboot the operating system.
    2. Look for the POST indicators **memory**, **keyboard**, **network**, **scsi**, **speaker**, which display across the bottom of the firmware console.
    3. Press the numeric 1 key after the word **keyboard** is displayed and before the word **speaker** is displayed.

## Using the system management services

Learn how to use each of the system management services (SMS) menus and how each option on the menus can help you manage your system.

**Notes:**

- If the firmware console is a graphics terminal, you might be asked to enter the password for the service processor's admin user that was set using the Advanced System Management Interface (ASMI).
- In some of the following example menus, *Un* is used in place of *Ufeature\_code.model.serial number* for legibility.

If you have not performed the steps to start the system management services, see “Starting the system management services” on page 296 and select the correct procedure for your system before you continue.

The following table contains the titles of the menus or tasks that can be accessed in the SMS application. Use it to access and review the specific task that you want.

*Table 41. SMS menus and descriptions*

Menu or task	Description
Main Menu	Describes the opening menu when first starting SMS.
Select Language	You can change the language used by the SMS menus.
Setup Remote IPL	You can enable and set up the remote startup capability of your server.
Adapter Configuration	You can set the network speed, enable or disable spanning tree, and set the protocol.
Speed, Duplex	You can set the interface speed at which the card runs and select half or full duplex.
Spanning Tree Enabled	You can enable or disable the spanning tree option.
Protocol	You can set the appropriate protocol for your network.
Ping Test	You can test an adapter's network connection to a remote system.
Change SCSI Settings	You can view and change the addresses of the SCSI controllers attached to your system.
Select Console	You can select which console to use to display the SMS menus.
Select Boot Options	You can view and set various options regarding the installation devices and boot devices. The Select boot options menu gives you the following options: Select Install or Boot Device, Select Boot Devices, Multiboot Startup
Normal Mode Boot or Service Mode Boot	You can have your system perform a boot in the normal or service mode.
Hard Drive	Displays a menu identifying the different types of hard drives installed on your system. (for example, SCSI or SSA)
Set Boot Sequence	You can set the location of the device in the boot list. It gives options to Display current settings, Restore default settings, Multiboot startup, and Exiting system management services

After the SMS starts, the following menu is displayed:

Main Menu

1. Select Language
2. Setup Remote IPL (Initial Program Load)
3. Change SCSI Settings
4. Select Console
5. Select Boot Options

-----  
Navigation keys:

X = eXit System Management Services

-----  
Type the number of the menu item and press Enter or Select a Navigation key: \_

On all menus except the main menu, there are several navigation keys:

**M** Return to the main menu.

**ESC** Return to the previous menu.

**X** Exit the SMS and start the operating system.

If you enter X, you are asked to confirm your choice to exit the SMS menus and start the operating system.

When there is more than one page of information to display, there are two additional navigation keys:

**N** Display the next page of the list.

**P** Display the previous page of the list.

**Note:** The lowercase navigation key has the same effect as the uppercase key that is shown on the menu. For example, **m** or **M** returns you to the main menu.

On each menu, you are given the option of choosing a menu item and pressing Enter (if applicable), or selecting a navigation key.

### Select Language

**Note:** If you are using a TTY (ASCII) terminal, it must support the ISO-8859 character set to correctly display languages other than English. When you select this option, you can change the language used by the SMS menus.

#### SELECT LANGUAGE

1. English
2. Francais
3. Deutsch
4. Italiano
5. Espanol

#### ----- Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

-----  
Type the number of the menu item and press Enter or Select a Navigation key: \_

### Setup Remote IPL

When you select this option, you can enable and set up the remote startup capability of your server. A list of network interface card (NIC) adapters in the server is displayed. An example of this menu follows:

#### NIC Adapters

Device	Slot	Hardware Address
1. Port 1 - 2 PORT Gigabit Et	Un-P1-T9	00096bff616b
2. Port 2 - 2 PORT Gigabit Et	Un-P1-T10	00096bff616a
3. 10/100/1000 Base-TX PCI-X	Un-CB1-C03-T1	000295e3814f

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

Type the number of the menu item and press Enter or Select a Navigation key: \_

When you select an adapter, the Network Parameters menu is displayed:

#### Network Parameters

Port 1 - 2 PORT Gigabit Et    Un-P1-T9    00096bff616b

1. IP Parameters
2. Adapter Parameters
3. Ping Test

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

Type the number of the menu item and press Enter or Select a Navigation key: \_

Selecting the IP (Internet Protocol) parameters option displays the following menu:

#### IP Parameters

Port 1 - 2 PORT Gigabit Et    Un-P1-T9    00096bff616b

1. Client IP Address    [000.000.000.000]
2. Server IP Address    [000.000.000.000]
3. Gateway IP Address    [000.000.000.000]
4. Subnet Mask    [255.255.255.000]

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

Type the number of the menu item and press Enter or Select a Navigation key: \_

To change IP parameters, type the number of the parameters for which you want to change the value. Entering IP parameters on this menu automatically updates the parameters on the ping test menu.

**Attention:** If the client system and the server are on the same subnet, set the gateway IP address to [0.0.0.0].

When you select **Adapter Configuration**, you can set the network speed, enable or disable spanning tree, and set the protocol as shown in the following menu:

#### Adapter Configuration

Port 1 - 2 PORT Gigabit Et    Un-P1-T9    00096bff616b

1. Speed, Duplex
2. Spanning Tree Enabled
3. Protocol

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

Type the number of the menu item and press Enter or Select a Navigation key: \_

When you select the **Speed, Duplex** option, you can set the interface speed at which the card runs and select one of the following options. The current setting is indicated by "<===".

#### Full Duplex

This setting enables concurrent sending and receiving. This is usually wanted (and should be enabled) when your system is connected to a network switch.

#### Half Duplex

This setting requires an adapter to only send or receive at a single point in time. When your system is connected to a hub, it auto-negotiates and uses half duplex to avoid collisions.

#### Auto-negotiation

This is the process of deciding whether to work in full duplex mode or half duplex mode.

Auto-negotiation allows the adapter to decide for itself which mode is optimal depending on the type of network it is attached to.

#### Adapter Configuration

Port 1 - 2 PORT Gigabit Et    Un-P1-T9    00096bff616b

1. auto, auto
2. 10, half
3. 10, full
4. 100, half
5. 100, full

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

Type the number of the menu item and press Enter or Select a Navigation key: \_

When you select the **Spanning Tree Enabled** option, you can enable or disable the spanning tree. If this option is enabled, because the network to which the system is being attached supports spanning trees, the firmware imposes a waiting period of up to 60 seconds before the adapter is allowed to communicate with the network. If this option is disabled, the network adapter can access the network immediately after the system is connected.

The spanning tree protocol is a link-management protocol that provides path redundancy while preventing duplicate loops in a network. The spanning tree option is enabled or disabled on the network switch. If the LAN adapter port being configured with the SMS adapter menus is attached to a network switch that has the spanning tree protocol enabled, the spanning tree option on the **Adapter Configuration** menu remains enabled, which is the default. If the network switch does not support the spanning tree protocol, or it is disabled, the spanning tree option on the **Adapter Configuration** menu can be disabled. Leaving this option enabled does not affect the adapter's operation. This setting

potentially affects the ping test and NIM installation. If the port's spanning tree setting is disabled, but it is enabled on the network switch to which it is attached, the ping test and NIM installation might fail even though the network and the adapter are operational.

When you select the **Protocol** option, you can set the appropriate protocol for your network as shown in the following.

```
Protocol
Port 1 - 2 PORT Gigabit Et   Un-P1-T9   00096bff616b

1. Standard <===
2. IEEE802.3

-----
Navigation keys:
M = return to main menu
ESC key = return to previous screen      X = eXit System Management Services
-----
Type the number of the menu item and press Enter or Select a Navigation key: _
```

Select the **Ping Test** option from the network parameters menu to test an adapter's network connection to a remote system. After you select the ping test option, the same series of menus takes you through setting up the IP parameters and the adapter configuration before attempting the ping test.

#### Notes:

- After the ping test is initiated, it might take 60 seconds or longer to return a result.
- When the ping test passes or fails, the firmware stops and waits for a key to be pressed before continuing.

### Change SCSI Settings

When you select this option, you can view and change the addresses of the SCSI controllers attached to your system.

```
SCSI Utilities

1. Hardware Spin Up Delay
2. Change SCSI Id

-----
Navigation keys:
M = return to main menu
ESC key = return to previous screen      X = eXit System Management Services
-----
Type the number of the menu item and press Enter or Select a Navigation key: _
```

### Select Console

When you select the Select Console utility, you can select which console to use to display the SMS menus. This selection is only for the SMS menus and does not affect the console used by the operating system.

Follow the instructions that are displayed on the menu. The firmware automatically returns to the menu on which the POST indicators (memory, keyboard, network, SCSI, speaker) display across the bottom of the menu. Press the numeric 1 key after the word **keyboard** is displayed and before the word **speaker** is displayed to return to the SMS main menu.

**Note:** If you do not change the console to another device before removing the current console, you must reattach the current console to change your console selection.

## Select Boot Options

Select this option to view and set various options regarding the installation devices and boot devices.

1. Select Install or Boot a Device
2. Select Boot Devices
3. Multiboot Startup

-----  
Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

-----  
Type the number of the menu item and press Enter or Select a Navigation key: \_

## Select Install or Boot Device

You can select a device from which to boot or install the operating system. This option is for the current boot only.

## Select Boot Devices

You can set the boot list.

## Multiboot Startup

Toggles the multiboot startup flag, which controls whether the multiboot menu is invoked automatically on startup.

If you select **Select Install or Boot Device**, the following menu is displayed:

Select Device Type

1. Diskette
2. Tape
3. CD/DVD
4. IDE
5. Hard Drive
6. Network
7. List All Devices

-----  
Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

-----  
Type the number of the menu item and press Enter or Select a Navigation key: \_

If you select **Hard Drive**, a menu similar to the following is displayed:

#### Select Hard Drive Type

1. SCSI
2. SSA
3. SAN
4. SAS
5. SATA
6. USB
7. IDE
8. ISA
9. List All Devices

-----

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

-----

Type the number of the menu item and press Enter or Select a Navigation key: \_

If you select **SCSI**, for example, all of the SCSI adapters that are in the system, are displayed on the next menu. Depending on the devices that are installed in your system, a menu similar to the following is displayed:

Version EM310\_024

SMS 1.6 (c) Copyright IBM Corp. 2000, 2005 All rights reserved.

-----

#### Select Media Adapter

1. Un-P1-T14 /pci@80000002000000d/pci@2/pci1069,b166@1/scsi@0
2. Un-P1-T12 /pci@80000002000000f/pci@2,2/pci1069,b166@1/scsi@0
3. Un-P1-T13 /pci@80000002000000f/pci@2,2/pci1069,b166@1/scsi@1
4. List all devices

-----

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

-----

Type the number of the menu item and press Enter or Select a Navigation key: \_

When you select an adapter, the next menu displays the devices of the requested type that are attached to that adapter. In the following example, all of the SCSI hard files that are attached to the first adapter are listed:

Version EM310\_024

SMS 1.6 (c) Copyright IBM Corp. 2000, 2005 All rights reserved.

-----

Select Device Number	Device Current Position	Device Name
----------------------------	-------------------------------	----------------

1	1	SCSI 73407 MB Harddisk Un-P1-T14 /pci@80000002000000d/pci@2/pci1069,b166@1/scsi@0
---	---	---

-----

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

-----

Type the number of the menu item and press Enter or Select a Navigation key: \_

You can now select the appropriate device for this installation or boot.



When a device is selected for installing the operating system, or to boot from, the Select Task menu retrieves more information about the device, or to boot from that device in normal mode or service mode. The following is an example of this menu.

```
Select Task

SCSI 73407 MB Harddisk Un-P1-T14 /pci080000002000000d/pci02/pci1069,b16601/scsi00

1. Information
2. Normal Mode Boot
3. Service Mode Boot

-----
Navigation keys:
M = return to main menu
ESC key = return to previous screen      X = eXit System Management Services
-----
Type the number of the menu item and press Enter or Select a Navigation key: _
```

If you select either **Normal Mode Boot** or **Service Mode Boot**, the next menu asks, Are you sure? If you answer yes, the device is booted in the appropriate mode. If you answer no, the firmware returns to the Select Task menu.

### Select Boot Devices

**Note:** To minimize the search time for bootable devices, these menus follow this hierarchy:

device type -> bus type -> adapter -> devices attached to the adapter

By selecting **List All Devices** from the Select Device Type menu or the Select Media Type menu, you can view all of the potentially bootable devices at one time.

The List All Devices function can take a long time on a large system with many I/O adapters and devices, such as large disk arrays.

Select **Select Boot Devices** to view and change the customized boot list, which is the sequence of devices read at startup.

```
Configure Boot Device Order

1. Select 1st Boot Device
2. Select 2nd Boot Device
3. Select 3rd Boot Device
4. Select 4th Boot Device
5. Select 5th Boot Device
6. Display Current Setting
7. Restore Default Setting

-----
Navigation keys:
M = return to main menu
ESC key = return to previous screen      X = eXit System Management Services
-----
Type the number of the menu item and press Enter or Select a Navigation key: _
```

When you select any of the options 1-5, the Select Device Type menu is displayed.

#### Select Device Type

1. Diskette
2. Tape
3. CD/DVD
4. IDE
5. Hard Drive
6. Network
7. None
8. List All Devices

---

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

---

Type the number of the menu item and press Enter or Select a Navigation key: \_

When you select a device type, such as option 5, a Select Media Type menu is displayed. The following is an example of that menu.

#### Select Media Type

1. SCSI
2. SSA
3. SAN
4. IDE
5. ISA
7. None
8. List All Devices

---

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

---

Type the number of the menu item and press Enter or Select a Navigation key: \_

When you select the media type, all adapters of that type are displayed on the Select Media Adapter menu. The following is an example of that menu for a SCSI media type.

Version EM310\_024

SMS 1.6 (c) Copyright IBM Corp. 2000, 2005 All rights reserved.

---

#### Select Media Adapter

1. Un-P1-T14 /pci@800000002000000d/pci@2/pci1069,b166@1/scsi@0
2. Un-P1-T12 /pci@800000002000000f/pci@2,2/pci1069,b166@1/scsi@0
3. Un-P1-T13 /pci@800000002000000f/pci@2,2/pci1069,b166@1/scsi@1
4. List all devices

---

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

---

Type the number of the menu item and press Enter or Select a Navigation key: \_

Then, you must select each adapter individually to see the devices that are attached to it. The following is an example of this menu for the first adapter in the previous example:

```

Version EM310_024
SMS 1.6 (c) Copyright IBM Corp. 2000, 2005 All rights reserved.
-----
Select   Device
Device   Current   Device
Number   Position   Name
-----
1         1       SCSI 73407 MB Harddisk Un-P1-T14 /pci@800000002000000d/pci@2/
                               pci1069,b166@1/scsi@0
-----

Navigation keys:
M = return to main menu
ESC key = return to previous screen          X = eXit System Management Services
-----
Type the number of the menu item and press Enter or Select a Navigation key: _

```

When you select a device type, you can view detailed information about the device or set the device location in the boot list from the Select Task menu. The following is an example of the menu for a hard disk.

```

Select Task

SCSI 73407 MB Harddisk Un-P1-T14 /pci@800000002000000d/pci@2/pci1069,b166@1/scsi@0
1. Information
2. Set Boot Sequence: Configure as 1st Boot Device
-----

Navigation keys:
M = return to main menu
ESC key = return to previous screen          X = eXit System Management Services
-----
Type the number of the menu item and press Enter or Select a Navigation key: _

```

Selecting **Information** displays a menu similar to the following for a hard disk.

```

Device Information
/pci@800000002000000d/pci@2/pci1069,b166@1/scsi@1/sd@5,0
      : (Bootable)
DEVICE      : SCSI 73407 MB Harddisk Un-P1-T14 /pci@800000002000000d/pci@2/
                               pci1069,b166@1/scsi@0
NAME        : sd
DEVICE-TYPE  : block

Parent Information
IBM,FW-ADAPTER-NAME: Ultra-320
NAME         : scsi
DEVICE-TYPE  : scsi-2
-----

Navigation keys:
M = return to main menu
ESC key = return to previous screen          X = eXit System Management Services
-----
Type the number of the menu item and press Enter or Select a Navigation key: _

```

When you select the **Set Boot Sequence** option, you can set the location of the device in the boot list.

## Display Current Settings

This option displays the current setting of the customized boot list. An example of this menu, with one device in the boot list, follows.

#### Current Boot Sequence

1. SCSI 73407 MB Harddisk Un-P1-T14 /pci080000002000000d/pci02/pci1069,b16601/scsi00
2. None
3. None
4. None
5. None

---

#### Navigation keys:

M = return to main menu

ESC key = return to previous screen

X = eXit System Management Services

---

Type the number of the menu item and press Enter or Select a Navigation key: \_

## Restore Default Settings

This option restores the boot list to the default boot list. The default boot list varies depending on the devices that are installed in the system.

The default boot list is as follows:

1. Primary diskette drive (if installed)
2. Optical drive (if installed)
3. Tape drive (if installed)
4. Hard disk drive (if installed)
5. Network adapter

## Multiboot Startup

Multiboot Startup toggles the multiboot startup flag, which controls whether the multiboot menu is invoked automatically on startup.

## Exiting system management services

After you finish using the SMS menus, type x (for exit) to boot your system.

## Power-on self-test keys

Learn how the Power-on self-test (POST) keys can start services or initiate service mode boots used for configuring the system and diagnosing problems.

After power is turned on and before the operating system is loaded, the system does a power-on self-test (POST). This test performs checks to ensure that the hardware is functioning correctly before the operating system is loaded. During the POST, a POST screen is displayed, and POST indicators appear on the firmware console (if one is connected).

The POST keys, if pressed after the keyboard POST indicator is displayed and before the last POST indicator speaker is displayed, cause the system to start services or to initiate service mode boots used for configuring the system and diagnosing problems.

**Note:** The program function keys (F1-F12) on a keyboard attached to the service processor are not used and are ignored. After the keyboard POST indicator is displayed, you must use the numeric number keys.

## Numeric 1 key

The numeric 1 key, when pressed during POST, starts the system management services interface.

### **Numeric 5 key**

The numeric 5 key, when pressed during POST, initiates a system boot in service mode using the default service mode boot list.

This mode attempts to boot from the first device of each type found in the list. It does not search for other bootable devices of that type if the first device is not bootable. Instead, it continues to the next device type in the list. The firmware supports up to five entries in the boot list.

**Note:** This is the preferred method of loading standalone AIX diagnostics from CD-ROM.

The default boot sequence is:

1. Diskette (if installed)
2. CD-ROM (if installed)
3. Hard file
4. Tape drive (if installed)
5. Network
  - a. Token ring
  - b. Ethernet

### **Numeric 6 key**

The numeric 6 key works like the numeric 5 key, except that firmware uses the customized service mode boot list that was set up by AIX when AIX was first booted, or manually using the AIX service aids.

**Note:** This is the preferred method of loading online AIX diagnostics from the boot hard disk.

---

## **Collecting reference codes and system information**

Learn how to collect reference codes and other system information.

The reference codes and system information can help determine the correct solution to fix a problem.

### **Using the control panel to collect reference codes and system information**

Learn how to use the control panel to collect reference codes and other system information.

Follow these steps to collect reference codes and system information (functions 11 through 20) using the control panel:

1. On the control panel, press the increment button until 11 is shown on the Function/Data display.
  - a. Press Enter.
  - b. Record the 32-character code: 16 characters from the first line, and 16 characters from the second line of the Function/Data display.
2. Press the increment button until 12 is shown on the Function/Data display.
  - a. Press Enter.
  - b. Record the 32-character code.
3. Press the increment button until 13 is shown on the Function/Data display.
  - a. Press Enter.
  - b. Record the 32-character code.

4. Press the increment button until 14 is shown on the Function/Data display.
  - a. Press Enter.
  - b. Record the 32-character code.
5. Press the increment button until 15 is shown on the Function/Data display.
  - a. Press Enter.
  - b. Record the 32-character code.
6. Press the increment button until 16 is shown on the Function/Data display.
  - a. Press Enter.
  - b. Record the 32-character code.
7. Press the increment button until 17 is shown on the Function/Data display.
  - a. Press Enter.
  - b. Record the 32-character code.
8. Press the increment button until 18 is shown on the Function/Data display.
  - a. Press Enter.
  - b. Record the 32-character code.
9. Press the increment button until 19 is shown on the Function/Data display.
  - a. Press Enter.
  - b. Record the 32-character code.
10. Press the increment button again until 20 is shown on the first line of the Function/Data display.
  - a. Press Enter.
  - b. Record the machine type, model, and serial number that is shown.

**Note:**

1. If 11 is shown in the Function/Data display on the control panel display, the numbers that follow are the reference codes.
2. If a number other than 11 is shown in the Function/Data display, the number might not indicate a problem with the system. These reference codes might indicate functions you select from the control panel display.
3. If you have a console with Type and Reference Code columns on it, record the data under the Type column as the first 4 characters of function 11 on the problem reporting form. If an A, B, C, or D is displayed as the first character in the Type column, use the data in the Reference Code column as the last 4 characters of function 11.

## Using AIX tools to collect reference codes and system information

Learn how to use AIX tools to collect reference codes and other system information.

1. Log in as root user, or use CE login.
2. At the command line, type `diag` and press Enter.
3. From the Function Selection menu, select **Task Selection** and press Enter.
4. Select **Display Previous Diagnostic Results** and press Enter.
5. From the Display Previous Diagnostic Results display, select **Display Diagnostic Log Summary**. The Display Diagnostic Log is displayed showing a chronological list of events.
6. Look in the **T** column for the most recent **S** entry.
7. Select this row in the table and press Enter.
8. Choose **Commit**. The details of this log entry are shown.
9. Record the SRN value shown near the end of the entry.
10. Exit to the command line.

---

## Supporting diagnostics

Learn more about procedures that can aid you in analyzing problems.

Occasionally your problem analysis will lead you to more extensive procedures that can help analyze a problem.

## Running the online and stand-alone diagnostics

Use these tools to diagnose hardware problems on your AIX or Linux systems.

Use these diagnostics only if you are directed to do so by your next level of support or your hardware service provider.

Diagnostics are available for AIX and Linux systems, which can help you perform hardware analysis. Additionally, there are various service aids in AIX diagnostics that can help you with service tasks on the system. If there is a problem, you will receive a Service Request Number (SRN) that can pinpoint the problem and determine a corrective action.

If you have AIX installed and it is running, you can perform online diagnostics. However, if the installed AIX cannot be started, or you have Linux installed, you will need to run the diagnostics from CD or from a NIM server.

### Running the online diagnostics

If you have AIX installed and it can be started, use this procedure to perform diagnostic procedures when directed from another procedure or by service and support.

When you run the online diagnostics, and AIX is installed, the support for some devices might not be automatically installed. If this happens, that device will not display in the test list when online diagnostics run.

Three modes are available for running the online diagnostics:

- **Service mode** provides the most complete check of the system resources, but requires that no other programs are running on the system. When possible, run the diagnostics in service mode.
- **Maintenance mode** allows you to check most of the available resources, with the exception of SCSI adapters, memory, processor, and the disk drive used for paging.
- **Concurrent mode** allows you to run the online diagnostics on some of the system resources while the system is running normal activity.

### Running the online diagnostics in service mode:

Use this procedure to run the online diagnostics in service mode.

Perform the following steps:

1. Stop all programs including the AIX operating system.
2. Remove all tapes, diskettes, and CDs.
3. Turn off the system unit power.
4. Turn on the system unit power.
5. After the keyboard POST indicator displays on the firmware console, and before the last POST indicator (speaker) displays, press 6 on the keyboard or ASCII terminal to indicate that a service mode boot should be initiated using the customized service mode boot list.
6. Enter any passwords, if requested.
7. When the Diagnostic Operating Instructions screen displays, follow the online instructions to check the desired resources.

8. When finished, contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs).

#### **Running the online diagnostics in maintenance mode:**

Use this procedure to run the online diagnostics in maintenance mode.

Maintenance mode requires that all activity on the system running the AIX operating system be stopped so that the online diagnostics have most of the resources available. All of the system resources, except the SCSI adapters, memory, processor, and the disk drive used for paging can be checked.

Perform the following steps to run the online diagnostics in maintenance mode:

1. Stop all programs running on the system except the AIX operating system. If you need help, contact the system administrator.
2. Log in to the AIX operating system as root user or use CE login.
3. Type the shutdown -m command to stop all activity on the AIX operating system and put it into maintenance mode.
4. When a message indicates that the system is in maintenance mode, enter the diag command to invoke the diagnostic controller so you can run the diagnostics.

**Note:** It might be necessary to set TERM type again.

5. Enter any passwords, if requested.
6. When the Diagnostic Operating Instructions screen displays, follow the online instructions to check the desired resources.

**Note:** If you do not receive the Diagnostic Operating Instructions display, try to run the stand-alone diagnostics. For details, see “Running stand-alone diagnostics” on page 313.

7. When finished, press Ctrl+D to log off from root user or CE login.
8. Contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs).

#### **Running the online diagnostics in concurrent mode:**

Use this procedure to run the online diagnostics in concurrent mode.

Use concurrent mode to run online diagnostics on some of the system resources while the system is running normal activity.

Because the system is running in normal operation, the following resources cannot be tested in concurrent mode:

- SCSI adapters connected to paging devices
- Disk drive used for paging
- Some display adapters and graphics related devices

The following levels of testing exist in concurrent mode:

##### **Share-test level**

This level tests a resource while the resource is being shared by programs running in the normal operation. This testing is mostly limited to normal commands that test for the presence of a device or adapter.



### Sub-test level

This level tests a portion of a resource while the remaining part of the resource is being used in normal operation. For example, you could test one port of a multiport device while the other ports are being used in normal operation.

### Full-test level

This level requires the device to not be assigned or used by any other operation. This level of testing on a disk drive might require the use of the vary off command. Use the diagnostics display menus to allow you to vary off the needed resource.

Perform the following steps to run online diagnostics in concurrent mode:

1. Log in to the AIX operating system as root user, or use CE login. If you need help, contact the system administrator.
2. Enter the diag command to load the diagnostic controller, and display the online diagnostic menus.
3. If requested, enter a password.
4. When the Diagnostic Operating Instructions screen displays, follow the online instructions to check the desired resources.

**Note:** If you do not receive the Diagnostic Operating Instructions display, try to run the standalone diagnostics. For details, see “Running stand-alone diagnostics.”

5. When testing is complete, press F3 to return to the Diagnostic Operating Instructions display.
6. Press F3 again to return to the AIX operating system prompt.
7. Vary on any resources that you varied off.
8. Press Ctrl+D to log off from root user or CE login.
9. When finished, contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs).

## Running stand-alone diagnostics

Learn how to perform a stand-alone diagnostic procedure from CD-ROM or a Network Installation Management (NIM) server when directed from another procedure or by your next level of support.

### Running stand-alone diagnostics from CD:

Learn how to run stand-alone diagnostics from a CD.

1. Choose from the following options:
  - If the system is powered on, continue with step 2.
  - If the system is powered off, continue with step 3.
2. If the system is powered on, perform these steps:
  - a. Let the system administrator and system users know that the system unit will be shut down.
  - b. Stop all programs including the operating system.
  - c. Continue with step 4.
3. If the system is powered off, power it on.
4. Insert the diagnostic CD in the CD drive.
5. Restart the server.
6. Continue with “Selecting testing options.”

*Selecting testing options:*

1. When the keyboard POST indicator (the word *keyboard*) is shown on the firmware console, and before the last POST indicator (the word *speaker*) is shown, press the 5 key on either the attached keyboard or the ASCII keyboard to indicate that a service mode boot should be initiated using the default service mode boot list.

2. When the Welcome screen is displayed, define the following:

- System console
- Language to be used
- Type of terminal

**Note:** Depending on the terminal emulator selected, the function keys (Fn) might not function. In this case, use the ESC key and the number in the screen menus. For example, F3 = ESC key and the #3.

3. When the Diagnostics Operating Instructions are displayed, press Enter.

**Note:** If you are unable to load the diagnostics to the point where the Diagnostic Operating Instructions display is shown, contact your next level of support or your hardware service provider.

4. From the Function Select screen, select one of the following:

- If you want to run diagnostics in Problem Determination mode, continue with the next step.
- If you want to run diagnostics in Task Selection (Service Aids) mode, go to step 11.

5. Select **Problem determination** and press Enter.

6. Check the list of resources that is displayed. Does the list of resources match what you know to be installed in your system?

- **Yes:** Continue with the next step.
- **No:** Record any information you have about the missing resource and check to ensure that the missing resource is installed correctly. If you cannot correct the problem with a missing resource, replace the missing resource (contact your service provider if necessary). To test the available resources, continue with the next step.

7. Select **All Resources**, or the specific resource or resources to be tested, and press the P7 (commit) key.

8. Record any error information you receive during the diagnostics, including service request numbers (SRNs) or SRCs, to report to your service provider.

9. When testing is complete, press the F3 key to return to the Diagnostic Operating Instructions.

10. Choose from the following options:

- To continue testing, return to step 7.
- To exit stand-alone diagnostics, select the exit function key from the menu and press Enter. Continue with step 19.

11. Select **Task Selection list** and press Enter.

12. To perform one of these tasks, select the **Task Selection** option from the Function Selection menu. After a task is selected, a resource menu might be presented showing all resources supported by the task.

13. From the Task selection list, select the service aid task you want to perform. For example, Update and manage system Flash.

14. Follow the instructions for the task selected on each menu or panel.

15. Record any information you receive during the diagnostics, including service request numbers (SRNs), to report to your service provider.

16. Record any information you receive during the diagnostics, including service request numbers (SRNs), to report to your service provider.

17. When testing is complete, press the F3 key to return to the Diagnostic Operating Instructions.

18. Choose from the following options:

- To continue testing, return to step 13.
- To exit stand-alone diagnostics, select the exit function key from the menu and press Enter. Continue with the next step.

19. Remove the CD from the drive.

20. When finished, contact your next level of support or your hardware service provider with any information you received during the diagnostics, including service request numbers (SRNs) and any missing resources.

## Performing a slow boot

Learn how to perform a slow boot using the control panel or ASMI menus depending on your configuration.

In some cases, you need to perform a slow-mode boot in order to perform extended diagnostic testing.

**Note:** A slow-mode boot might yield a new reference code on the control panel, or new errors in the service processor error log. When the server reports a new error code, record it for use in subsequent steps.

### Using the control panel to perform a slow boot

Learn how to use the control panel to perform a slow boot.

In some cases, you need to perform a slow-mode boot in order to perform extended diagnostic testing.

**Note:** A slow-mode boot might yield a new reference code on the control panel, or new errors in the service processor error log. When the server reports a new error code, record it for use in subsequent steps.

1. Record any reference codes that are displayed on the control panel. For details, see “Collecting reference codes and system information” on page 309.
2. Stop the operating system by performing the following steps:
  - a. Log in to the system as a user with the authority to run the shutdown or pwrdownsys (Power Down System) command.
  - b. At the command line, enter one of the following commands:

**Note:** These commands stop the operating system. The system power turns off, the power-on light begins to slowly blink, and the system goes into a standby state.

    - If your system is running AIX, type shutdown
    - If your system is running Linux, type shutdown -h now
3. On the control panel, use the increment or decrement buttons to scroll to function 02.
4. Press Enter to start function 02. The current IPL type (with pointer) and speed is displayed.
5. Use the increment or decrement buttons to scroll through the IPL types and speeds.
6. When manual is shown, press Enter to select the IPL type of manual. The current IPL type and speed (with pointer) is displayed.
7. Use the increment or decrement buttons to scroll through the IPL speeds.
8. When S is shown, press Enter to select the IPL speed of slow.
9. To exit function 02, press Enter multiple times until just 02 is displayed.
10. Power on the server by pressing the white power button. Then return to the procedure that caused you to perform a slow boot. **This ends the procedure.**

### Using the ASMI menus to perform a slow boot

Learn how to use the ASMI menus to perform a slow boot.

In some cases, you need to perform a slow-mode boot in order to perform extended diagnostic testing.

**Note:** A slow-mode boot might yield a new reference code on the control panel, or new errors in the service processor error log. When the server reports a new error code, record it for use in subsequent steps.

1. Record any reference codes being displayed. For details, see “Collecting reference codes and system information” on page 309.
2. Shut down the server.
3. On the ASMI Welcome pane, specify your user ID and password, and click **Log In**.
4. Expand **Power/Restart Control** and select **Power On/Off System**.
5. Record the settings so that you can re-enter them after you complete the service actions.
6. On the Power on/off system menu, select the following:
  - Select **Slow** in the Set System Boot Speed field.
  - Select **Running** in the Boot to system server firmware field.
7. Select **Save Settings**.

**Note:** These settings will apply to all future boots. After you complete the service action, change the settings back to what you recorded in step 5.

8. After you are done, return to the step in the procedure that caused you to perform a slow boot. **This ends the procedure.**

---

## Contacting IBM service and support

Use this information to learn how to contact the IBM service and support organization.

In general, the term *service* includes repair of hardware, the ability to ask usage and defect questions about your software, and on-site and remote support for any system concerns through IBM Support.

For up-to-date contact information, visit the Directory of Worldwide Contacts Web site

([www.ibm.com/planetwide/](http://www.ibm.com/planetwide/)) .

Type of problem	Call
<ul style="list-style-type: none"> <li>• Advice</li> <li>• Migrating</li> <li>• "How to"</li> <li>• Operating</li> <li>• Configuring</li> <li>• Ordering</li> <li>• Performance</li> <li>• General information</li> </ul>	<ul style="list-style-type: none"> <li>• 1-800-IBM-CALL (1-800-426-2255)</li> <li>• 1-800-IBM-4YOU (1-800-426-4968)</li> </ul>
<b>Software:</b> <ul style="list-style-type: none"> <li>• Fix information</li> <li>• Operating system problem</li> <li>• IBM application program</li> <li>• Loop, hang, or message</li> </ul> <b>Hardware:</b> <ul style="list-style-type: none"> <li>• IBM system hardware broken</li> <li>• Hardware reference code</li> <li>• IBM input/output (I/O) problem</li> <li>• Upgrade</li> </ul>	1-800-IBM-SERV (1-800-426-7378)

---

## Appendix F. Accessibility features

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products successfully.

The following list includes the major accessibility features:

- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are tactilely discernible and do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

### IBM and accessibility

See the IBM Accessibility Center at <http://www.ibm.com/able/> for more information about the commitment that IBM has to accessibility.

If you need an accessible version of this publication, send a request to [reslink@us.ibm.com](mailto:reslink@us.ibm.com). In the request, make sure that you include the publication number and the title.



---

## Notices

This information was developed for products and services offered in the U.S.A.

The manufacturer may not offer the products, services, or features discussed in this document in other countries. Consult the manufacturer's representative for information on the products and services currently available in your area. Any reference to the manufacturer's product, program, or service is not intended to state or imply that only that product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any intellectual property right of the manufacturer may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any product, program, or service.

The manufacturer may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the manufacturer.

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:** THIS INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. The manufacturer may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to Web sites not owned by the manufacturer are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this product and use of those Web sites is at your own risk.

The manufacturer may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning products not produced by this manufacturer was obtained from the suppliers of those products, their published announcements or other publicly available sources. This manufacturer has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to products not produced by this manufacturer. Questions on the capabilities of products not produced by this manufacturer should be addressed to the suppliers of those products.

All statements regarding the manufacturer's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The manufacturer's prices shown are the manufacturer's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

The drawings and specifications contained herein shall not be reproduced in whole or in part without the written permission of the manufacturer.

The manufacturer has prepared this information for use with the specific machines indicated. The manufacturer makes no representations that it is suitable for any other purpose.

The manufacturer's computer systems contain mechanisms designed to reduce the possibility of undetected data corruption or loss. This risk, however, cannot be eliminated. Users who experience unplanned outages, system failures, power fluctuations or outages, or component failures must verify the accuracy of operations performed and data saved or transmitted by the system at or near the time of the outage or failure. In addition, users must establish procedures to ensure that there is independent data verification before relying on such data in sensitive or critical operations. Users should periodically check the manufacturer's support websites for updated information and fixes applicable to the system and related software.

---

## Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM  
System p

Intel<sup>®</sup>, Intel Inside<sup>®</sup> (logos), MMX, and Pentium<sup>®</sup> are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, Windows NT<sup>®</sup>, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java<sup>™</sup> and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

UNIX<sup>®</sup> is a registered trademark of The Open Group in the United States and other countries.

Other company, product or service names may be trademarks or service marks of others.



---

## Electronic emission notices

### Class A Notices

The following Class A statements apply to the IBM System p servers that contain the POWER6 processor.

#### Federal Communications Commission (FCC) statement

**Note:** This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

#### Industry Canada Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

#### Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A respecte est conforme à la norme NMB-003 du Canada.

#### European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 89/336/EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:  
IBM Technical Regulations  
Pascalstr. 100, Stuttgart, Germany 70569  
Tele: 0049 (0)711 785 1176  
Fax: 0049 (0)711 785 1283  
E-mail: tjahn@de.ibm.com

**Warning:** This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

## VCCI Statement - Japan

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

The following is a summary of the VCCI Japanese statement in the box above.

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

## Electromagnetic Interference (EMI) Statement - People's Republic of China

### 声 明

此为 A 级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Declaration: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may need to perform practical action.

## Electromagnetic Interference (EMI) Statement - Taiwan

### 警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

The following is a summary of the EMI Taiwan statement above.

Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user will be required to take adequate measures.

**IBM Taiwan Contact Information:**

台灣IBM 產品服務聯絡方式：  
台灣國際商業機器股份有限公司  
台北市松仁路7號3樓  
電話：0800-016-888

## Electromagnetic Interference (EMI) Statement - Korea

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Please note that this equipment has obtained EMC registration for commercial use. In the event that it has been mistakenly sold or purchased, please exchange it for equipment certified for home use.

## Germany Compliance Statement

### Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

### Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 89/336/EWG in der Bundesrepublik Deutschland.

**Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336) für Geräte der Klasse A.**

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

**Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.**

---

## Terms and conditions

Permissions for the use of these publications is granted subject to the following terms and conditions.

**Personal Use:** You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of the manufacturer.

**Commercial Use:** You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of the manufacturer.

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any data, software or other intellectual property contained therein.

The manufacturer reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by the manufacturer, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

THE MANUFACTURER MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THESE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

---

# Index

## A

access control configuration 147  
Advanced System Management  
  menu 145  
asmmenu command 145

## B

back up HMC data task 93  
bar, status 38  
bkconsdata command 145  
bkprofdata command 146

## C

capacity on demand  
  change 148  
chaccfg command 147  
change  
  access control configuration 147  
  capacity on demand 148  
  capacity on demand advanced  
    functions 175  
  hardware resources 153  
  HMC user 151  
  led 159  
  media readiness 159  
  partition state 172  
  system password 171  
  system state 172  
  utilization data collection  
    settings 160  
  welcome text 175  
Change Licensed Internal Code for the  
  current release 117  
Change Network Settings task 94  
change user interface settings task 95  
change user password task 96  
chcod command 148  
chhmcusr command 151  
chhwres command 153  
chkmedia command 159  
chled command 159  
chlparutil command 160  
chsyspwd command 171  
chsysstate command 172  
chusrtca command 175  
chvet command 175  
command  
  rmlparutil 228  
command line 135  
commands  
  asmmenu 145  
  bkconsdata 145  
  bkprofdata 146  
  chaccfg 147  
  chcod 148  
  chhmcusr 151  
  chhwres 153  
  chkmedia 159

commands (*continued*)  
  chled 159  
  chlparutil 160  
  chsyspwd 171  
  chsysstate 172  
  chusrtca 175  
  chvet 175  
  cpcump 176  
  cpsysplan 177  
  defsysplanres 178  
  deploysysplan 179  
  dump 181  
  getupgfiles 182  
  hmcshutdown 183  
  hmcwin 183  
  installios 184  
  logssh 185  
  lpar\_netboot 185  
  lpcfgop 186  
  lsaccfg 187  
  lscod 188  
  lsdump 189  
  lshmc 191  
  lshmcusr 192  
  lshwinfo 193  
  lshwres 195  
  lsled 198  
  lslic 200  
  lslock 201  
  lslparutil 202  
  lsmediadev 207  
  lsrefcode 208  
  lssaccfg 209  
  lssvcevents 209  
  lssyscfg 211  
  lssysconn 213  
  lssysplan 213  
  lssysplanres 214  
  lsvet 214  
  migrfcfg 215  
  mkaccfg 215  
  mkhmcusr 216  
  mksyscfg 217  
  mksysconn 223  
  mksysplan 224  
  mkvterm 225  
  monhmc 225  
  pedbg 226  
  pesh 227  
  rmaccfg 227  
  rmhmcusr 228  
  rmlock 228  
  rmprofdata 229  
  rmsyscfg 229  
  rmsysconn 230  
  rmsysplan 232  
  rmsysplanres 232  
  rmvterm 233  
  rsthwres 233  
  rstprofdata 234  
  rstupgdata 235

commands (*continued*)  
  saveupgdata 236  
  startdump 237  
  updhmc 238  
  updlic 240  
  viosvrcmd 242  
configuration 32  
  remote operation 133  
console data  
  backup 145  
copy  
  dumps 176  
  system plan 177  
cpdump command 176  
cpsysplan command 177  
Create Serviceable Event task 107  
create system plan task 90  
create welcome text task 96  
creating  
  access control object 215  
  hmc user 216  
  system connection 223  
  system plan file 224  
  system resources 217  
custom groups 29  
  tree interface 29

## D

debug tools 226  
define  
  system plan resource 178  
defsysplanres command 178  
delete key 136  
deploy  
  system plan 179  
deploy system plan task 90  
deploysysplan command 179  
disable remote commands 136  
drop-down menu  
  views 29

## E

enable remote commands 136  
export system plan task 91

## F

filtering 35  
format media task 96, 107  
frames 29

## G

getdump command 181  
getupgfiles command 182  
graphical user interface 133

## H

- Hard Drive repository 117
- hardware management console web browser
  - getting ready to use 137
  - introduction 134
  - requirements 137
- HMC commands 145
- HMC management 32
  - alphabetical listing 32
  - categorized list 32
  - configuration 32
- HMC Management tasks 93
- hmcshutdown command 183
- hmcwin command 183

## I

- import system plan task 91
- installios command 184
- interface, web-based user 19

## L

- launch guided setup wizard task 97
- launch remote HMC task 97
- launching tasks
  - context menus 26
  - tasks menu 26
  - tasks pad 24
  - web-based user interface 24
- Licensed Internal Code 117
- Licensed Internal Code update 117
- list
  - access control information 187
  - capacity on demand activation information 214
  - capacity on demand information 188
  - console or serviceable events 209
  - dump information 189
  - environmental information 193
  - hardware resources 195
  - hmc configuration information 191
  - hmc user information 192
  - led 198
  - licensed internal code levels 200
  - lock information 201
  - reference codes 208
  - service agent configuration information 209
  - storage media devices 207
  - system connections 213
  - system plan resources 214
  - system plans 213
  - system resources 211
  - utilization data 202
- load serviceable events task 108
- lock HMC screen task 97
- logical partition 43, 47
- logical partition tasks
  - schedule operations 71
- logoff or disconnect task 98
- logssh command 185
- lpar\_netboot command 185
- lpcfgop command 186

- lsaccfg command 187
- lscod command 188
- lsdump command 189
- lshmc command 191
- lshmcusr command 192
- lshwinfo command 193
- lshwres command 195
- lsled command 198
- lslic command 200
- lslock command 201
- lsiparutil command 202
- lsmediadev command 207
- lsrefcode command 208
- lssacfg command 209
- lssvcevents command 209
- lssyscfg command 211
- lssysconn command 213
- lssysplan command 213
- lssysplanres command 214
- lsvet command 214

## M

- manage certificates task 98
- manage connection monitoring task 108
- manage custom groups task 30
  - pattern match group 30
- manage customer information task 108
- manage data replication 99
- manage dumps task 109
- manage eservice registration task 109
- manage inbound connectivity task 110
- manage outbound connectivity task 110
- manage power4 service agent task 111
- manage remote connections task 111
- manage remote support requests task 111
- manage serviceable event notification task 112
- manage serviceable events task 112
- manage systems call-home task 113
- manage task and resource roles task 99
- manage users and tasks task 101
- management, HMC 32
- management, systems 21
- menu, Advanced System Management 145
- menus
  - tasks 26
  - views 36
- migrate configuration 215
- migrctg command 215
- mkaccfg command 215
- mkhmcusr command 216
- mksyscfg command 217
- mksysconn command 223
- mksysplan command 224
- mkvterm command 225
- monhmc command 225
- monitoring
  - hmc subsystems and system resources 225

## N

- nodes 21
  - custom groups 29
  - frames 29
  - HMC Management 32
  - system plans 30
  - updates 33

## O

- open 5250 console task 101
- open restricted shell terminal task 102

## P

- Parameters, Power-On 42
- partition, logical 43, 47
- partitions 27
  - nodes 27
- pattern match group 30
- pedbg command 226
- pesh command 227
- Power-On Parameters 42
- profile data
  - backup 146

## R

- remote command execution task 102, 135
- remote operation task 102
- remote operations 133
- remote virtual terminal task 102
- remove
  - access control object 227
  - hmc user 228
  - lock 228
  - partition 229
  - partition profile 229
  - profile data 229
  - system connection 230
  - system plan 232
  - system plan resource 232
  - system profile 229
  - utilization data 228
  - virtual terminal session 233
- remove system plan task 91
- restore
  - hardware resources 233
  - profile data 234
  - upgrade data 235
- restore HMC data task 102
- rmaccfg command 227
- rmhmcusr command 228
- rmlock command 228
- rmlparutil command 228
- rmprofddata command 229
- rmsyscfg command 229
- rmsysconn command 230
- rmsysplan command 232
- rmsysplanres command 232
- rmvterm command 233
- rows, selecting 35
- rsthwres command 233
- rstprofddata command 234



rstupgdata command 235

## S

save upgrade data 236  
save upgrade data task 103  
saveupgdata command 236  
schedule operations task 44, 71, 103  
selecting 22  
selecting rows 35  
servers 21, 22  
    working with 22  
service management 33  
    alphabetical listing 33  
    categorized list 33  
    tasks 107  
shut down or restart task 104  
ssh clients 135  
start dump 237  
startdump command 237  
status bar 38  
    attentions LEDs 39  
    serviceable events 39  
    status overview 39  
    unacceptable 38  
status overview 39  
system plan tasks  
    create 90  
    deploy 90  
    export 91  
    import 91  
    remove 91  
    view 89  
system plans 30  
systems management 21, 41, 69, 81

## T

tables 35  
    column configuration 36  
    filtering 35  
    sorting 35  
task bar 20  
tasks  
    back up HMC data 93  
    Change Network Settings 94  
    change user interface settings 95  
    change user password 96  
    Create Serviceable Event 107  
    create welcome text 96  
    format media 96, 107  
    HMC Management 93  
    launch guided setup wizard 97  
    launch remote HMC 97  
    load serviceable events 108  
    lock HMC screen 97  
    logoff or disconnect 98  
    manage certificates 98  
    manage connection monitoring 108  
    manage custom groups 30  
    manage customer information 108  
    manage data replication 99  
    manage dumps 109  
    manage inbound connectivity 110  
    manage outbound connectivity 110  
    manage power4 service agent 111

tasks (*continued*)

    manage remote connections 111  
    manage remote support requests 111  
    manage serviceable events 112  
    manage systems call-home 113  
    manage task and resource roles 99  
    manage users and tasks 101  
    open 5250 console 101  
    open restricted shell terminal 102  
    remote command execution 102, 135  
    remote operation 102  
    remote virtual terminal 102  
    restore HMC data 102  
    save upgrade data 103  
    schedule operations 44, 71, 103  
    service Management 107  
    shut down or restart 104  
    systems management 41, 69, 81  
    test network connectivity 104  
    tip of the day 105  
    transmit service information 113  
    view HMC events 105  
    view licenses 105  
    view network topology 106  
tasks manage eservice registration 109  
tasks manage serviceable event  
    notification 112  
tasks menu 26  
test network connectivity task 104  
tip of the day task 105  
transmit service information task 113

## U

update  
    hmc code 238  
    licensed internal code 240  
updates 33  
updhmc command 238  
updlc command 240  
user interface, web-based 19  
user-defined groups 30  
    nodes 30  
using  
    a remote HMC 134  
    remote command line 135

## V

view HMC events task 105  
view licenses task 105  
view network topology task 106  
view system plan task 89  
views drop-down menu 29  
views menu 36  
viosvrcmd commadn 242  
viosvrcmd command 242  
virtual terminal session 225

## W

web browser  
    getting ready to use 137  
    introduction 134  
    requirements 137

web-based user interface

    components  
        banner 19  
        navigation pane 19  
        status bar 19  
        task bar 19  
        work pane 19  
    context menus 26  
    HMC management 32  
    launching tasks 24, 26  
    nodes  
        custom groups 29  
        frames 29  
        HMC management 32  
        partitions 27  
        servers 21  
        service management 33  
        system plans 30  
        updates 33  
        user-defined groups 30  
    resizing the panes 20  
    service management 33  
    status bar 38  
    status exceptions 38, 39  
    status overview 39  
    tables 35  
        column configuration 36  
        filtering 35  
        selecting rows 35  
        sorting 35  
    work pane 34









Printed in USA

SA76-0085-00

