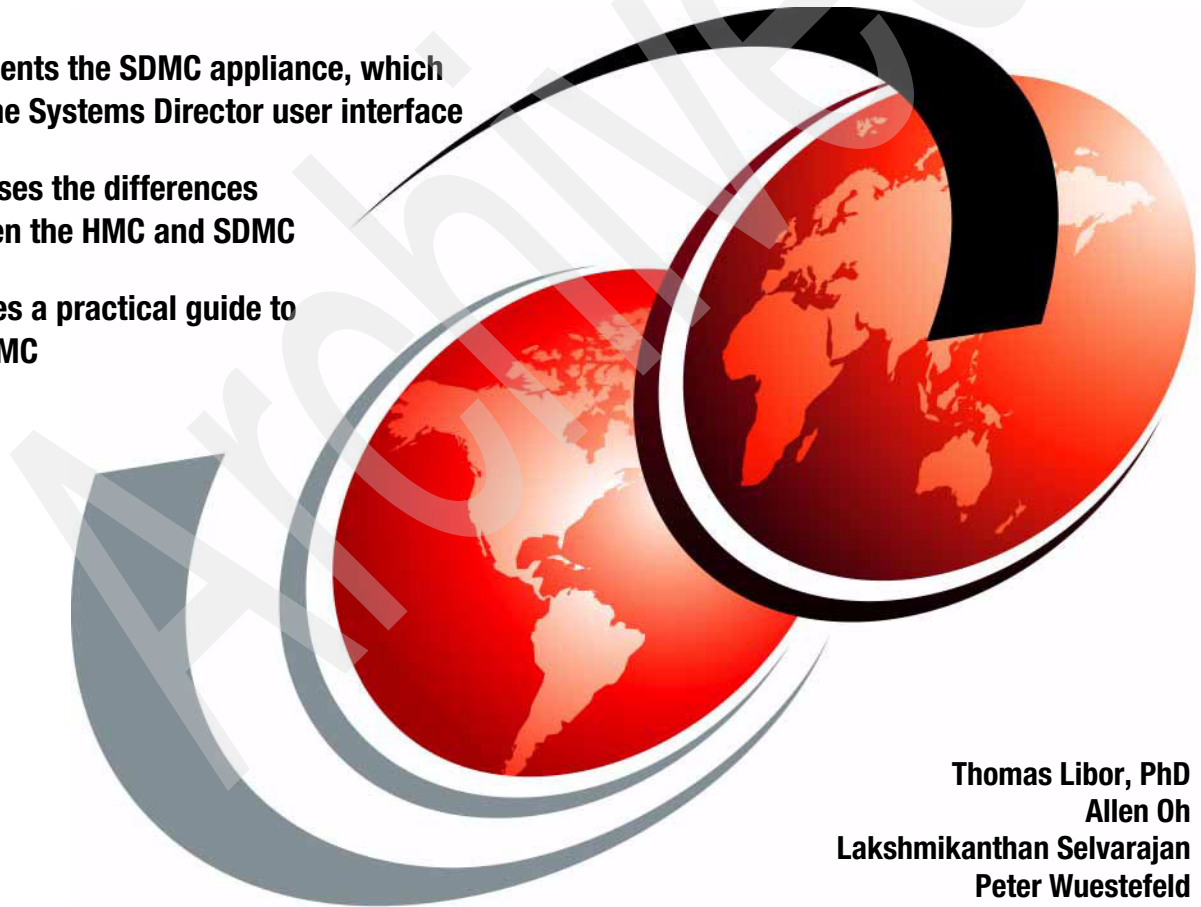


IBM Systems Director Management Console Introduction and Overview

Documents the SDMC appliance, which
uses the Systems Director user interface

Discusses the differences
between the HMC and SDMC

Provides a practical guide to
the SDMC



Thomas Libor, PhD
Allen Oh
Lakshmikanthan Selvarajan
Peter Wuestefeld



International Technical Support Organization

**IBM Systems Director Management Console:
Introduction and Overview**

April 2011

Archived

Note: Before using this information and the product it supports, read the information in “Notices” on page xix.

First Edition (April 2011)

This edition applies to Version 6, Release 730, Service Pack 1048A of SDMC Build Level 1.

Note: This book is based on a pre-GA version of a product and may not apply when the product becomes generally available. We recommend that you consult the product documentation or follow-on versions of this IBM Redbooks publication for more current information.

© Copyright International Business Machines Corporation 2011. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

| | |
|------------------------------------------------------------------|-------|
| Figures | ix |
| Tables | xv |
| Examples | xvii |
| Notices | xix |
| Trademarks | xx |
| Preface | xxi |
| The team who wrote this book | xxii |
| Now you can become a published author, too! | xxiii |
| Comments welcome | xxiii |
| Stay connected to IBM Redbooks | xxiv |
| Chapter 1. Overview | 1 |
| 1.1 Power Systems management consoles | 2 |
| 1.2 Positioning the Systems Director Management Console | 3 |
| 1.3 IVM, HMC, and SDMC support | 6 |
| 1.4 Systems Director Management Console structure | 7 |
| 1.5 Terminology | 10 |
| 1.6 Functional differences | 10 |
| 1.6.1 Enhanced virtualization management | 11 |
| 1.6.2 Users and roles | 11 |
| 1.6.3 Additional functions | 12 |
| 1.6.4 User interface enhancements | 12 |
| 1.6.5 Redundancy model | 12 |
| 1.6.6 Backup and restore | 12 |
| 1.6.7 SDMC considerations | 13 |
| Chapter 2. Installation | 15 |
| 2.1 Prerequisites | 16 |
| 2.1.1 Hardware appliance | 16 |
| 2.1.2 Software appliance | 16 |
| 2.2 Installation of the hardware appliance | 17 |
| 2.2.1 Hardware installation | 18 |
| 2.2.2 Hardware appliance installation | 18 |
| 2.3 Installation of the software appliance | 19 |
| 2.3.1 SDMC software appliance installation media specifics | 19 |

| | | |
|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|-----------|
| 2.3.2 | VMware installation | 19 |
| 2.3.3 | Red Hat KVM installation | 24 |
| 2.4 | Setup wizard | 28 |
| 2.5 | SDMC software licensing requirements | 38 |
| 2.5.1 | SDMC hardware appliance | 39 |
| 2.5.2 | SDMC software appliance. | 39 |
| 2.5.3 | Licensing for cores of managed systems | 39 |
| Chapter 3. Basic operation | | 41 |
| 3.1 | Features overview | 42 |
| 3.1.1 | Power Server management | 42 |
| 3.1.2 | PowerVM Virtualization management. | 44 |
| 3.1.3 | Power Unit management. | 45 |
| 3.1.4 | POWER processor-based blades management | 46 |
| 3.1.5 | SDMC appliance management | 46 |
| 3.1.6 | Service and support management | 47 |
| 3.1.7 | Hierarchical management | 48 |
| 3.1.8 | Update management. | 48 |
| 3.2 | Using the web interface. | 49 |
| 3.2.1 | Layout of the web interface | 51 |
| 3.2.2 | Launching a task. | 52 |
| 3.2.3 | Resource views | 55 |
| 3.3 | Command-line interface | 59 |
| Chapter 4. Making the transition to the IBM Systems Director Management Console | | 61 |
| 4.1 | Concepts | 62 |
| 4.2 | IVM to SDMC transition. | 62 |
| 4.2.1 | What is transitioned. | 63 |
| 4.2.2 | How to transition | 63 |
| 4.2.3 | Messages | 64 |
| 4.3 | HMC to SDMC transition. | 65 |
| 4.3.1 | What is transitioned. | 65 |
| 4.3.2 | What is not transitioned. | 65 |
| 4.3.3 | Interactive transition using graphical user interface | 65 |
| 4.3.4 | Interactive transition using the command-line interface | 68 |
| 4.3.5 | Offline transition using the graphical user interface | 68 |
| 4.3.6 | Offline transition using the command-line interface | 71 |
| 4.4 | Transition in a private network | 72 |
| 4.4.1 | SDMC as the DHCP server. | 73 |
| 4.4.2 | HMC as the DHCP server. | 73 |
| Chapter 5. System management | | 75 |
| 5.1 | System discovery | 76 |

| | | |
|-------------------|-----------------------------------------------------|------------|
| 5.1.1 | System discovery functions | 76 |
| 5.1.2 | Discovery of POWER processor-based blades | 81 |
| 5.1.3 | Using the command-line interface | 82 |
| 5.1.4 | Auto discovery | 82 |
| 5.1.5 | IP address rules | 83 |
| 5.2 | System discovery using the HMC | 84 |
| 5.3 | System management operations | 86 |
| 5.3.1 | Edit Host page | 86 |
| 5.3.2 | Operations page | 87 |
| 5.3.3 | System Configuration page | 88 |
| 5.3.4 | Virtual Resources page | 88 |
| 5.3.5 | Hardware page | 88 |
| 5.3.6 | Release Management page | 89 |
| 5.3.7 | System Status and Health page | 89 |
| 5.3.8 | Service and Support Manager page | 89 |
| 5.3.9 | State mappings between HMC and SDMC | 90 |
| 5.4 | Hierarchical management | 91 |
| 5.4.1 | Enabling hierarchical management | 92 |
| 5.4.2 | Using hierarchical management | 93 |
| 5.4.3 | Hierarchical management security | 93 |
| 5.5 | Capacity on Demand | 94 |
| 5.5.1 | Launching the CoD task | 94 |
| 5.5.2 | Capacity on Demand | 95 |
| 5.5.3 | Advanced Functions | 96 |
| 5.5.4 | CoD operations | 97 |
| Chapter 6. | Power Unit management | 99 |
| 6.1 | Power Unit managment | 100 |
| 6.1.1 | Edit Power Unit page | 101 |
| 6.1.2 | Bulk Power Assembly (BPA) Status page | 102 |
| 6.1.3 | Change Password page | 102 |
| 6.1.4 | Initialize Frame page | 103 |
| 6.1.5 | Launch Advanced System Management page | 104 |
| 6.1.6 | Power Off Unowned IO Units page | 104 |
| 6.1.7 | Rebuild page | 104 |
| Chapter 7. | Firmware updates | 107 |
| 7.1 | Update Manager | 108 |
| 7.1.1 | Readiness Check page | 110 |
| 7.1.2 | Installing updates | 112 |
| 7.1.3 | Power Firmware Management tasks | 126 |
| Chapter 8. | Virtual Server operation | 131 |
| 8.1 | Virtual Server creation | 132 |

| | |
|-------------------------------------------------------------------------|-----|
| 8.2 Virtual Server activation | 152 |
| 8.3 Virtual Server shutdown | 157 |
| 8.4 Virtual Server management | 159 |
| 8.4.1 Command-line usage | 182 |
| 8.4.2 Current Configuration | 182 |
| 8.4.3 Virtual Server Profiles | 185 |
| 8.4.4 Server Profiles | 188 |
| 8.5 Suspend and resume | 192 |
| 8.5.1 Suspend a Virtual Server | 193 |
| 8.5.2 Resume a Virtual Server | 194 |
| 8.6 Mobility | 195 |
| Chapter 9. IBM Systems Director Management Console management .. | 197 |
| 9.1 User management and security | 198 |
| 9.1.1 Hardware Management Console concepts | 198 |
| 9.1.2 IBM Systems Director concepts | 200 |
| 9.1.3 Assigning a role to a user | 218 |
| 9.1.4 User authentication and authorization | 222 |
| 9.1.5 User management | 223 |
| 9.2 Network configuration | 240 |
| 9.2.1 Configuring network settings | 241 |
| 9.2.2 Configuring network settings using the SDMC CLI | 252 |
| 9.2.3 Testing network connectivity | 253 |
| 9.3 Backup and restore | 253 |
| 9.3.1 SDMC hardware appliance backup and restore | 253 |
| 9.3.2 SDMC software appliance backup and restore on VMware | 256 |
| 9.3.3 SDMC software appliance backup and restore on KVM | 261 |
| 9.4 Problem determination | 264 |
| 9.4.1 Available logs | 264 |
| 9.4.2 IBM Systems Director logs | 267 |
| 9.4.3 Audit logs | 269 |
| 9.4.4 Using pedbg | 269 |
| 9.4.5 Using pesh | 270 |
| 9.5 SDMC appliance update | 271 |
| Chapter 10. Command-line interface | 275 |
| 10.1 SDMC command-line interface | 276 |
| 10.1.1 IBM Systems Director appliance commands | 276 |
| 10.1.2 IBM Systems Director application commands | 278 |
| 10.1.3 Power Systems management commands | 280 |
| 10.2 HMC commands supported on the SDMC | 282 |
| 10.3 HMC commands not supported on the SDMC | 287 |
| Chapter 11. Schedule operations | 289 |

| | | |
|--------------------|----------------------------------------------------------------------------------------------|------------|
| 11.1 | Scheduling operations for managed systems and Virtual Servers | 290 |
| 11.1.1 | Schedule tab | 292 |
| 11.1.2 | Notification | 293 |
| 11.1.3 | Options | 293 |
| 11.1.4 | Creating the job | 294 |
| 11.2 | Editing, deleting, and copying, and viewing the properties of a scheduled operation. | 294 |
| 11.3 | Automation Manager | 297 |
| Chapter 12. | High availability and redundancy | 299 |
| 12.1 | Systems Director Management Console High Availability versus redundant setup. | 300 |
| 12.2 | Active/Passive High Availability overview | 302 |
| 12.2.1 | High availability terminology | 304 |
| 12.2.2 | SDMC High Availability synchronized data | 305 |
| 12.2.3 | SDMC High Availability processes monitored | 306 |
| 12.2.4 | Active/Passive High Availability: Log location | 306 |
| 12.3 | Active/Passive High Availability: Configuration planning | 307 |
| 12.3.1 | Network requirements | 308 |
| 12.3.2 | DHCP considerations | 311 |
| 12.4 | High Availability configuration | 312 |
| 12.4.1 | Configuration using SDMC High Availability setup wizard | 313 |
| 12.4.2 | Steps to install High Availability using the CLI | 321 |
| 12.5 | Active/Passive High Availability: Updates | 322 |
| 12.6 | Active/Passive High Availability: Upgrades | 322 |
| Chapter 13. | Advanced System Management Interface | 325 |
| 13.1 | Connecting to ASMI using the SDMC | 326 |
| 13.2 | Connecting to ASMI using the CLI | 329 |
| 13.3 | Using ASMI | 329 |
| Chapter 14. | Service and support | 335 |
| 14.1 | Introduction | 336 |
| 14.2 | Setup wizard | 337 |
| 14.3 | Call Home | 343 |
| 14.4 | Serviceable event processing | 346 |
| 14.4.1 | Detection of serviceable events | 346 |
| 14.4.2 | Persistent storage and management of serviceable event data | 347 |
| 14.4.3 | Transmission of service requests and EED to IBM Support | 347 |
| 14.4.4 | Processing of duplicate events | 347 |
| 14.4.5 | User actions | 348 |
| 14.4.6 | Closure of serviceable events | 350 |
| 14.5 | Support File Management (dump). | 351 |
| 14.5.1 | Support Files view | 351 |

| | |
|------------------------------------------------------------------------------------------|------------|
| 14.5.2 Support Files Management | 355 |
| 14.6 Service and Support Manager command-line interface | 362 |
| 14.7 Service and Support Manager tasks | 363 |
| 14.8 First Failure Data Capture | 364 |
| 14.9 Guided Repair | 365 |
| 14.9.1 Differences from HMC | 366 |
| Appendix A. Command-line reference | 367 |
| IBM Power Systems management commands | 368 |
| IBM Systems Director application commands | 370 |
| Event commands | 371 |
| Scheduler commands | 373 |
| SSM commands | 375 |
| High availability commands. | 380 |
| User commands | 383 |
| Other commands. | 385 |
| Appendix B. IBM Systems Director base functions | 389 |
| Base functions | 390 |
| Appendix C. IBM Systems Director Management Console distribution details. | 393 |
| IBM Systems Director Management Console virtual disk images | 394 |
| Abbreviations and acronyms | 395 |
| Related publications | 397 |
| IBM Redbooks | 397 |
| Online resources | 397 |
| Help from IBM | 398 |
| Index | 399 |

Figures

| | |
|----------------------------------------------------------------------------|----|
| 1-1 HMC and IVM management of POWER servers | 2 |
| 1-2 SDMC administrative framework. | 4 |
| 1-3 Positioning the IBM Systems Director Management Console. | 5 |
| 1-4 SDMC: Hardware appliance structure. | 8 |
| 2-1 SDMC connection | 18 |
| 2-2 Deploy OVF Template from vSphere Client | 21 |
| 2-3 Deploying from a file or URL | 22 |
| 2-4 Ready to Complete page: A summary of the deployment settings | 23 |
| 2-5 Selecting the locale for the system | 28 |
| 2-6 IBM Software License Agreement. | 29 |
| 2-7 Setup Wizard Welcome page | 30 |
| 2-8 Date and Time page | 31 |
| 2-9 Setup of passwords. | 32 |
| 2-10 Creating additional users | 33 |
| 2-11 Configure Agent Manager | 34 |
| 2-12 Summary page | 35 |
| 2-13 System Setup Processing page | 36 |
| 2-14 Console starting page | 37 |
| 2-15 IBM Systems Director login page | 38 |
| 3-1 SDMC Login page. | 49 |
| 3-2 Welcome page | 50 |
| 3-3 Context menu for server management | 53 |
| 3-4 Context menu for server management | 54 |
| 3-5 Context menu for Virtual Server management | 55 |
| 3-6 Table view | 56 |
| 3-7 Properties view | 57 |
| 3-8 Topology Map view | 58 |
| 4-1 Launch Transition wizard | 66 |
| 4-2 Managed systems in the Transition wizard | 67 |
| 4-3 Transition method using an exported data file | 70 |
| 4-4 Transition workflow | 72 |
| 5-1 System Discovery page | 77 |
| 5-2 Verify Connection page. | 78 |
| 5-3 Request Access page | 79 |
| 5-4 Extended management. | 85 |
| 5-5 Edit Host page. | 87 |
| 5-6 Server Preferences page | 92 |
| 5-7 CoD page | 95 |

| | |
|-------------------------------------------------------------------------------|-----|
| 6-1 Available Power Units | 100 |
| 6-2 Edit Power Unit page | 101 |
| 6-3 Bulk Power Assembly (BPA) Status page. | 102 |
| 6-4 Change Password page | 102 |
| 6-5 Initialize Frame page. | 103 |
| 6-6 Power Off Unowned IO Units page. | 104 |
| 6-7 Rebuild of a Power Unit | 104 |
| 7-1 Accessing the Update Manager page. | 108 |
| 7-2 Update Manager page | 109 |
| 7-3 Readiness Check page. | 110 |
| 7-4 Gather Target page. | 111 |
| 7-5 Readiness Check passed | 112 |
| 7-6 Update Manager: Settings and Check for Updates link | 114 |
| 7-7 Check for Updates page | 115 |
| 7-8 Import Updates from the local SDMC directory. | 117 |
| 7-9 Import Updates using FTP | 118 |
| 7-10 Installation links from Updates page | 119 |
| 7-11 Target systems selection on the Show Needed Updates page | 120 |
| 7-12 Show Needed Updates page | 121 |
| 7-13 Install Wizard Welcome page | 122 |
| 7-14 Select target systems | 123 |
| 7-15 Select systems from install wizard | 124 |
| 7-16 Target Check Results page. | 125 |
| 7-17 Power Firmware Management | 127 |
| 7-18 Power Firmware Management page. | 128 |
| 7-19 Accept | 129 |
| 7-20 Start Accept Task | 130 |
| 8-1 Welcome page with context menu: Create Virtual Server. | 133 |
| 8-2 Create Virtual Server wizard | 134 |
| 8-3 Create Virtual Server wizard: Virtual I/O Server Name | 135 |
| 8-4 Create Virtual Server wizard: IBM i Name panel. | 136 |
| 8-5 Create Virtual Server: Memory | 137 |
| 8-6 Create Virtual Server: Processor | 138 |
| 8-7 Create Virtual Server: Ethernet adapter | 139 |
| 8-8 Create Virtual Server: Manual storage allocation | 140 |
| 8-9 Create Virtual Server: Virtual Storage adapter creation | 141 |
| 8-10 Create Virtual Server: Assign storage adapter IDs | 142 |
| 8-11 Create Virtual Server: Manual SCSI adapter creation | 143 |
| 8-12 Create Virtual Server: Automatic adapter creation | 144 |
| 8-13 Create Virtual Server: Create virtual disk | 145 |
| 8-14 Create Virtual Server: Characteristics of a virtual disk | 146 |
| 8-15 Create Virtual Server: Virtual and physical disk selection. | 147 |
| 8-16 Create Virtual Server: Virtual Fibre Channel adapter selection | 148 |

| | | |
|------|--------------------------------------------------------------------------|-----|
| 8-17 | Create Virtual Server: Optical device and media selection | 149 |
| 8-18 | Create Virtual Server: Load Source and Console | 150 |
| 8-19 | Create Virtual Server: Assign physical adapters | 151 |
| 8-20 | Activate Virtual Server: Profile option | 153 |
| 8-21 | Activating Virtual Server: DefaultProfile selected | 154 |
| 8-22 | Activating Virtual Serve: Keylock position and boot mode | 155 |
| 8-23 | Welcome page: State and detailed state shown after activation. | 156 |
| 8-24 | Shut down a Virtual Server | 157 |
| 8-25 | Shutdown options | 158 |
| 8-26 | Manage Virtual Server menu entry | 160 |
| 8-27 | Manage Virtual Server: General Settings | 161 |
| 8-28 | Tasks button in General Settings tab | 162 |
| 8-29 | Manage Virtual Server: Processor tab | 163 |
| 8-30 | Manage Virtual Server: Dedicated processor mode | 164 |
| 8-31 | Manage Virtual Server: Dedicated memory settings | 165 |
| 8-32 | Manage Virtual Server: Shared memory settings | 166 |
| 8-33 | Manage Virtual Server: Network page | 167 |
| 8-34 | Manage Virtual Server: Edit Virtual Ethernet Adapter | 168 |
| 8-35 | Manage Virtual Server: Add Virtual Storage Adapter | 169 |
| 8-36 | Manage Virtual Server: Create Virtual SCSI Storage Adapter | 170 |
| 8-37 | Manage Virtual Server: Create Virtual FC Storage Adapter | 171 |
| 8-38 | Manage Virtual Server: Storage Devices | 172 |
| 8-39 | Manage Virtual Server: Add Physical Volume | 173 |
| 8-40 | Manage Virtual Server: Add Fibre Channel | 174 |
| 8-41 | Manage Virtual Server: Media Devices page | 175 |
| 8-42 | Manage Virtual Server: Add Physical Media | 176 |
| 8-43 | Manage Virtual Server: Adding virtual media | 177 |
| 8-44 | Manage Virtual Server: Modify virtual media | 178 |
| 8-45 | Manage Virtual Server: Physical Adapters | 179 |
| 8-46 | Manage Virtual Server: Add physical adapters | 180 |
| 8-47 | Manage Virtual Server: Physical adapter addition pending | 181 |
| 8-48 | Current Configuration and Profile management | 183 |
| 8-49 | Save Current Configuration to a profile | 184 |
| 8-50 | Tasks button in Manage Virtual Server page: Server not activated . . . | 185 |
| 8-51 | Tasks button in Manage Virtual Servers page: Server in SMS | 186 |
| 8-52 | Manage Profiles page | 187 |
| 8-53 | Actions menu in Manage Profiles page | 187 |
| 8-54 | Manage Profiles: Edit Virtual Server properties | 188 |
| 8-55 | Server Profile initial menu | 189 |
| 8-56 | Server Profile with on Virtual Server Profile added | 190 |
| 8-57 | Server Profile: Warning while trying to add profiles using AMS | 191 |
| 8-58 | Select Suspend operation from Virtual Server menu | 193 |
| 8-59 | Validate and suspend | 194 |

| | | |
|------|-------------------------------------------------------------------|-----|
| 8-60 | Select Validate from the partition page | 195 |
| 8-61 | Click Validate | 196 |
| 9-1 | Systems Director Management Console: Initial users page | 203 |
| 9-2 | Initial Roles page. | 206 |
| 9-3 | Create Role wizard: Name page. | 207 |
| 9-4 | Create Role wizard: Permissions page. | 208 |
| 9-5 | Create Roles: Summary page. | 209 |
| 9-6 | Groups in the SDMC interface | 211 |
| 9-7 | Groups page | 212 |
| 9-8 | Group Editor Wizard: Initial page | 213 |
| 9-9 | Group Editor Wizard: Type and Location | 214 |
| 9-10 | Group Edit Wizard: Define page with systems selected | 215 |
| 9-11 | Group Edit Wizard: Select page with groups expanded | 216 |
| 9-12 | Group Edit Wizard: Summary page | 217 |
| 9-13 | Groups page with the newly created group. | 218 |
| 9-14 | Users page: Assigning a role | 219 |
| 9-15 | Assign Role wizard: Roles page | 220 |
| 9-16 | Assign Role wizard: Groups | 221 |
| 9-17 | Assign Role: Summary | 222 |
| 9-18 | Welcome page | 224 |
| 9-19 | Create User Account page | 225 |
| 9-20 | Configure an LDAP client | 229 |
| 9-21 | Configure LDAP client wizard | 230 |
| 9-22 | Create User Account: LDAP | 231 |
| 9-23 | Configure Kerberos client page. | 233 |
| 9-24 | Kerberos Client Configuration wizard | 234 |
| 9-25 | Create user account: Kerberos | 235 |
| 9-26 | Users page | 237 |
| 9-27 | User properties page. | 238 |
| 9-28 | Edit user properties: General tab | 239 |
| 9-29 | Configure Network on the Welcome page | 242 |
| 9-30 | Network Configuration wizard | 243 |
| 9-31 | DHCP server. | 244 |
| 9-32 | Setting a static IP address | 245 |
| 9-33 | Host and Gateway menu. | 248 |
| 9-34 | DNS menu. | 249 |
| 9-35 | Job for network configuration | 250 |
| 9-36 | Job scheduled notification. | 250 |
| 9-37 | Restart necessary | 251 |
| 9-38 | Take snapshot from vSphere client. | 257 |
| 9-39 | Take Virtual Machine Snapshot page | 258 |
| 9-40 | Selecting data store | 259 |
| 9-41 | Revert to Current Snapshot | 260 |

| | | |
|-------|--------------------------------------------------------------|-----|
| 9-42 | Snapshot manager | 261 |
| 9-43 | View Trace Logs | 266 |
| 9-44 | Console Logging and Tracing Configuration | 268 |
| 9-45 | Update IBM Systems Director link | 273 |
| 9-46 | Select the SDMC appliance from the Context Chooser | 274 |
| 11-1 | Scheduling operations for managed systems example | 290 |
| 11-2 | Scheduling Backup Profile Data | 291 |
| 11-3 | Task Launch Dialog page | 292 |
| 11-4 | Successful creation of a job | 294 |
| 11-5 | Active and Schedule Jobs overview | 295 |
| 11-6 | Job Properties page | 296 |
| 11-7 | Log of the job | 296 |
| 11-8 | Automation Manager | 297 |
| 12-1 | Redundant versus active/passive SDMC High Availability | 300 |
| 12-2 | Add an New Agent Manager | 302 |
| 12-3 | SDMC High Availability environment before and after failover | 303 |
| 12-4 | Active/Passive configuration sequence | 304 |
| 12-5 | High Availability network topology | 308 |
| 12-6 | Shared and non-shared DHCP configurations | 312 |
| 12-7 | High Availability Settings page | 313 |
| 12-8 | Welcome page | 314 |
| 12-9 | Secondary Node page | 315 |
| 12-10 | Replication IP Address settings page | 316 |
| 12-11 | Network Status IP address | 317 |
| 12-12 | Adding floating IP addresses | 318 |
| 12-13 | Agent Manager IP Address page | 319 |
| 12-14 | Summary page | 320 |
| 13-1 | Connecting to ASMI using the SDMC | 326 |
| 13-2 | Selecting the Service Processor | 327 |
| 13-3 | ASMI login | 328 |
| 14-1 | Service and Support Manager Getting Started Wizard | 337 |
| 14-2 | Welcome page of the SSM Getting Started Wizard | 338 |
| 14-3 | Company contact page | 339 |
| 14-4 | System location page | 340 |
| 14-5 | Connection page | 341 |
| 14-6 | Authorize IBM IDs | 342 |
| 14-7 | Summary page | 343 |
| 14-8 | Service and Support context menu | 344 |
| 14-9 | Service and Support Manager page | 345 |
| 14-10 | Problems page | 348 |
| 14-11 | Problems: General properties | 349 |
| 14-12 | Problem Explanation page | 350 |
| 14-13 | Service and Support Manager | 352 |

| | | |
|-------|---------------------------------------------------|-----|
| 14-14 | Manage Support Files system wide view | 353 |
| 14-15 | Support Files in the context menu of a host | 354 |
| 14-16 | Serviceable Problem Support Files view. | 355 |
| 14-17 | Collect Support Files page | 357 |
| 14-18 | Properties of a support file | 360 |
| 14-19 | Tasks in Active and Schedule Jobs page | 363 |

Tables

| | | |
|------|---------------------------------------------------------------------------------|-----|
| 1-1 | Server firmware support | 6 |
| 1-2 | POWER6 support by SDMC | 9 |
| 1-3 | POWER7 support by SDMC | 9 |
| 1-4 | Side-by-side comparison of terminology | 10 |
| 2-1 | Hardware appliance requirements | 16 |
| 2-2 | Software appliance hardware requirements | 16 |
| 4-1 | Status Manager Error/Resolution messages | 64 |
| 5-1 | State mapping | 90 |
| 9-1 | Default users on HMC and SDMC | 198 |
| 9-2 | User roles on the HMC and SDMC | 199 |
| 9-3 | Table of ports for the SDMC firewall | 246 |
| 9-4 | Log files | 264 |
| 9-5 | IBM Systems Director logs | 267 |
| 9-6 | Tracing and Logging settings | 268 |
| 10-1 | Listing of IBM Systems Director appliance commands | 277 |
| 10-2 | Listing of IBM Systems Director application commands | 279 |
| 10-3 | HMC commands supported at the SDMC | 282 |
| 10-4 | HMC commands not supported by the SDMC | 287 |
| 12-1 | Differences between a redundant and a replication High Availability environment | 301 |
| A-1 | chtunecfg command | 368 |
| A-2 | impdata command | 368 |
| A-3 | mk5250 command | 369 |
| A-4 | refdev command | 369 |
| A-5 | rmdump command | 369 |
| A-6 | IBM Systems Director commands replaced | 370 |
| A-7 | appleventactionplan command | 371 |
| A-8 | createeventactionplan command | 371 |
| A-9 | listeventactionplans commands | 371 |
| A-10 | listventactions command | 372 |
| A-11 | listevents command | 372 |
| A-12 | listeventtypes command | 372 |
| A-13 | listfilters command | 373 |
| A-14 | canceljobactivation command | 373 |
| A-15 | getjobactivationlog command | 373 |
| A-16 | getjobstatus command | 374 |
| A-17 | listjobactivations command | 374 |
| A-18 | listjobactivaitonsbysystem command | 374 |

| | | |
|------|------------------------------------|-----|
| A-19 | listjobs command | 374 |
| A-20 | chkssmconfig command | 375 |
| A-21 | collectsptfile command | 375 |
| A-22 | cpsptfile command | 376 |
| A-23 | lssptfile command | 377 |
| A-24 | lssvcproblem command | 378 |
| A-25 | rmsptfile command | 378 |
| A-26 | ssmimport command | 379 |
| A-27 | submitsptfile command | 380 |
| A-28 | configureHA command | 380 |
| A-29 | failover command | 382 |
| A-30 | removeHA command | 383 |
| A-31 | mkuser command | 383 |
| A-32 | rmuser command | 384 |
| A-33 | enablehierachicalmgmt command | 385 |
| A-34 | isglobalserver command | 385 |
| A-35 | licensestatus command | 386 |
| A-36 | printInformation command | 386 |
| A-37 | simffdc command | 386 |
| A-38 | ssh_for_dsh command | 386 |
| A-39 | startdiscovery command | 387 |
| A-40 | updatelicense command | 387 |
| C-1 | Seven virtual disk images for SDMC | 394 |

Examples

| | |
|------------------------------------------------------------------------|-----|
| 2-1 OVF Tool CLI using an OVA file on Windows | 24 |
| 2-2 Sample domain.xml file | 26 |
| 8-1 Create Virtual Server using smcli mksyscfg | 152 |
| 8-2 Activate a Virtual Server using smcli chsysstate | 156 |
| 8-3 Shutting down a Virtual Server using smcli chsysstate | 158 |
| 8-4 Adding physical adapters using smcli chsyscfg | 182 |
| 8-5 Creating System Profile with smcli mksyscfg | 192 |
| 9-1 Listing the sysadmin user using the smcli lsuser command | 201 |
| 9-2 Listing user groups using smcli lsusergp | 203 |
| 9-3 Listing the SMAAdministrator role using smcli lsrole | 205 |
| 9-4 Creating a role using the smcli mkrole command | 209 |
| 9-5 Listing a role using the smcli lsrole command | 210 |
| 9-6 Deleting a role using the smcli rmrole command | 210 |
| 9-7 Creating a user using the CLI | 226 |
| 9-8 Listing a user using smcli lsuser | 226 |
| 9-9 Structure of the cfgldap command | 227 |
| 9-10 mkuser command with LDAP credentials | 231 |
| 9-11 Structure of the cfgkrb command | 232 |
| 9-12 mkuser command with Kerberos credentials | 236 |
| 9-13 Changing a user using the smcli chuser command | 239 |
| 9-14 Deleting a user with the smcli rmuser command | 240 |
| 9-15 Testing network connectivity using ping | 253 |
| 10-1 lsbundle listing (excerpt) | 278 |
| 10-2 Listing of psm commands (excerpt) | 280 |
| 10-3 SDMC command output | 282 |
| 12-1 Configuring High Availability using the CLI | 321 |

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM 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: *IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "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. IBM 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 non-IBM Web sites 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 IBM product and use of those Web sites is at your own risk.

IBM 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 measurement 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 non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

| | | |
|---------------------------|-----------------------------------------------------------------------------------------------------|-----------------|
| Active Memory™ | POWER5™ | RETAIN® |
| AIX® | POWER6® | System i® |
| BladeCenter® | POWER7™ | System p® |
| DB2 Universal Database™ | PowerVM™ | System Storage® |
| DB2® | POWER® | System x® |
| Electronic Service Agent™ | Redbooks® | System z® |
| IBM® | Redpaper™ | Tivoli® |
| Power Systems™ | Redbooks (logo)  ® | |

The following terms are trademarks of other companies:

Snapshot, and the NetApp logo are trademarks or registered trademarks of NetApp, Inc. in the U.S. and other countries.

Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel, Intel logo, Intel Inside logo, and Intel Centrino logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

This IBM® Redbooks® publication positions the IBM Systems Director Management Console (SDMC) against the IBM Hardware Management Console (HMC). The IBM Systems Director Management Console provides system administrators the ability to manage IBM Power System® servers as well as IBM Power Blade servers. It is based on IBM Systems Director.

This publication is designed for system administrators to use as a deskside reference when managing Virtual Servers (formerly partitions) using the SDMC.

The major functions that the SDMC provides are server hardware management and virtualization management. You can find further information about virtualization management in the following documents:

- ▶ *IBM PowerVM™ Virtualization: Introduction and Configuration*, SG24-7940
- ▶ *IBM PowerVM Virtualization: Managing and Monitoring*, SG24-7590
- ▶ *IBM PowerVM: Live Partition Mobility*, SG24-7460
- ▶ *IBM System p Advanced POWER Virtualization (Power VM) Best Practices*, REDP-4194
- ▶ *PowerVM Virtualization Active Memory™ Sharing*, REDP-4470
- ▶ *Advanced POWER Virtualization on IBM System p Virtual I/O Server Deployment Examples*, REDP-4224

In this book, we discuss how to:

- ▶ Configure the SDMC.
- ▶ Manage the SDMC itself.
- ▶ Manage Virtual Servers.
- ▶ How to make the transition from HMC to SDMC.
- ▶ Establish redundant SDMC configurations.
- ▶ Use the enhanced service and support functions.

In addition, we explain how to use the new SDMC graphical user interface based on the IBM Systems Director and the SDMC command line, which is composed of IBM Systems Director commands and HMC commands.

The team who wrote this book

This book was produced by a team of specialists from around the world working at the International Technical Support Organization, Poughkeepsie Center.

Thomas Libor, PhD is an IT Specialist in Germany. He has 10 years of experience in Power Systems™ and AIX®. He is an IBM Certified Advanced Technical Expert for Power Systems with AIX and an IBM Certified Advanced Technical Expert for IBM System Storage® 2009. His areas of expertise include virtualization, high availability, IBM Storage, Linux®, and networking. He holds a PhD in Chemistry from the Philipps-University in Marburg, Germany.

Allen Oh is a Senior System Engineer and Solutions Architect for MoreDirect, an IBM Premier Business Partner authorized to sell and service IBM Power System System x®, and storage throughout the United States. He has over fourteen years of experience in UNIX®, AIX, and enterprise server and storage technology. Allen holds several senior level industry certifications and is an IBM Certified Advanced Technical Expert in Power Systems and AIX. He is a graduate of the University of Southern California.

Lakshmikanthan Selvarajan is a Staff Software Engineer working at Systems and Technology Group in IBM India. He has 7 years of experience in developing software applications using the J2EE framework. He holds a degree in Information Technology from Bharathidasan University, India. He has been with IBM since 2006 and working on developing system management solutions for IBM Power Systems. His areas of expertise include Power Systems management, web security, and J2EE technologies.

Peter Wuestefeld is a Pre-Sales Systems Engineer with IBM Premier Business Partner SVA GmbH in Germany. With sixteen years of experience in AIX and Power Systems, he specializes in a wide field of AIX topics. Peter holds a Master's degree in Prehistoric Archaeology from the Eberhard-Karls- University of Tuebingen, Germany.

Thanks to the following people for their contributions to this project:

Scott Broussard, Dominique Clain, Rich Conway, Karyn Corneli, Craig DeBellis, Craig Dinsdale, Carol Hernandez, Eric R Larese, Derek Matocha, Andy Mills, Minh Nguyen, Amartey Pearson, Brian Preston, Ashok Shamsundar, Mark Smith, Anna Sortland

IBM US

Priya Kannan and Raghu Rajarao
IBM India

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:

ibm.com/redbooks

- ▶ Send your comments in an email to:

redbooks@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- ▶ Find us on Facebook:
<http://www.facebook.com/IBMRedbooks>
- ▶ Follow us on Twitter:
<http://twitter.com/ibmredbooks>
- ▶ Look for us on LinkedIn:
<http://www.linkedin.com/groups?home=&gid=2130806>
- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:
<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>
- ▶ Stay current on recent Redbooks publications with RSS Feeds:
<http://www.redbooks.ibm.com/rss.html>

Overview

The IBM Systems Director Management Console (SDMC) is the successor to the Hardware Management Console (HMC) and the Integrated Virtualization Manager (IVM).

It supports all POWER6™ and POWER7 processor-based systems (including Power Systems blades) with the exception of the 575.

In this chapter, we introduce the SDMC, show some of its history, and position it in the Power Systems environment. There are new concepts to learn and new terminology shows up, so we explain to you what has changed.

We also discuss the value proposition of the SDMC and the management framework in which it is embedded.

This chapter contains the following items for discussion:

- ▶ Power Systems management consoles
- ▶ Positioning the SDMC
- ▶ Transition to the SDMC
- ▶ A brief overview of the SDMC structure
- ▶ An introduction to new terminology
- ▶ A comparison between the functionality of management consoles

1.1 Power Systems management consoles

The Hardware Management Console (HMC) allows for management of Power Systems from entry level servers to high-end systems. Management of entry systems is also possible with the Integrated Virtualization Manager (IVM), a function of the Virtual I/O server. The IVM is confined to the system the Virtual I/O Server is installed on, while the Hardware Management Console can administer up to 256 LPARs. An HMC does not allow for management of POWER processor-based blades; they are solely supported by IVM, as shown in Figure 1-1. The resulting difference in handling mixed environments adds complexity to administration.

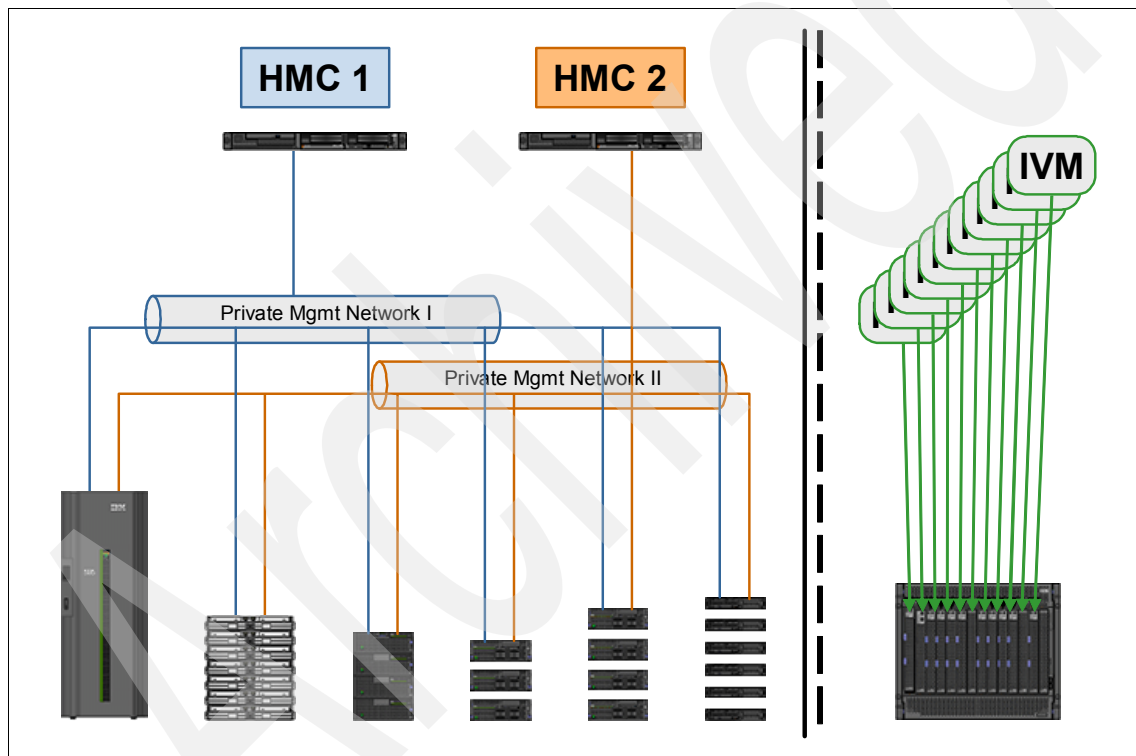


Figure 1-1 HMC and IVM management of POWER servers

With the SDMC, the scope of administered systems spans from POWER processor-based blades to high-end systems, allowing for a single, consistent approach to systems administration.

The characteristics of those management consoles are as follows:

- ▶ Hardware Management Console:
 - Is implemented as an external, independent appliance
 - Administers entry level up to high-end systems
 - Can administer more than one managed system
 - Allows for more than one Virtual I/O Servers per managed system
- ▶ Integrated Virtualization Manager:
 - Runs directly on top of a Virtual I/O Server
 - Administers POWER processor-based blades up to entry level servers
 - Administers only one managed system per IVM
 - Allows for only one Virtual I/O Server installed on the system

1.2 Positioning the Systems Director Management Console

The SDMC represents the next generation of management appliances for Power Systems. The IBM Systems Director approach required changes to functions that were available in the management consoles before. The SDMC is designed to replace both Hardware Management Console and Integrated Virtualization Manager in Power Systems administration. Thus, it can manage Power Systems directly, but can also work with the Hardware Management Console and Integrated Virtualization Manager side-by-side to ease transition.

The SDMC is designed to be integrated into the administrative framework of IBM Systems Director and has the same look and feel. It provides a common interface for systems administration across the data center. It is designed to administer Power Systems the way you did it in the past using the Hardware Management Console. The only exception is administering systems previously managed by the Integrated Virtualization Manager.

See Figure 1-2 for an overview of how the SDMC is placed in an enterprise-wide administration framework.

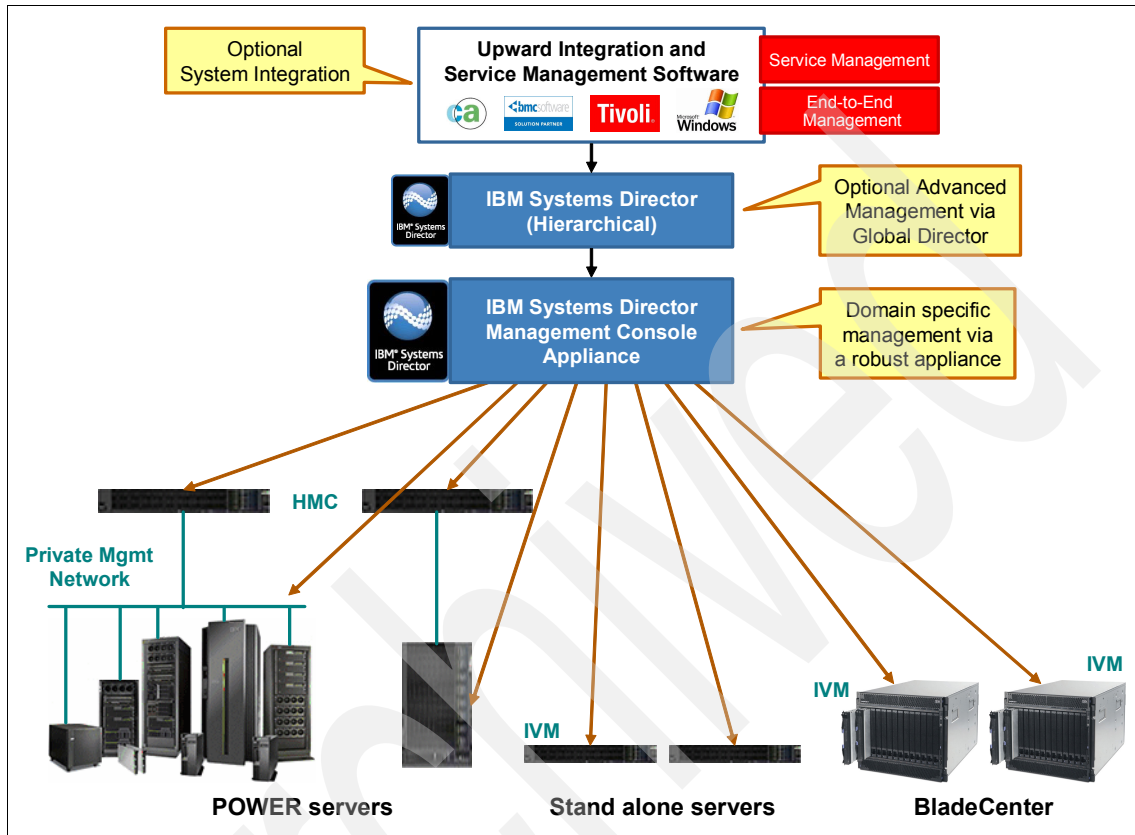


Figure 1-2 SDMC administrative framework

The SDMC is positioned to unify platform management for IBM Systems, providing a consistent look-and-feel for common management tasks. By integrating Power Systems management into the IBM Systems Director framework, it allows for easy management of many systems of different types. It addresses the administration and management challenges that show up where server scale-out introduces economies of scale. It also enables the integration of Power Systems into data center management tools from Tivoli® and other third parties.

See Figure 1-3 for a schematic overview. This figure shows where the SDMC fits into the overall view of IBM Systems Director systems management.

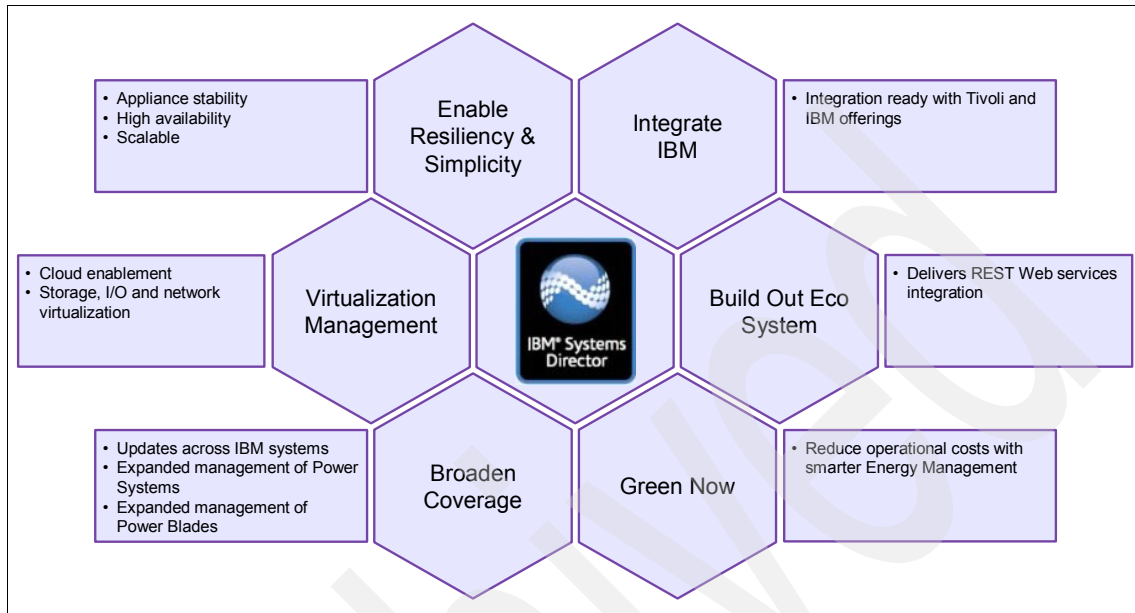


Figure 1-3 Positioning the IBM Systems Director Management Console

As a successor to both Hardware Management Console and Integrated Virtualization Manager, SDMC enables administrators to work with a high-level view of systems. It organizes tasks in a single panel instead of using different menus like the Hardware Management Console and Integrated Virtualization Manager do. This single panel simplifies views of systems and day-to-day tasks.

As it was with older POWER processor based systems, the transition to a new management console structure requires that management for POWER5/POWER5+ processor based systems continues with either Hardware Management Console or Integrated Virtualization Manager. Figure 1-2 on page 4 illustrates administration paths for these systems. Note that the SDMC can administer Hardware Management Console and Integrated Virtualization Manager as well. This eases transition from older environments into new ones.

1.3 IVM, HMC, and SDMC support

The transition will begin in the second half of 2011, as new virtualization features will be only supported by the SDMC. Systems in current installations will be supported by the Hardware Management Console as long as firmware requirements are met. See Table 1-1 for an overview of which POWER processor based systems are supported.

Table 1-1 Server firmware support

| | IVM | HMC | SDMC |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High-end servers | Not Supported | Supported | Supported (hardware appliance only) |
| Low-end Servers and midrange Servers | Supported | Supported | Supported |
| Blades | Supported | Not Supported | Supported |
| Server families supported | <ul style="list-style-type: none"> ▶ POWER5/POWER5+: Yes ▶ POWER6/POWER6+: Yes ▶ POWER7™: Yes | <ul style="list-style-type: none"> ▶ POWER5/POWER5+: Yes ▶ POWER6/POWER6+: Yes ▶ POWER7: Yes | <ul style="list-style-type: none"> ▶ POWER5/POWER5+: No ▶ POWER6/POWER6+: Yes ▶ POWER7: Yes |
| Multiple system support | No | Yes | Yes |
| Firmware version support | Same supported firmware versions as HMC | Same supported firmware versions as HMC | Same supported firmware versions as HMC For Blades: <ul style="list-style-type: none"> ▶ POWER6@: Version 350_107 ▶ POWER7: 730_035 ▶ PS703 PS705: 730_031 |
| Server families support details | <ul style="list-style-type: none"> ▶ Blades: JS21 and beyond ▶ POWER5/POWER5+: 550Q Express and below ▶ POWER6/POWER6+: All HV ▶ POWER7: All HV | <ul style="list-style-type: none"> ▶ Blades: None ▶ POWER5/POWER5+: All ▶ POWER6/POWER6+: All ▶ POWER7: All | <ul style="list-style-type: none"> ▶ Blades: JS22 and beyond (POWER6 and POWER7) ▶ POWER5/POWER5+: None ▶ POWER6/POWER6+: All ▶ POWER7: All |

Both Hardware Management Console and Integrated Virtualization Manager will receive updates to support systems in the POWER7 family. No support for future advanced virtualization and availability features will be added. Also, no support will be available for future POWER processors, as these will be exclusively managed by the SDMC.

Note: The SDMC does not support the Power 575, POWER5 technology-based systems and POWER5 technology-based I/O towers connected to a POWER6 technology-based server.

This support plan is the same plan as the support plan for the Hardware Management Console. For proper and supported function, the firmware level of managed systems and of the Hardware Management Console always had to match the Supported Code Combinations, as documented in the POWER code matrix. The Supported Code Combinations are available at IBM Fix Central in the Hardware Management Console section at the following address:

<http://www.ibm.com/support/fixcentral>

1.4 Systems Director Management Console structure

The SDMC is available as a software and a hardware appliance. The software appliance will replace the Integrated Virtualization Manager. The hardware appliance is required for management of midrange systems and high-end systems. The SDMC releases can be used alongside the Hardware Management Console during trials and deployment, which eases transition.

The SDMC virtual machine contains Linux as the base operating system. For the software appliance, the client supplied virtualization options for different hypervisors include Red Hat Enterprise Virtualization KVM or VMware ESX/ESXi.

The SDMC is also available as follows:

- ▶ Software appliance
 - Replaces Integrated Virtualization Manager or HMC.
 - Can be installed on either VMware or KVM.
 - The client supplies the hardware.
- ▶ Hardware appliance
 - Replaces Hardware Management Console.
 - Pre-installed system like an HMC.
 - Hardware provided by IBM.
 - Uses the RHEV-H hypervisor.

The virtualization layer for the hardware appliance is fixed and cannot be changed. Installation, backup to media, and restore from media is possible as it is with the Hardware Management Console.

The hardware appliance is structured as shown in Figure 1-4.

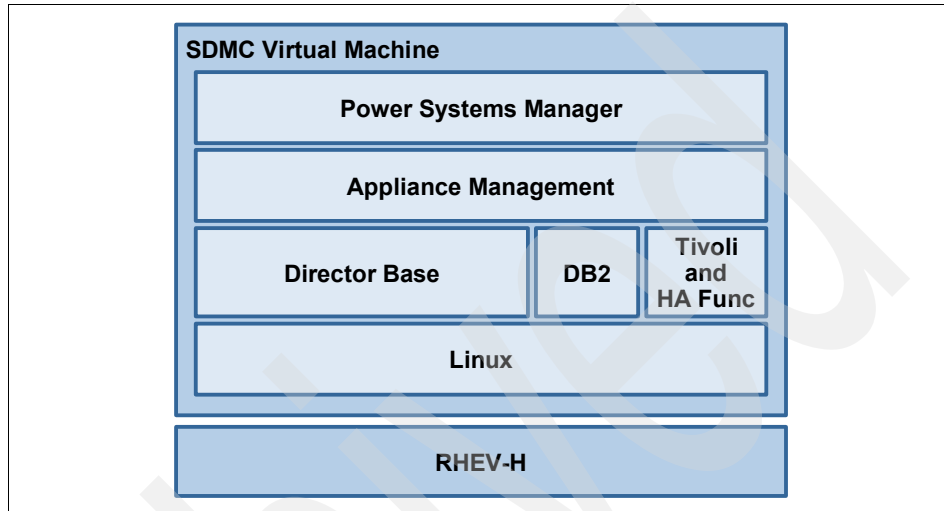


Figure 1-4 SDMC: Hardware appliance structure

Support for POWER processor based systems with either software or hardware appliance depends on the type of Power Systems. See Table 1-2 on page 9 and Table 1-3 on page 9 for a complete listing of which appliance is supported with which system. Also, note the exception for the POWER 575, which is supported with the Hardware Management Console only.

Table 1-2 POWER6 support by SDMC

| POWER6 models | Machine types | SDMC |
|---------------|---------------|--------------|
| 595 | 9119-FHA | HW APP Only |
| 575 | 9125-F2A | HMC Only |
| 570 | 9117-MMA | HW APP Only |
| 570 | 9406-MMA | HW APP Only |
| 560 | 8234-EMA | HW APP Only |
| 550 | 8204-E8A | HW or SW APP |
| 550 | 9409-M50 | HW or SW APP |
| 520 | 8203-E4A | HW or SW APP |
| 520 | 8203-E4A | HW or SW APP |
| 520-SB | 8261-E4A | HW or SW APP |
| 520 | 9408-M25 | HW or SW APP |
| 520 | 9407-M15 | HW or SW APP |
| JS22 | 7998-61X | HW or SW APP |
| JS12 | 7998-60X | HW or SW APP |

Table 1-3 POWER7 support by SDMC

| POWER7 models | Machine types | SDMC |
|---------------|---------------|--------------|
| 795 | 9119-FHB | HW APP Only |
| 780 | 9179-MHB | HW APP Only |
| 770 | 9117-MMB | HW APP Only |
| 755 | 8236-E8C | HW or SW APP |
| 750 | 8233-E8B | HW or SW APP |
| 720 | 8202-E4B | HW or SW APP |
| 740 | 8205-E6B | HW or SW APP |
| 710/730 | 8231-E2B | HW or SW APP |
| PS701 | 8406-71Y | HW or SW APP |
| PS700 | 8406-70Y | HW or SW APP |

1.5 Terminology

Based on the integration into IBM Systems Director, a common terminology replaces the Hardware Management Console and Integrated Virtualization Manager specific terminology. Table 1-4 shows a mapping of terminology used on the Hardware Management Console versus the terminology used in the SDMC. Terminology might change slowly, so you might see and hear old terminology mixed with new terminology for a period of time.

Table 1-4 Side-by-side comparison of terminology

| HMC terminology | SDMC terminology |
|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Managed System | Server |
| Frame / BPA | Power Unit |
| LPAR / Logical Partition | Virtual Server |
| Users: hscpe, hscroot | pe, sysadmin |
| HMC Roles: <ul style="list-style-type: none">▶ hmcsuperadmin▶ hmcoperator▶ hmcuser | Director Roles: <ul style="list-style-type: none">▶ SMAAdministrator▶ SMManager▶ SMUser |
| Partition mobility | Relocation |
| Remove connection | Remove a managed endpoint (MEP) |
| Server/Frame/LPAR states For example, Operating (see Table 5-1 on page 90 for additional information) | Director states, for example, Started |

1.6 Functional differences

The SDMC incorporates most functions of the Hardware Management Console. This incorporation has been done through direct mapping of commands or by replacing functions that are present already in IBM Systems Director. Some functions are not available in the first release of the SDMC, notably the ability to handle system plans.

The command-line interface has been mostly kept the same. On the SDMC, most of the commands are just preceded by `smcli`. This new prefix might require changes to existing scripts that use the Hardware Management Console.

Though the SDMC retains most of the features that were available in the HMC, there are a few functional differences that exist between the SDMC and the HMC. These differences are directed towards adapting to the IBM Systems Director environment and also towards making the user interface simpler and more intuitive.

This section describes the functional differences between the HMC and the SDMC.

1.6.1 Enhanced virtualization management

Here are some of the key enhancements in virtualization management that are available in the SDMC:

- ▶ SDMC offers a simplistic IVM-like user interface for virtualization functions, such as creating a Virtual Server.
- ▶ The views of Virtual Server properties and dynamic logical partitioning are combined to present a single view from where you can perform all Virtual Server operations.
- ▶ SDMC provides the ability to modify the resource assignment of your Virtual Servers even when they are in the stopped state.
- ▶ SDMC can now manage virtual slots automatically leading to an enhanced VIOS management.

1.6.2 Users and roles

The concepts of users and roles in the SDMC remain the same as it was in the HMC. The user interfaces for creating and managing users and roles have changed in the SDMC. SDMC follows the IBM Systems Director way of creating and managing users and roles. SDMC supports the usage of LDAP and Kerberos servers. You can create users that use LDAP or Kerberos for authentication. Resource roles in HMC are referred to as Groups in SDMC. Also, the session timeout and the idle timeout settings are global and not configured per user.

1.6.3 Additional functions

The SDMC comes with the IBM Systems Director base management functions which offers you additional capabilities to manage your heterogeneous and large homogeneous infrastructure better. These capabilities include:

- ▶ Automation manager
- ▶ Status manager
- ▶ Firmware and device microcode updates through the Update Manager
- ▶ Call home support

1.6.4 User interface enhancements

SDMC provides you with an user interface that is tightly integrated with the broader IBM Systems Director user interface. Most of the tasks in SDMC have the same flow they had in HMC, with slight enhancements and adjustments made to provide an IBM Systems Director look and feel. Some of the functions have been enhanced for ease of use.

1.6.5 Redundancy model

The existing redundancy model available in HMC is available in the SDMC as well. You can connect two SDMCs to a managed system, where an SDMC can act as the redundant SDMC. You can also use an HMC for redundant management. Apart from this redundancy model, IBM Systems Director provides an active-passive availability model that is optional for the SDMC users. In this model, two SDMC nodes can manage a single server, of which one node is used (active) and the other is not used (passive) waiting for failover. The existing HMC active-active redundancy model is available in addition to the active-passive availability model provided by the IBM Systems Director.

1.6.6 Backup and restore

SDMC provides the capability to back up the whole virtual machine onto removable media or a remote FTP server. You can restore using the backup file from the removable media or from a remote FTP server. The restore will be full image deployment and all existing files will be replaced from the backup. Unlike the HMC, SDMC backs up the entire disk instead of individual files.

The backup function requires that the SDMC be temporarily shut down to quiesce the disks, but it will be immediately restarted while the disk files are copied to removable media or a remote FTP server. The restore function takes under an hour to complete.

1.6.7 SDMC considerations

Here is the list of limitations for SDMC when compared with the HMC:

- ▶ The system plans feature is not available in SDMC.
- ▶ Replication of user data, groups data, LDAP or Kerberos configuration data, and outbound connectivity configuration data is not supported in SDMC.
- ▶ Management of POWER5™ technology-based systems is not supported.
- ▶ There is no modem or VPN support for the Call Home function.
- ▶ Capturing of log information using the **pedbg** command is less granular.
- ▶ Disconnecting and reconnecting to old sessions of SDMC is not possible.

Archived

Installation

In this chapter, we describe the installation of the IBM Systems Director Management Console (SDMC). We describe in detail the requirements for the hardware and software installation, the installation of the hardware and software appliance itself, and the setup wizard.

2.1 Prerequisites

This section lists the requirements and pre-requisites for the hardware and software appliance. The hardware appliance is required for all midrange and high-end systems (POWER6 technology based 550 server and higher, and POWER7 technology-based 750 servers and higher).

2.1.1 Hardware appliance

The hardware appliance comes preloaded on IBM x86 hardware (7042-CR6). The hardware appliance consists of a virtual image (guest) that resides on a Red Hat linux (host), as shown in Figure 1-4 on page 8. The host hypervisor is transparent and does not require user interaction. The requirements for both the host and the guest are defined in Table 2-1.

Table 2-1 Hardware appliance requirements

| | |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host configuration | <ul style="list-style-type: none">▶ 4-core CPU (Intel® Nehalem architecture)▶ 8 GB RAM▶ Two 500 GB disks (with RAID 0)▶ Two network interface cards (NIC) minimum |
| Guest configuration | <ul style="list-style-type: none">▶ Four virtual CPUs▶ 6 GB RAM▶ 500 GB disk▶ Two to four network interface cards (NIC) |

2.1.2 Software appliance

The software appliance is only supported on IBM x86 hardware. The software appliance also consists of a host/guest system; the hardware requirements are listed in Table 2-2. The CPU and memory parameters for the guest configuration (the virtual machine) should be reserved for use of the software appliance; the parameters for the host configuration (the hardware) are used for both the hypervisor and software appliance together and should meet the minimum requirements.

Table 2-2 Software appliance hardware requirements

| | |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host configuration | <ul style="list-style-type: none">▶ 4-core CPU (Intel Nehalem architecture or better)▶ 8 GB RAM▶ 500 GB of disk space▶ Between one and four Ethernet adapters |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| | |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Guest configuration | <ul style="list-style-type: none"> ▶ Four virtual CPUs ▶ 6 GB RAM ▶ 500 GB disk (can be thin-provisioned) ▶ Between one and four Ethernet adapters |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Recommendation: Although the disks in the guest configuration can be thin provisioned, we do not recommend it. There is no guarantee that the disk space is there when it is needed, which would cause problems.

The supported host operating systems and hypervisors are:

- ▶ Red Hat Enterprise Linux (RHEL) 5.5 with KVM (kvm-83-164.el5) or later. Requires at least one network bridge.
- ▶ VMware ESXi 4.01 or later.
- ▶ VMware ESX 4 or later.

The VMWare hypervisor requires another machine to be configured with either:

- ▶ Windows® XP with VMware Virtual Infrastructure Client or VMware OVF Tool installed
- ▶ Linux (preferably Red Hat Enterprise Linux (RHEL 5.5)) with VMware OVF Tool installed

For the system firmware levels, POWER servers require 7.3.0 of the POWER firmware to support SDMC with one exception: POWER6 technology-based POWER processor-based blades firmware requires level 3.5.7.

2.2 Installation of the hardware appliance

The hardware appliance is required for midrange and high-end Power Systems, but can also manage low-end systems. The hardware appliance comes pre-installed on the IBM x86 hardware (a 7042-CR6). Set up and configure the system with the setup wizard, as shown in 2.4, “Setup wizard” on page 28.

The hardware appliance consists of a virtual image that resides on a Red Hat Linux configured host system (see Figure 1-4 on page 8). Login to the host system or access the hypervisor are not permitted. All communications will be done through a special channel from guest to host.

2.2.1 Hardware installation

For the hardware appliance, you need at least one network connection to connect to the service processor of your POWER machines. To configure a private and an open network, as shown in Figure 2-1, you need at least two network connections: One in an open network over which you can reach the SDMC through a web browser, and one private network for connecting the SDMC with the service processor of your POWER machines, as shown in Figure 2-1.

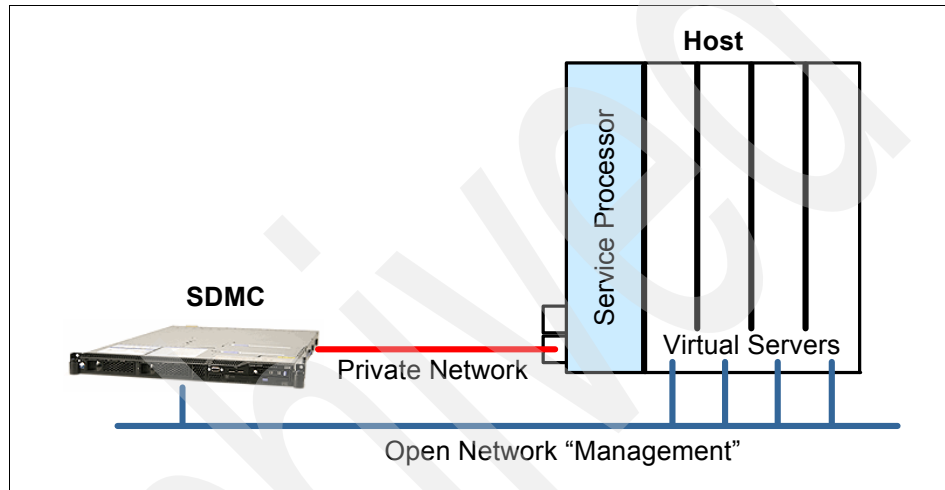


Figure 2-1 SDMC connection

2.2.2 Hardware appliance installation

To reinstall the hardware appliance, use the two installation DVDs that came with the hardware. Installation options include a direct installation from the DVDs or a Network (PXE) boot.

The installation from the DVDs takes nearly an hour. To install the hardware appliance, you should perform the following steps.

Note: At the time of writing, only an early build of the hardware appliance was available; therefore, the next steps could be different.

1. Insert DVD1 and boot from it. You are asked if you want to erase all existing data on disk. Select **[Y]es**, and then choose the disk to which to install.

2. After DVD1 is copied, the following prompt appears:

Press Enter to shutdown the system. After the system is powered off, apply power and remove media from the drive to complete the installation.

Follow those instructions. After the system powers down, make sure you remove the first DVD as soon as you power on the system.
3. After the system regains power, you see the following prompt:

Please insert media 2 into the drive, and press Enter when ready.

Insert DVD2 and press Enter.
4. At the end of the installation process, the setup wizard (see 2.4, “Setup wizard” on page 28) will appear, with which you can do the initial configuration of the SDMC.

2.3 Installation of the software appliance

The SDMC software appliance can be installed in the customer's existing x86 virtualized infrastructure (see 2.1, “Prerequisites” on page 16 for the minimum hardware requirements). Customer supplied virtualization hypervisor options include VMware (vSphere server and ESXi Version 4 or later; at least Version 4.1 is required if USB support is desired) and Red Hat Enterprise Linux (RHEL) Enterprise KVM Version 5.5 or later.

2.3.1 SDMC software appliance installation media specifics

The following media is available for installation:

- ▶ Users can install from DVD media. Due to the single-layer DVD size limitation, the shipped media will contain multiple DVDs containing disk images, OVF, and a manifest.

You can order the media from the ESS Web site:

<http://www.ibm.com/eserver/ess>

2.3.2 VMware installation

For the SDMC installation, the user can use any of the standard mechanisms in VMware to deploy an OVF/OVA file. Two deployment methods will be supported for VMware ESX and ESXi 4:

- ▶ A command-line utility using the OVF Tool

- A graphical interface on the VMWare Virtual Infrastructure Client

To use the CLI method of deployment for VMware, customers must install the VMware OVF Tool on a Windows or Linux machine. Download the VMware OVF Tool from the following address:

<http://communities.vmware.com/community/vmtn/vsphere/automationtools/ovf>

Note: In the below examples for the CLI installation, the thin provisioned format is selected as the format to store the virtual machines virtual disks. In this format, the storage is allocated on demand as data is written to the virtual disks. This is only supported on VMFS3 and newer datastores. Otherwise, the thick format, in which the storage is allocated immediately, can also be used.

Note: If using thin provisioning as in the below examples, ensure that you have the space needed to contain the SDMC data. Using thick provisioning would guarantee that you have the required storage.

After performing either of the above steps to deploy the OVA file and create the SDMC appliance, the user needs to configure the public and private network interfaces on the VM client within VMware. The user can then map the logical adapters in the SDMC image to the VMnetworks defined in VMware as part of the Setup Wizard process. Refer to 2.4, “Setup wizard” on page 28 for more information.

Steps for using VMware vSphere Client with OVA (web download)

The SDMC software appliance installation can be performed from the vSphere client GUI using the OVA downloaded from the IBM website by performing the following steps.

Note: vSphere Client is only available for Windows and can be downloaded from the web address for the ESX or ESXi Server.

1. Obtain the OVA file that contains the SDMC Virtual Machine.

2. Select **File** → **Deploy OVF Template**, as shown in Figure 2-2.

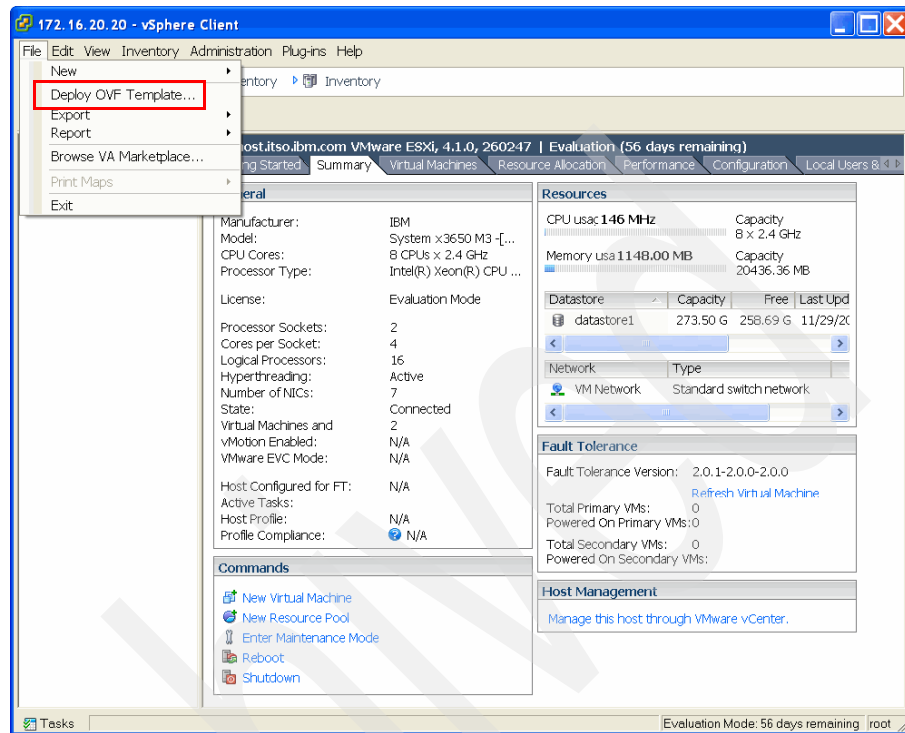


Figure 2-2 Deploy OVF Template from vSphere Client

3. Select the **Deploy from file** radio button and click the **Browse** button. Navigate to the folder you created, highlight the OVA, and click **OK**. Click **Next**, as shown in Figure 2-3.

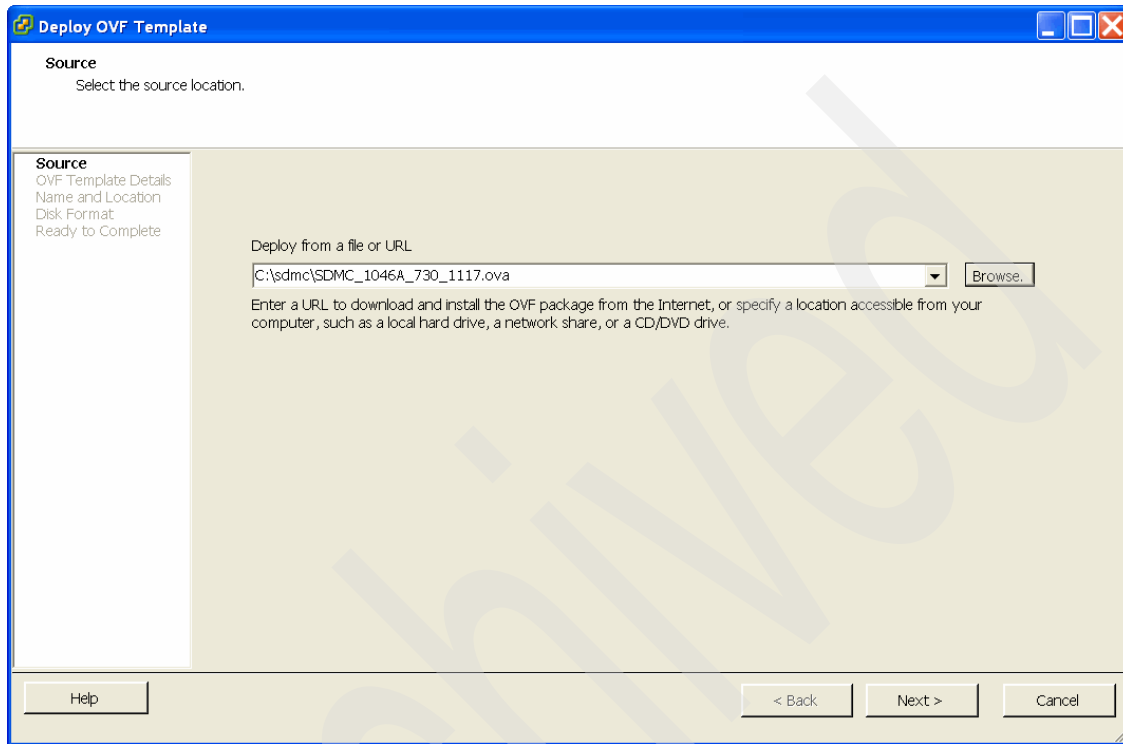


Figure 2-3 Deploying from a file or URL

- Continue through the pages until you reach the **Ready to Complete** page. Review the deployment settings and click **Finish** to start the deployment of the SDMC (Figure 2-4).

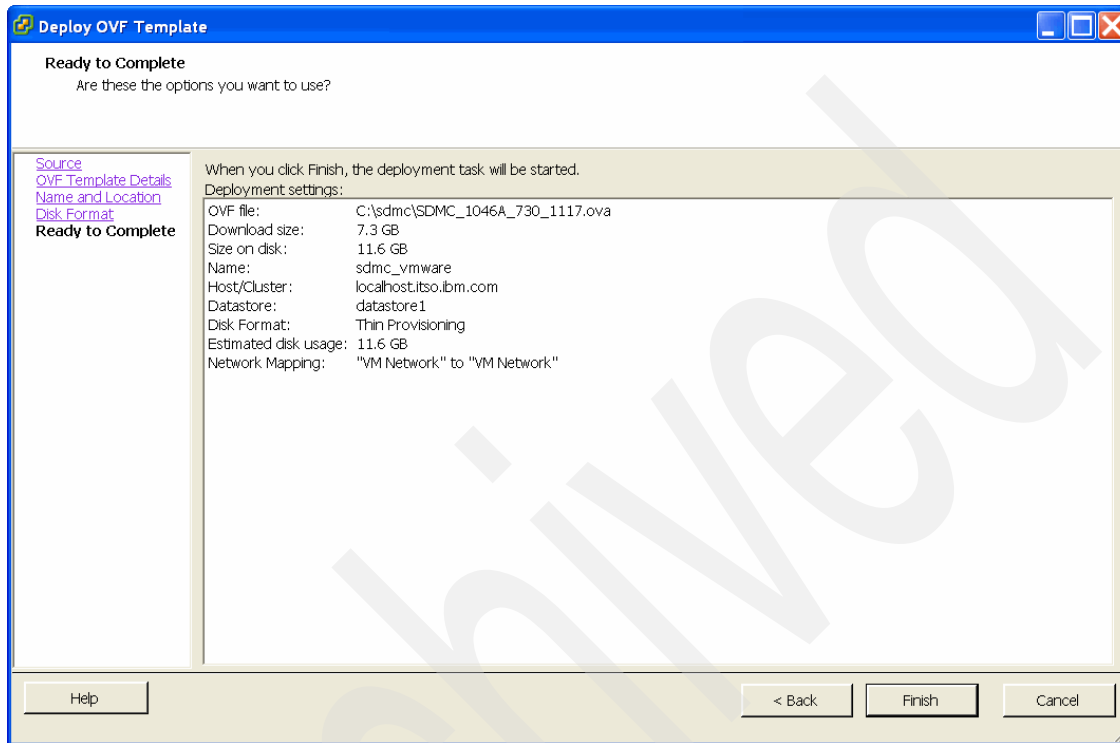


Figure 2-4 Ready to Complete page: A summary of the deployment settings

Steps for using the OVF Tool CLI with OVA

To use the OVF Tool CLI with OVA, perform the following steps:

- Obtain the OVA file that contains the SDMC Virtual Machine.

2. Because all files and images needed are contained within the OVA, you can simply deploy the package. Note that the descriptive syntax within and including the <> should be replaced with the appropriate user-specified string:

- On Linux:

```
/usr/bin/ovftool --name=SDMC -ds=<datastore name on ESX>  
[-dm=thin] <OVA filename> vi://<user>:<password>@<ESX hostname>
```

- On Windows (Example 2-1):

```
"Program Files\VMware\VMware OVF Tool\ovftool.exe" --name=SDMC  
-ds=<datastore name on ESX> [-dm=thin] <OVA filename>  
vi://<user>:<password>@<ESX hostname>
```

Example 2-1 OVF Tool CLI using an OVA file on Windows

```
C:\>"Program Files\VMware\VMware OVF Tool\ovftool.exe" --name=sdmc  
-ds=datastore1 -dm=thin "c:\sdmc\SDMC_1046A_730_1117.ova"  
"vi://root:passw0rd@172.16.20.20"  
Output:  
Opening OVA source: c:\sdmc\SDMC_1046A_730_1117.ova  
Opening VI target: vi://root@172.16.20.20/  
Target: vi://172.16.20.20/
```

2.3.3 Red Hat KVM installation

You can install the SDMC software appliance on KVM by using the pre-installed virtual disks.

Installing the SDMC software appliance from pre-installed virtual disks

To install the SDMC software appliance from pre-installed virtual disks, perform the following steps:

1. Verify that virtualization software is installed on RHEL.

You must have KVM, libvirt, and VM manager installed. Run the **virsh** command as root to determine whether you can see the virsh shell.

2. Download <SDMC Installation filename>.tar.gz to the host.
3. Extract virtual disk images from CSDA.tar.gz by running the following command:

```
tar -xzf SDMC_1046A_730_1117.tar.gz
```

This command extract the disk images (dvm disk1.img, dvm disk2.img, dvm disk3.img,...dvm disk7.img).

4. Create the domain XML file (or use the template, if it is present).

You have to provide custom values for the following fields:

- MAC addresses (mac address tag). You can use the following script to generate MAC addresses:

```
echo -n 00:1A:64 ; for i in `seq 1 3` ; do echo -n `echo  
":$RANDOM$RANDOM" | cut -n -c -3` ;done; echo \n
```

Replace the 00:1A:64 with your preferred prefix.

- Bridge name (source bridge tag). To discover the available bridges on your host, run the **brctl show** command. A second bridge is needed for the private management network.
- VM name, source files for hard disks and CDROM. You might want to update the memory and CPU values.

Note: Do not use `<driver name='qemu' cache='writeback'/>` for disks. Although this tag improves disk I/O performance, it might cause image corruption. Refer to https://bugzilla.redhat.com/show_bug.cgi?id=572825 for details.

Also note the `<serial>` tag for the output of VM progress and other messages. Without it, the output of the OS boot will not go to the VNC session and you might think that the boot is hung.

Note: Do not use the default bridge `virbr0` that is visible after installing the virtualization software. This bridge is for outbound traffic of virtual machines only; incoming connections are not allowed.

There is an IBM document called *Quick Start Guide for Installing and Running KVM*, with a chapter on network bridging, that can be found on the IBM InfoCenter website at:

<http://publib.boulder.ibm.com/infocenter/lxinfo/v3r0m0/index.jsp?topic=/lxaai/kvminstall/lxaaikvminstallstart.htm>

Information is also available in the *Red Hat Enterprise Linux 5 Virtualization Guide*, which can be found at:

<http://www.redhat.com/>

Additional information can be found at:

http://wiki.libvirt.org/page/Networking#Creating_network_initscripts

See the sample `domain.xml` file in Example 2-2. The tags that might have to be customized for your specific environment have been annotated in bold.

Example 2-2 Sample domain.xml file

```
<domain type="kvm">
  <name>VM1</name>
  <uuid/>
  <memory>6144000</memory>
  <vcpu>4</vcpu>
  <os>
    <type arch="x86_64">hvm</type>
    <boot dev="hd"/>
  </os>
  <features>
    <acpi/>
  </features>
  <clock offset="utc"/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>destroy</on_crash>
  <devices>
    <disk type="file" device="disk">
      <source file="/vdisk1/vm1/dvmdisk1.img"/>
      <target dev="vda" bus="virtio"/>
    </disk>
  </devices>
</domain>
```

```

</disk>
<disk type="file" device="disk">
  <source file="/vdisk1/vm1/dvmdisk2.img"/>
  <target dev="vdb" bus="virtio"/>
</disk>
<disk type="file" device="disk">
  <source file="/vdisk1/vm1/dvmdisk3.img"/>
  <target dev="vdc" bus="virtio"/>
</disk>
<interface type="bridge">
  <source bridge="virbr1"/>
  <mac address="00:1A:64:27:30:19"/>
  <target dev="vnet0"/>
  <model type="e1000"/>
</interface>
<interface type="bridge">
  <source bridge="virbr1"/>
  <mac address="00:1A:64:27:30:20"/>
  <target dev="vnet1"/>
  <model type="e1000"/>
</interface>
<interface type="bridge">
  <source bridge="virbr1"/>
  <mac address="00:1A:64:27:30:21"/>
  <target dev="vnet2"/>
  <model type="e1000"/>
</interface>
<interface type="bridge">
  <source bridge="virbr1"/>
  <mac address="00:1A:64:27:30:22"/>
  <target dev="vnet3"/>
  <model type="e1000"/>
</interface>
<serial type="file">
  <source path="/vdisk1/vm1/boot.log"/>
  <target port="1"/>
</serial>
<input type="mouse" bus="ps2"/>
<graphics type="vnc" autoport="yes" listen=""/>
<video>
  <model type="cirrus" vram="9216" heads="1"/>
</video>
</devices>
</domain>

```

5. Define VM by running the following command:

```
virsh define <domain>.xml
```

6. Start VM by running the following command:

```
virsh start VM_name
```

Run the Setup Wizard on the KVM virtual machine console to customize the VM. Refer to 2.4, “Setup wizard” on page 28 for more details.

2.4 Setup wizard

The setup wizard guides you through the installation process. You must perform the following steps:

1. Select the locale for the system (see Figure 2-5). Click **OK**.

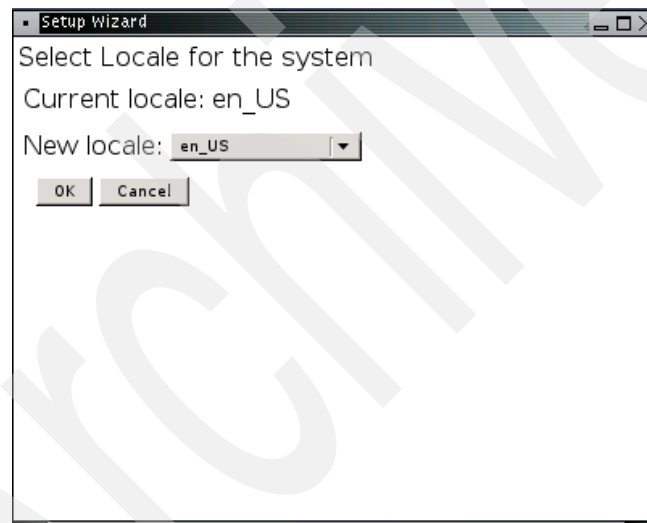


Figure 2-5 Selecting the locale for the system

At the time of the writing of this book, the following languages are supported:

- de: German
- en: English
- es: Spanish
- fr: French
- it: Italian
- ja: Japanese
- ko: Korean

- pt_br: Brazilian Portuguese
- zh_CN: Simplified Chinese
- zh_TW: Traditional Chinese

2. Accept the IBM Software License Agreement (Figure 2-6).

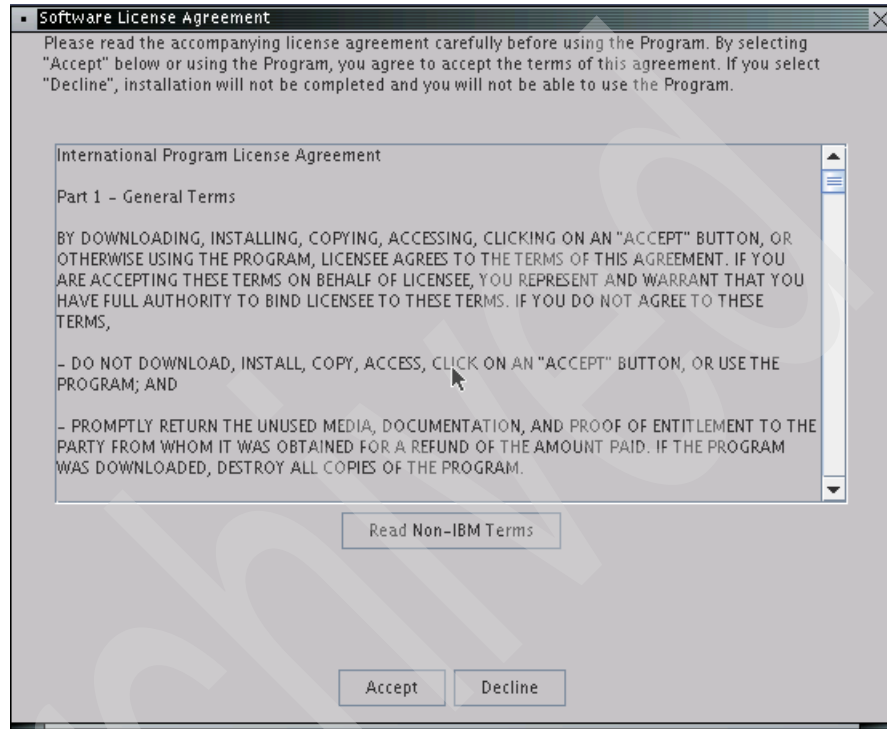


Figure 2-6 IBM Software License Agreement

3. After accepting the license agreement, the Welcome page of the setup wizard opens (Figure 2-7).

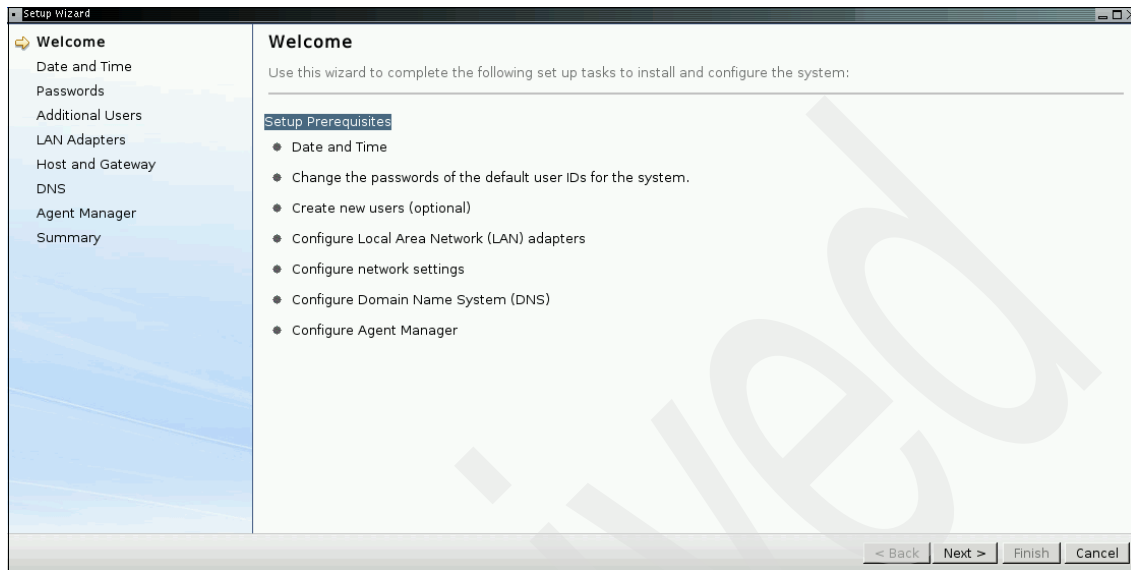


Figure 2-7 Setup Wizard Welcome page

Click **Next**.

4. Enter the date, time, and time zone for your location (Figure 2-8).

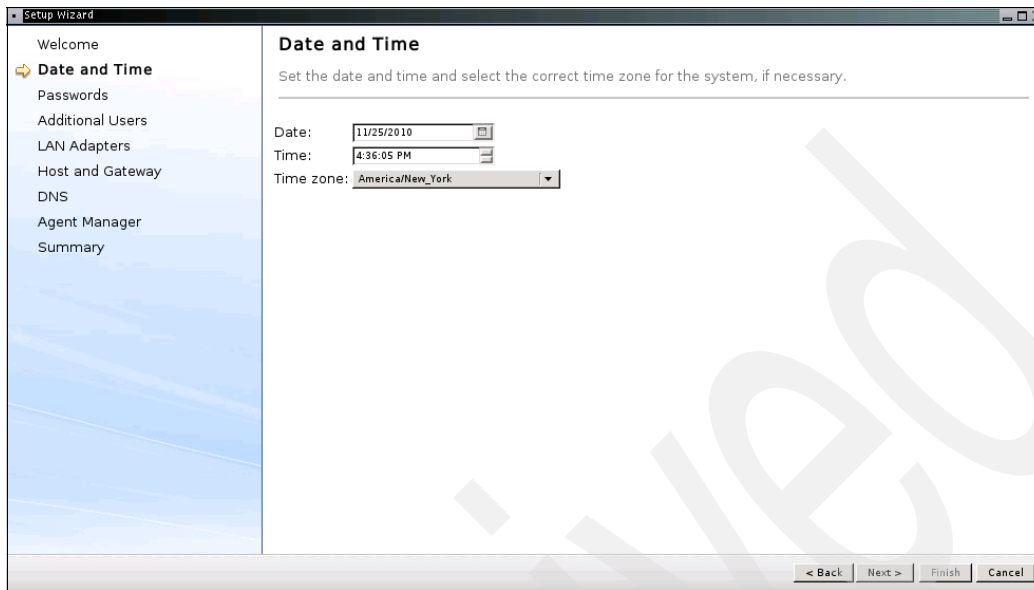


Figure 2-8 Date and Time page

5. The next four pages request the passwords for the sysadmin, root, and pe users (Figure 2-9).

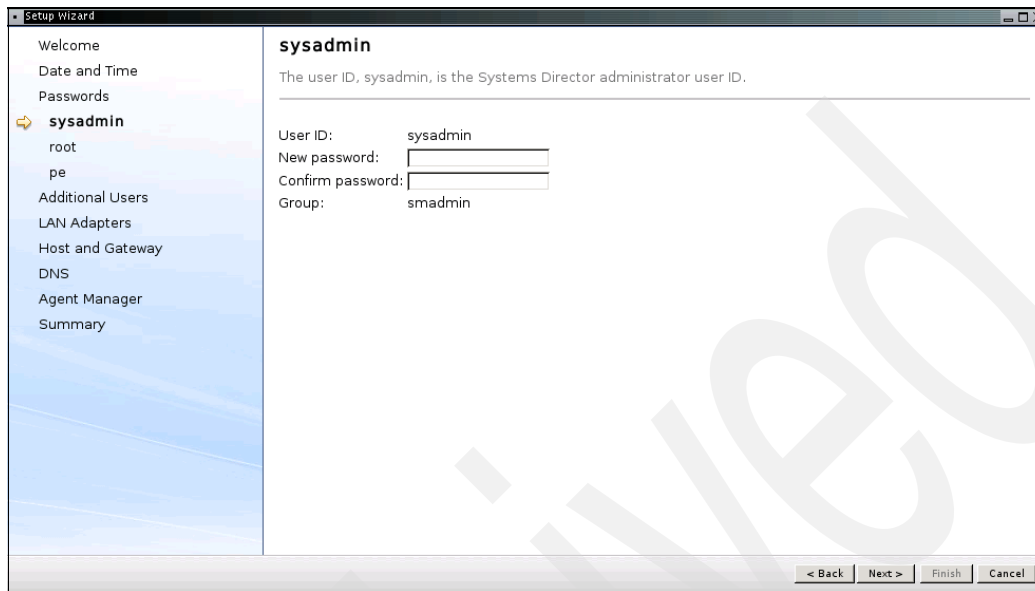


Figure 2-9 Setup of passwords

You should change them from the default password. The meaning of the users are as follows:

- | | |
|-----------------|-------------------------------------------------------------------------------------------------------------|
| sysadmin | The sysadmin user ID is the Systems Director administrator user ID (similar to the hscroot user on an HMC). |
| root | The root user ID is the service user ID for Systems Director. |
| pe | The pe user ID is the product engineer user ID for Systems Director (analogous to hscpe user on HMC). |

Use the following password rules:

- The password must contain at least seven characters, with a maximum of eight.
- The characters should be standard 7-bit ASCII characters.
- These characters include the characters A-Z, a-z, 0-9, and many special characters, such as tilde (~), exclamation mark (!), at sign (@), number sign (#), dollar sign (\$), percent sign (%), caret (^), ampersand (&), asterisk (*), left and right parentheses (), underscore (_), plus sign (+), hyphen (-), equals sign (=), left and right curly braces { }, left and right

square brackets ([]), backslash (\), colon (:), quotation mark ("), semicolon (;), and apostrophe (').

- Passwords can include special characters, but passwords must begin with an alphanumeric character.
6. Afterwards, you can optionally create additional users (Figure 2-10). You can do this step also after the setup is finished. Refer to 9.1, “User management and security” on page 198 for further information about users and roles.

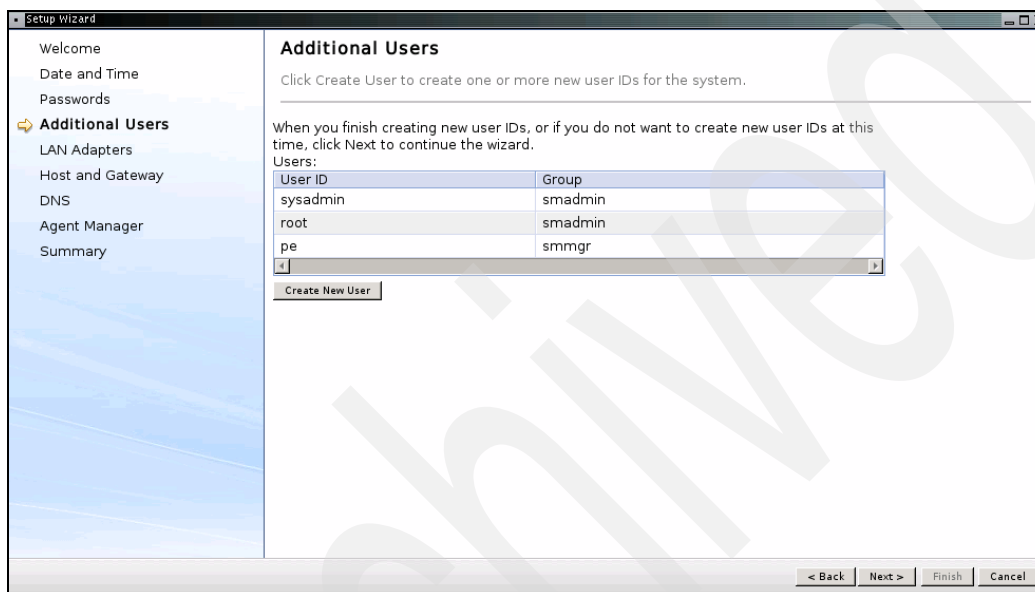


Figure 2-10 Creating additional users

7. The next pages set up the LAN-Adapters, Host and Gateway, and DNS. These steps are explained in detail in 9.2.1, “Configuring network settings” on page 241, so they will not be shown here.

8. The last page to complete is the Agent Manager configuration page (Figure 2-11). Here you have to provide the Resource Manager user ID, the Resource Manager password, and the Agent Registration password. You can specify different passwords, but you only need to remember them if you plan to use redundant management with the agents.

Information: IBM Systems Director uses a function called Agent Manager. The Agent Manager handles credentials and certificates between IBM Systems Director (referred to as the resource manager in the Agent Manager) and the common agent that is installed on a managed systems. The common agent reports informations about the managed system to the resource manager (IBM Systems Director) and performs tasks on the managed system as directed by the resource manager. For further information, refer to section 1.5, “Common Agent Services”, in *Implementing IBM Systems Director 6.1*, SG24-7694.

The screenshot shows a window titled "Setup Wizard" with a sidebar on the left containing the following links: Welcome, Date and Time, Passwords, Additional Users, LAN Adapters, Host and Gateway, DNS, **Agent Manager** (highlighted with a blue background and a right-pointing arrow), and Summary. The main area is titled "Configure Agent Manager" and contains the text: "IBM Systems Director uses common agent services for managing endpoints. The Agent Manager manages security of the common agents and management servers." Below this text are five input fields with labels: "*Resource Manager user ID:" (containing "admin"), "*Resource Manager password:" (masked with dots), "*Confirm Resource Manager password:" (masked with dots), "*Agent Registration password:" (masked with dots), and "*Confirm Agent Registration password:" (masked with dots). At the bottom right of the window are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Figure 2-11 Configure Agent Manager

9. After completing the last page and clicking **Next**, the Summary page opens (Figure 2-12). You can always go back from here to change some or all of the values you have entered.

Summary

Review the following settings, then click Finish. You can change some settings on this page, to change any other settings, click Back.

Date and Time

Date: 11/25/2010
Time: 4:36:05 PM
Time zone: America/New_York

Users

| User ID | Group | Description |
|----------|---------|----------------------|
| sysadmin | smadmin | System Administrator |
| root | smadmin | Service |
| pe | smmgr | Product Engineer |

LAN Adapters

LAN interface address: eth0 000C2918D2B5
Network type: Standard network interface
IP address: 172.16.20.25
Network mask: 255.255.255.0
Static IPv6 address: Prefix length

Host and Gateway

*Host name: sdmc-vmware
*Domain name: itso.ibm.com
*Gateway address: 172.16.20.1
IPv6 gateway address:
*Gateway device: any
*Host name IP address: 172.16.20.25

Configure Domain Name System (DNS)

Enable DNS services: false
DNS server search order:

< Back Next > Finish Cancel

Figure 2-12 Summary page

If you are satisfied with your choices, click **Finish**.

10.If all went well, you see the System Setup Processing page; a status of Success should be behind every listed item (Figure 2-13).

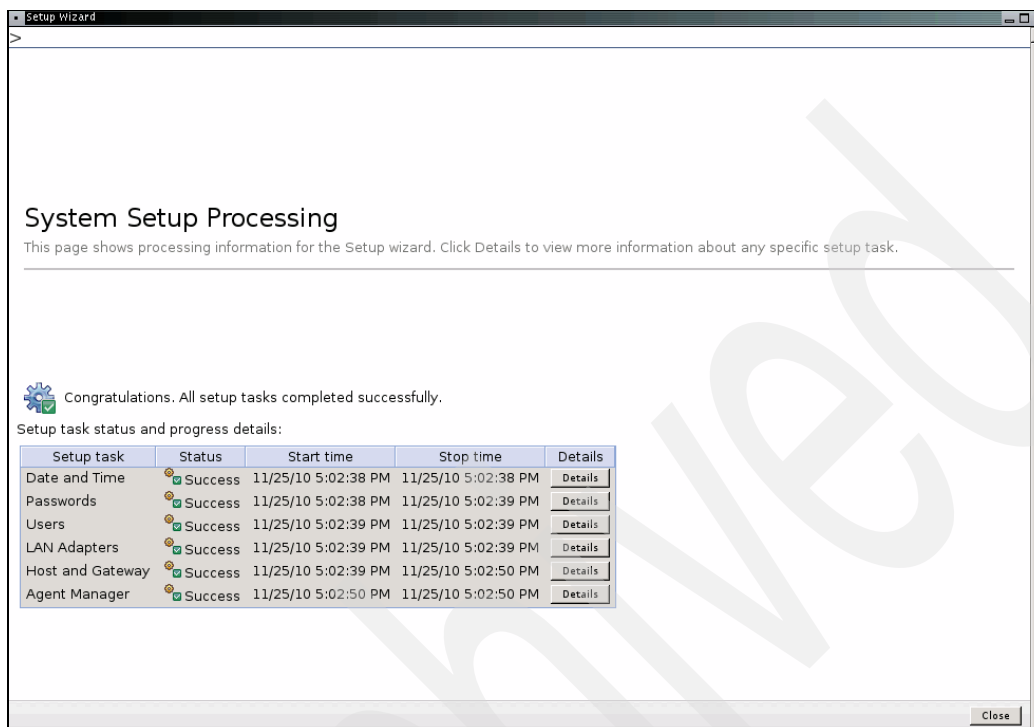


Figure 2-13 System Setup Processing page

If anything failed, you can view the cause by clicking the **Details** button.

11. After clicking **Close**, the SDMC boots and a startup page opens (Figure 2-14).

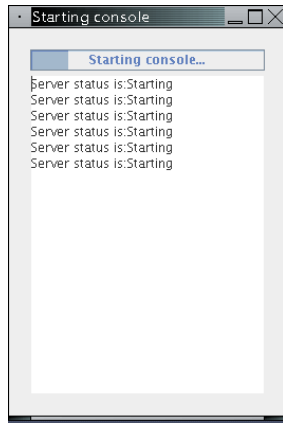


Figure 2-14 Console starting page

The startup takes up to five minutes. When the startup is finished, the Systems Director login page opens (Figure 2-15).

Note: Depending on the browser you use, you eventually have to accept a HTTPS-Certificate when accessing the appliance remotely.



Figure 2-15 IBM Systems Director login page

You can now access the SDMC either locally through the embedded browser, or remotely through a browser using `https://<address_of_your_SDMC>`, or using SSH.

2.5 SDMC software licensing requirements

The SDMC hardware appliance and software appliance has requisite product feature codes and software licensing that need to be purchased. In addition to the SDMC appliances, all of the servers managed by the SDMC(s) also need purchased licenses. These systems can be entry, mid, or high-end systems.

2.5.1 SDMC hardware appliance

For the SDMC hardware appliance, the customer needs to order the 7042-CR6 machine type with the SDMC feature code, including additional memory and a hard drive. When the SDMC feature code is ordered, the requisite SDMC software PIDs (5765-MCH) and SWMA PIDs (566x-MCH) are automatically appended to the order. The MCH SW and SWMA PIDs include license entitlement and support for the management server code.

2.5.2 SDMC software appliance

For the SDMC software appliance, the customer needs to license each installation of the management server code using SDMC software PIDs (5765-MCV) and SWMA PIDs (566x-MCV).

2.5.3 Licensing for cores of managed systems

In addition to the above SDMC licenses, the customer also needs to purchase licenses for any Power Systems cores they plan to manage with the SDMC. Managed core licenses are purchased by placing an order for IBM Systems Director Express Edition (5765-EXP). One year of software maintenance (SWMA) is included with the purchase of 5765-EXP. For additional SWMA orders, the customer places an order for IBM Systems Director Express Editions SWMA (566x-EXP).

Only the number of cores of the systems managed by SDMC(s) needs to be licensed, regardless of redundant management by multiple SDMCs.

Basic operation

This chapter provides an overview of features and tasks provided by IBM Systems Director Management Console (SDMC) and describes how to perform them using the graphical user interface.

3.1 Features overview

The SDMC is now available as part of the IBM Systems Director platform. This configuration provides a common appearance and navigation behavior with other management solutions, such as with IBM Tivoli products. The SDMC management functions seamlessly integrates with the base management functions that come with IBM Systems Director. All platform management functions are now managed from a single management interface.

The SDMC includes all the traditional server and virtualization management functions provided by the latest Hardware Management Console (HMC). These functions have the simplicity of the Integrated Virtualization Manager (IVM) interface. SDMC provides the following high level features:

- ▶ Power Server management
- ▶ PowerVM Virtualization management
- ▶ Power Unit (Frame) Management
- ▶ POWER processor-based blades management
- ▶ SDMC appliance management
- ▶ Service and support management
- ▶ Hierarchical management
- ▶ Update management

3.1.1 Power Server management

The Power Servers are referred to as *hosts* or *servers* in the SDMC. You can manage servers after discovering them from SDMC and requesting access to the server. Here are some of the common tasks that you can perform to manage your Power Server:

Discover servers and Power Units

Discovery is the process by which IBM Systems Director identifies and establishes connections with network level resources that it can manage. These resources include servers, switches, or printers. SDMC supports the discovery of Power Servers, Power Units (Bulk Power Controller) and POWER processor-based blades. Discovery in SDMC is a two step process compared to the one step process (Add Managed System) in the HMC.

| | |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Edit host | This task displays the properties of the server. The properties contain information about the processors, memory, I/O, and the capabilities of the server. This task should not be confused with the Properties task available on the context menu of the server, which displays the IBM Systems Director inventory information of the managed server. |
| Power on and power off | Use the Power On task to start a server. Use the Power Off task to shut down the server. |
| Manage passwords | You can change the SDMC access password when the server is in the Available state or update the password to set the admin, general, and the SDMC access passwords when the server is in the Waiting for Input state and the detailed state is Update Password Pending Authentication. |
| Capacity on Demand | Capacity on Demand (CoD) allows you to dynamically activate one or more resources on your server as your business peaks dictate. You can activate inactive processors and memory units that are already installed on your server on a temporary basis. |
| Power management | You can reduce the server's processor power consumption by enabling the Power Server mode. |
| Rebuild server | You can extract the configuration information from the server and rebuild the information on the SDMC. Rebuilding the server is useful when the state of the server is In Error and the detailed state is Incomplete. |
| Schedule operations | You can create a schedule for certain operations to be performed on the server without operator assistance. Scheduled operations are useful for situations where automatic, delayed, or repetitious processing of the server is necessary. The SDMC uses the IBM Systems Director scheduling to schedule the jobs. |
| Advanced System Management Interface | Advanced System Management Interface (ASMI) is a graphical interface that is part of the service processor firmware. The ASMI is required to set up the service processor and to perform service tasks, such as reading service processor logs, reading vital product data, and controlling the system power. |

Collect utilization data

You can set the SDMC to collect the resource utilization data for a specific server or for all the servers the SDMC manages. You can use this data to analyze trends and make resource adjustments.

3.1.2 PowerVM Virtualization management

SDMC provides you with all the PowerVM Virtualization management functions for the Power Server that you want to manage. Here are some of the virtualization management tasks that you can perform using the SDMC:

Create Virtual Servers

You can create a Virtual Server using the Create Virtual Server wizard. The user interface to create a Virtual Server is simplified and more intuitive in the SDMC.

Activate and shut down Virtual Servers

Use the Activate task to activate a Virtual Server on the server. You can activate a Virtual Server using its current configuration or any of its profiles.

Manage Virtual Servers

Use the Manage Virtual Server task to change the general properties and perform dynamic logical partitioning (DLPAR) operations on the Virtual Server. You can modify the processor, memory, and adapter assignments for a Virtual Server even when it is in the stopped state.

Manage profiles and system profiles

Use the Manage Profiles task to create, edit, copy, delete, or activate a profile for the selected Virtual Server. You can modify the resource configuration for a profile by editing it.

Mobility

Virtual Server mobility provides the ability to relocate a Virtual Server from one server to another. Active Virtual Server mobility allows you to relocate a started Virtual Server, including its operating system and applications, from one server to another. Inactive Virtual Server mobility allows you to relocate a stopped Virtual Server from one server to another.

Suspend and resume Virtual Servers

You can suspend Virtual Servers to store its state on a Storage Area Network (SAN). You can re-assign all processors and memory of a suspended partition to other partitions as needed. You can resume a suspended partition to bring it back to the started state. This feature is useful for performance management and energy management of servers.

Active Memory Sharing (AMS)

You can create a common pool of physical memory, which can be assigned to multiple Virtual Servers in a shared mode. AMS helps in increasing the memory utilization on the server.

Manage reserved storage device pool

Reserved storage device pool is an AMS pool of size zero. It is used to support a pool of storage devices on PowerVM Standard Edition for Virtual Server suspend and resume operations. This is available only if the server is capable of suspending and resuming.

Manage shared processor pools

Shared processors are physical processors whose processing capacity is shared among multiple Virtual Servers. You can assign a specific amount of processing capacity in a shared processor pool to each Virtual Server that uses shared processors.

Manage virtual networks

You can create and manage virtual switches (VSwitch) and virtual local area (VLAN) networks using this task.

Manage virtual storage

You can create and manage the virtual disks, storage pools, physical volumes, and optical devices in your server using this task.

3.1.3 Power Unit management

Here are some of the Power Unit management tasks that you can perform using the SDMC:

Initialize Power Unit Use this task to initialize a Power Unit. When you initialize a Power Unit, the I/O units and the servers contained within the Power Unit are powered on.

- Rebuild Power Unit** Use this task to rebuild the Power Unit information in the SDMC. Rebuilding the Power Unit is useful when the detailed state of the Power Unit is shown as Incomplete.
- Manage passwords** Use the change password task to change the SDMC access password on the Power Unit. You can use the Update password task to set the admin, general, and the SDMC access passwords when the Power Unit is in the Waiting for Input state and the detailed state is Update Password-Pending Authentication.
- Power on or power off I/O units**
Use this task to power on or power off an I/O unit. Only units or slots that reside in a power domain can be turned off.
- Bulk Power Assembly status**
Use this task to view the state of the connection from the SDMC to side A and side B of the bulk power assembly.

3.1.4 POWER processor-based blades management

The SDMC supports the management of the POWER processor-based blades. You can discover a POWER processor-based blade just like any other server, and after the SDMC is connected to the POWER processor-based blade, you can start managing it. You can only perform the tasks of which the POWER processor-based blade is capable.

3.1.5 SDMC appliance management

Here are some of the SDMC appliance management tasks that you can perform on the SDMC:

- Configure date and time**
Use this task to change the date and time of the SDMC appliance. You can also add or remove Network Time Protocol (NTP) servers that can be used by the SDMC appliance.
- Configure network** You can view the current network configuration for the SDMC appliance and also change the network settings.
- Configure Virtual Private Network (VPN)**
You can configure the VPN to allow inbound connectivity to the SDMC when working with remote support personnel.

Security and user management

You can create users and roles. You can assign permissions to roles and assign the roles to the user. This task allows the user to perform only the tasks that are assigned to the roles of the user. You can create groups of managed systems and assign them to a user to restrict management of only those managed systems. You are allowed to create user accounts in Lightweight Directory Access Protocol (LDAP) server or Kerberos servers.

3.1.6 Service and support management

Service and support manager (SSM) is an advanced manager available with the IBM Systems Director. It provides the overall serviceability of servers in an SDMC environment. It bundles the Electronic Service Agent™ (ESA), which performs the electronic service transactions to IBM, such as Call Home of serviceable problems, support files, inventory data, and performance management data. SDMC works in conjunction with SSM and provides service and support functions for Power Systems.

This section describes the features that are available as part of SSM for performing serviceability operations.

Monitoring supported Power Systems

SSM automatically adds Power Systems and Power Units into the Monitored Systems dynamic group upon discovery. SSM performs the following functions on behalf of the systems in the Monitored Systems group:

- ▶ Processing of serviceable events
- ▶ Collection of support files
- ▶ Collection of inventory
- ▶ Collection of performance measurement data

Processing serviceable events

SSM manages the entire life cycle of serviceable events and is responsible for the following functions:

- ▶ Detection of serviceable events
- ▶ Persistent storage and management of serviceable event data
- ▶ Transmission of service requests and extended error data to IBM
- ▶ Processing of duplicate events
- ▶ User actions for serviceable problems
- ▶ Closure of serviceable events

Support file management

SSM provides the following capabilities for managing support files such as extended error data collected along with serviceable events or system dumps:

- ▶ Collection of support files
- ▶ Transmission of support files to IBM
- ▶ Copying of support files to removable media devices
- ▶ Removal of support files from SDMC
- ▶ Space management of support files

Dumps

You can collect the following dumps using SSM:

- ▶ System
- ▶ System controller
- ▶ Node controller
- ▶ Resource controller
- ▶ Power

SSM tasks

SSM defines a number of tasks that can be performed on a periodic basis. These tasks include:

- ▶ Heartbeat task
- ▶ Inventory task
- ▶ Performance task

3.1.7 Hierarchical management

Hierarchical management is an environment where a global IBM Systems Director can discover and manage a SDMC and perform tasks on its managed systems. You have to enable the hierarchical management setting on the global IBM Systems Director and discover the SDMCs that you want to manage. This environment is useful when you want to use IBM Systems Director to manage multiple SDMCs and its managed systems at the same time.

3.1.8 Update management

The Update Manager is part of IBM Systems Director and provides tools for maintaining current versions of operating systems, device drivers, firmware, and BIOS, and IBM Systems Director code. Use the Update Manager to update your SDMC appliance. The update could be an update, upgrade, or an interim fix. You can use the Update Manager to perform firmware code updates.

3.2 Using the web interface

SDMC provides a web interface similar to the HMC. Power on the SDMC appliance and you should see the login page of the SDMC Graphical user interface. You can also access SDMC remotely using a browser such as Firefox or Internet Explorer.

For logging in remotely, open the browser and point the browser to the following URL:

`https://system_name`

system_name is the host name or IP address of the SDMC system.

A login page opens (Figure 3-1).

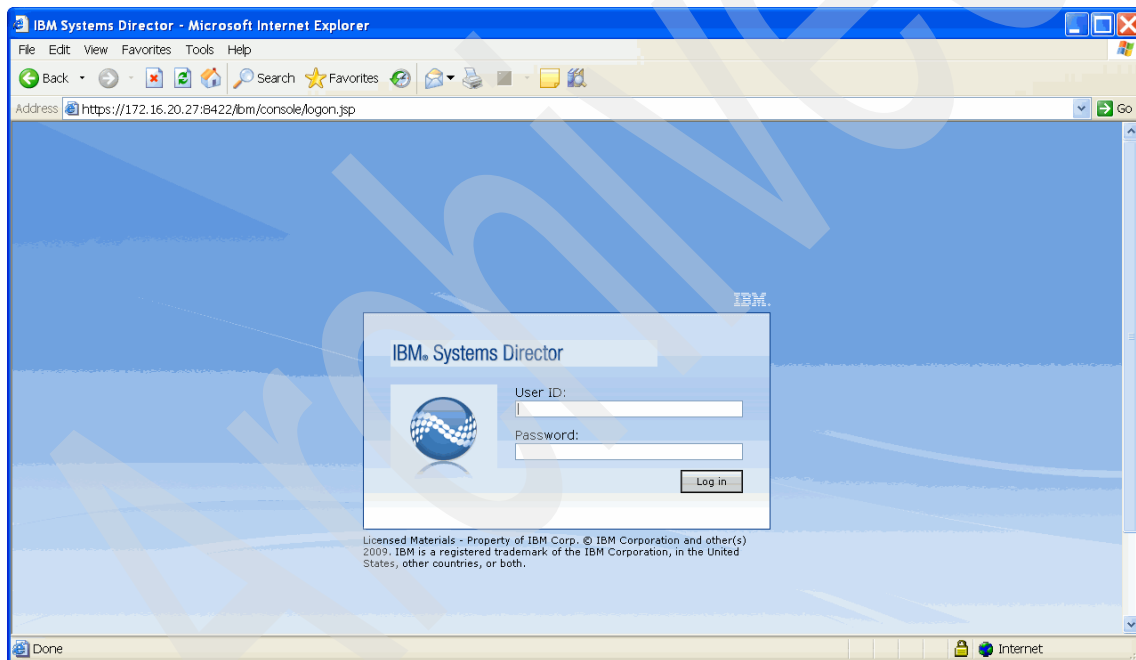


Figure 3-1 SDMC Login page

Enter the user ID and password that corresponds to an authorized SDMC user and click **Log in**. You should see the Welcome page (Figure 3-2) after logging in successfully into the SDMC.

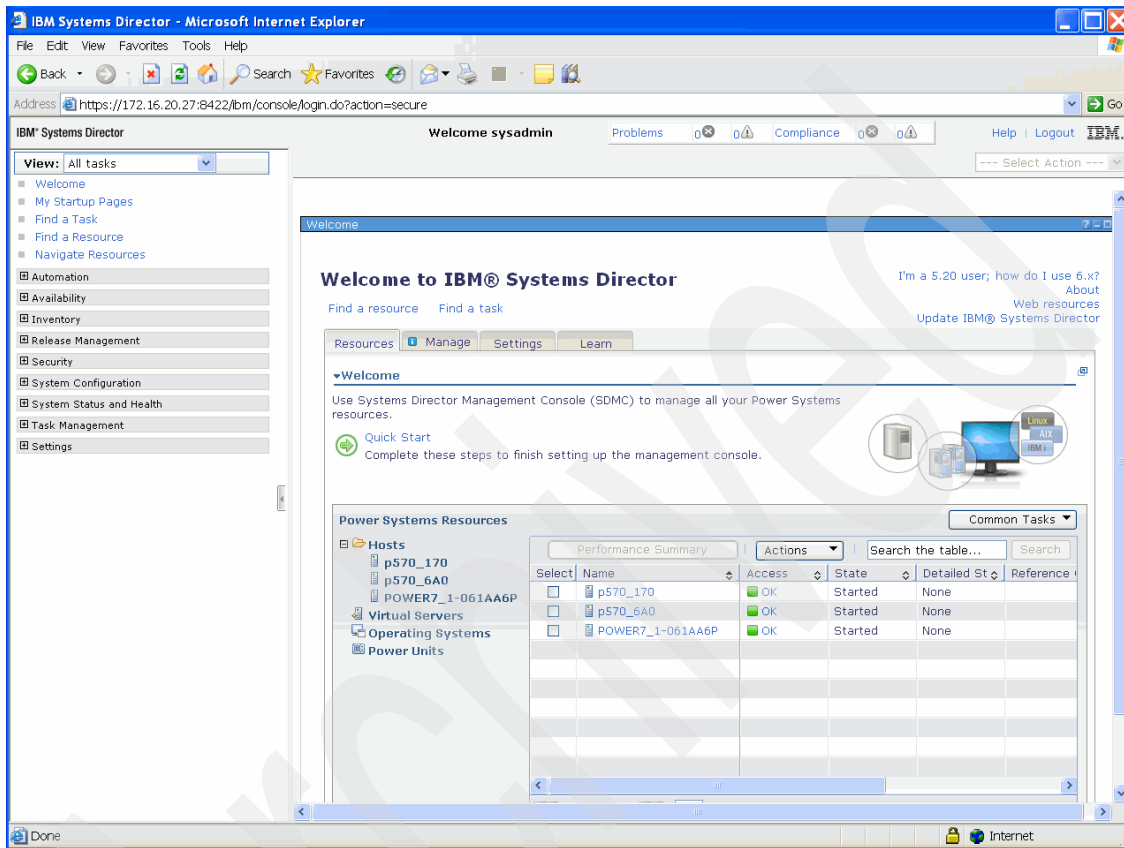


Figure 3-2 Welcome page

The Welcome page has four tabs:

- ▶ Resource
- ▶ Manage
- ▶ Settings
- ▶ Learn

The Resource tab provides a dashboard of all the servers, Virtual Servers, Power Units, and operating systems that your SDMC is currently managing. You can see the properties of these managed systems and can execute tasks on them using the context menu. You can also launch the common tasks, such as discovery, and transition away from the Welcome page. The Welcome page only shows the power resources that you will be managing using the SDMC.

There could be other non-Power Systems that are discovered and managed by SDMC. You can see these systems in the Navigate Resources page. The Welcome page has certain columns that are not available in the Navigate Resources page. These columns hold data specific to Power resources that the SDMC is managing.

The Manage tab in the Welcome page lists the various managers that are available in SDMC. You can click any of the managers to perform specific operations. The Settings tab provides the interface to the tasks that are related to managing your SDMC appliance itself. These tasks include:

- ▶ High availability settings
- ▶ Configure Date/Time
- ▶ Configure Network
- ▶ Configure VPN
- ▶ Service and Support Manager Getting Started Wizard
- ▶ Configure LDAP client
- ▶ Configure Kerberos client
- ▶ Create user account
- ▶ Change user account password
- ▶ View user accounts

You can click any of the tasks, which lead to a new tab on the content area where you can make changes to various settings.

3.2.1 Layout of the web interface

The SDMC web interface provides tasks and views to help you manage your environment. The web interface is composed of six areas, as shown in Figure 3-2 on page 50:

| | |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Navigation area | The navigation area, in the left portion of the web interface, provides categories of tasks that you can perform on your managed systems. Examples of typical tasks are Navigate Resources, Inventory, Security, System Status and Health, and Settings. |
| Content area | When you open the web interface, by default you see the Welcome page for SDMC in the content area. The content area changes depending on the item that you select in the navigation area. The content area displays the view, pages, or forms for the tasks that you launch on the managed systems. The views, pages, and forms are displayed as tabs in the content area. |

You can open multiple views or pages and have them open as tabs at the same time. You can switch between the tabs in the content area performing multiple operations at the same time.

Problems and Compliance status bar

This bar provides you with a quick snapshot of problems and compliance issues related to your environment. Click the number (if any) for the Problems or Compliance to view complete details about them in the Active Status view.

View list

This list helps you customize your navigation area. You can create your own list of tasks that you want to see in the navigation area and enable it by selecting it in the View list. For more information, see section 5.4.1, “Customizing the navigation area”, in *Implementing IBM Systems Director 6.1*, SG24-7694.

Select Action menu

This list provides the following ways to work with task pages:

- **My Startup Pages:** Customize the pages that are started automatically when you log into the SDMC.
- **Manage Open Pages:** You can close one or more open pages using this option.
- **Close page:** Close the current page that you are viewing.

Help

Displays the help information for the SDMC.

Logout

Logs you out of the SDMC.

3.2.2 Launching a task

You can launch all the tasks from the Welcome page itself. The hosts, Virtual Servers, and Power Units are listed under the Resources tab of the Welcome page. The tasks are available through the context menu of the listed resource. The Actions button also lists the tasks based on the selected resource. You have to click the **Actions** button after selecting the resource. The tasks pertaining to the selected resource are displayed and available. The tasks listed are based on the Operating state, Access state, and the Detailed state of the resource. The Detailed state is the state that uses the same terminology as in the HMC. The common tasks can be launched from the Common Tasks menu available in the Welcome page.

Figure 3-3 shows a snapshot of the layout of the management tasks on the context menu of the server.

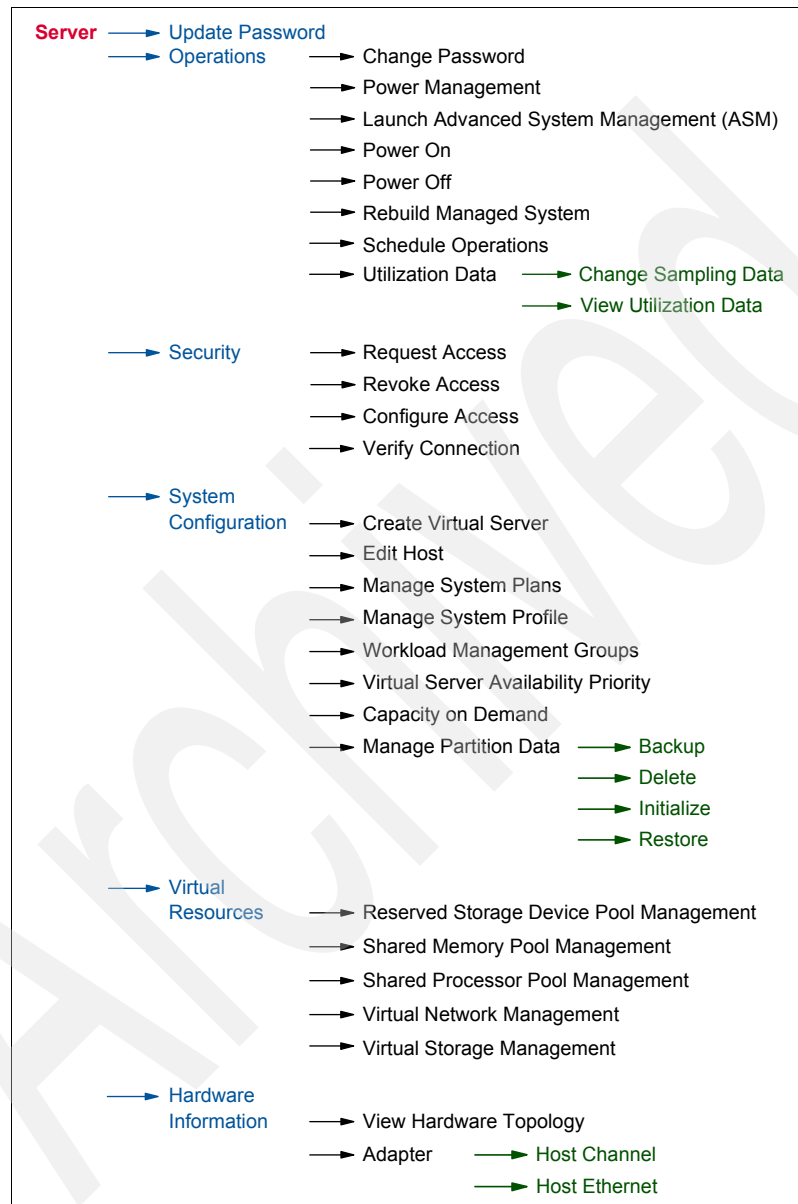


Figure 3-3 Context menu for server management

Figure 3-4 shows the other tasks that are available in the context menu of the server.

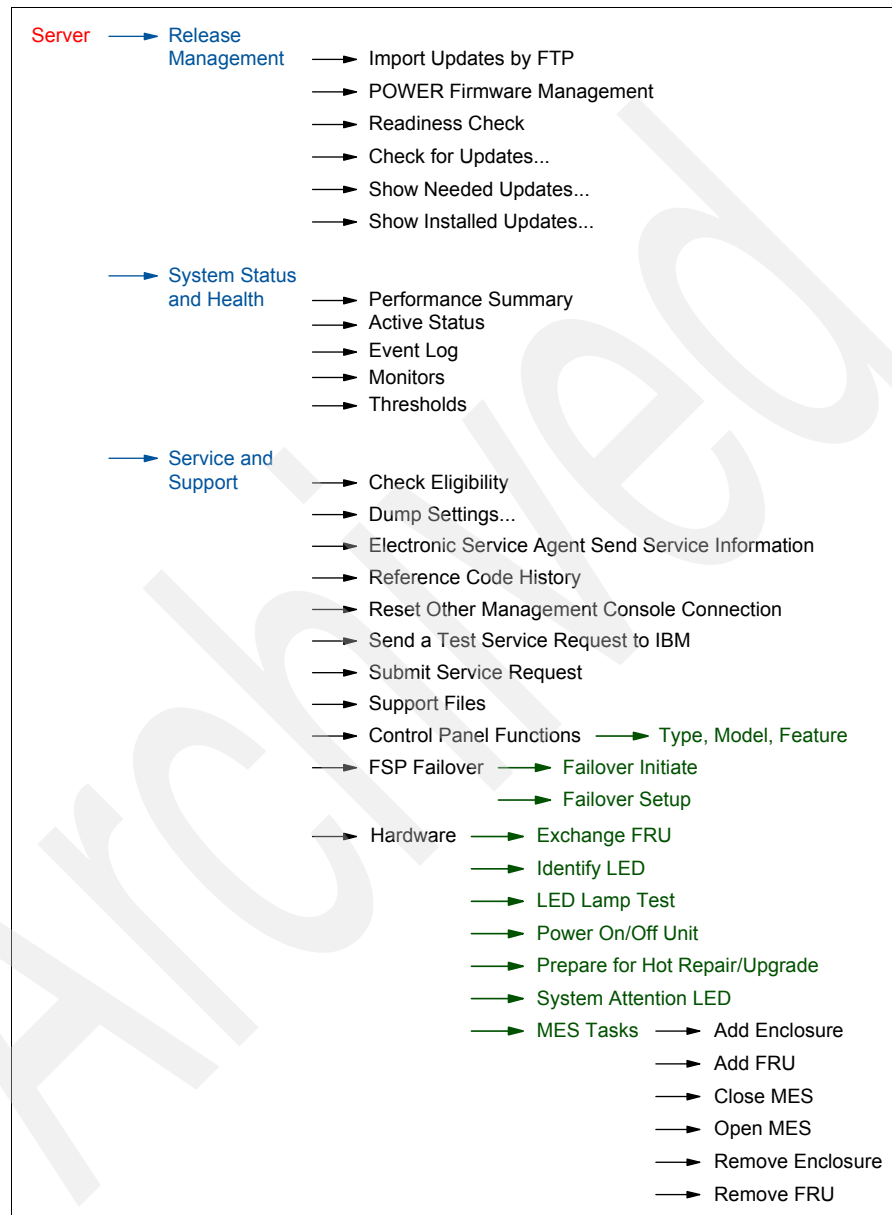


Figure 3-4 Context menu for server management

Figure 3-5 shows a snapshot of the layout of the management tasks available on the context menu of the Virtual Server.

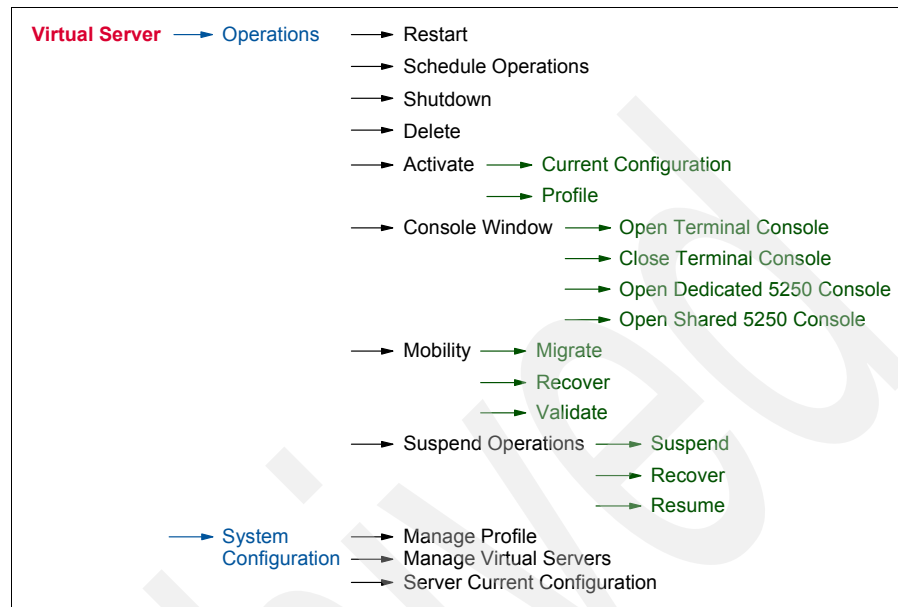


Figure 3-5 Context menu for Virtual Server management

3.2.3 Resource views

SDMC provides a number of ways to view information about your resources and manage them. The views are displayed only from the Navigate Resources page. Here are the different views that are available:

- ▶ Table view
- ▶ Properties view
- ▶ Topology view

Each of the views are explained in following sections.

Table view

The table view displays a list of resources along with their information in a table format (Figure 3-6). The various properties of the resource are displayed in the various columns of the table.

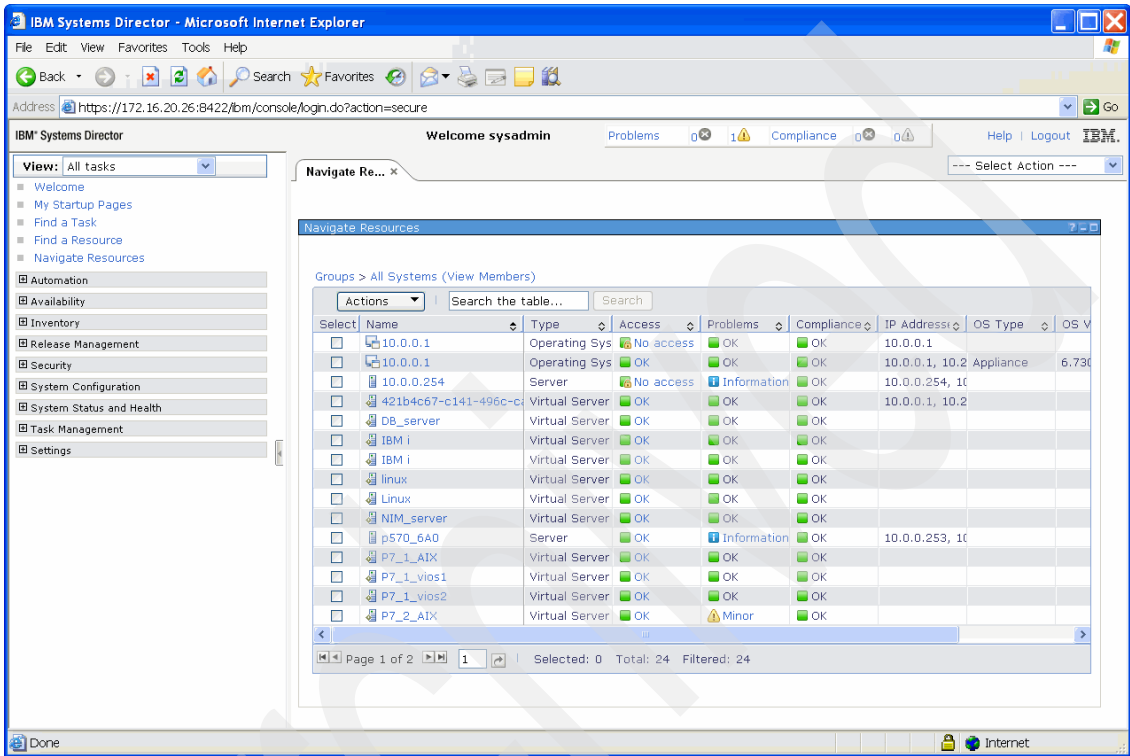


Figure 3-6 Table view

Properties view

The properties view displays a list of properties and other detailed information related to the selected resource. You can access the properties view from any view by selecting a resource and selecting **Action** → **Properties**. The properties view is shown in Figure 3-7.

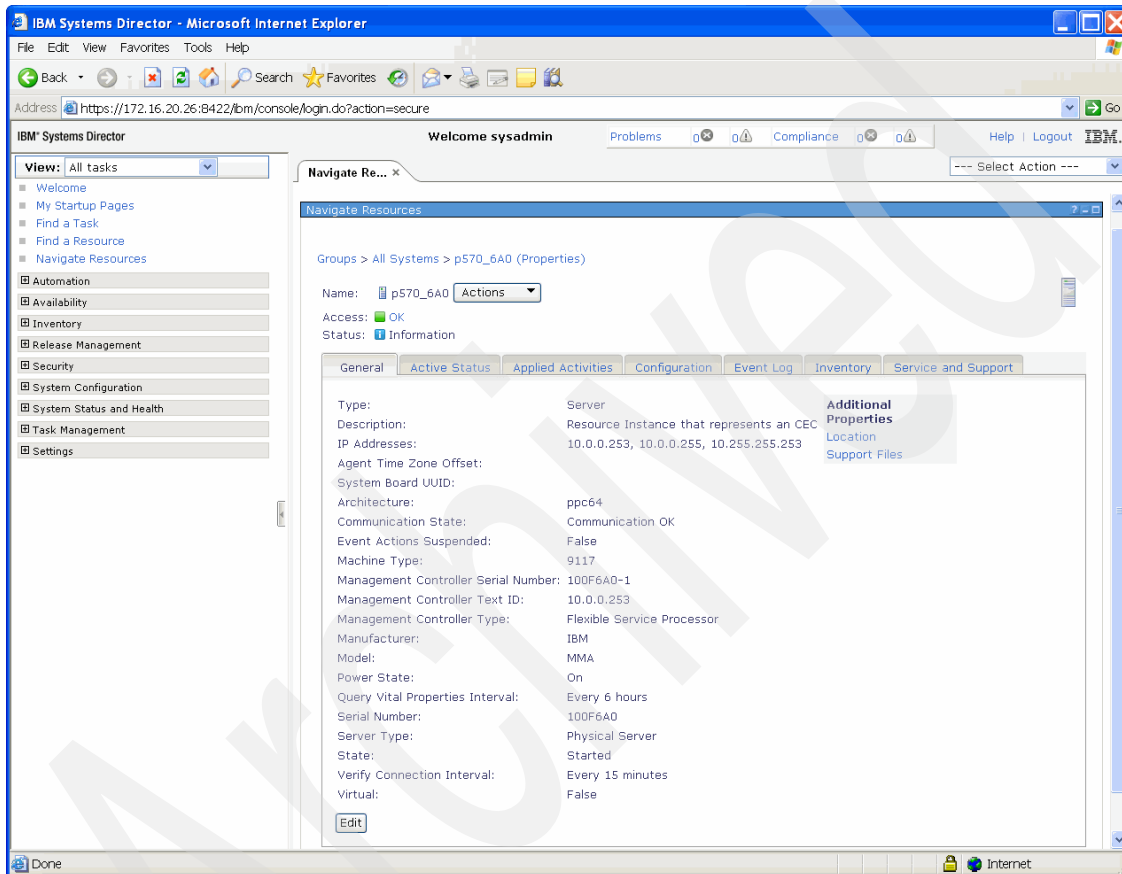


Figure 3-7 Properties view

The properties view only shows the inventory information collected from the managed system or the Virtual Server. For the HMC-like properties related to managing a Power Server, see the Edit Host page for systems and Manage Virtual Server page for Virtual Servers.

Topology view

The topology view displays the relationship among your resources. Select a resource and select **Actions** → **Topology Perspectives** → **Basic**. The Basic selection provides a topology map that shows key resources that are related to the selected resource. The topology map view shows a graphical view of your resources and their relationships. You can drill down and view the relationships among these resources and other resources in your environment. You can also view and edit resource properties. The topology map view is shown in Figure 3-8.

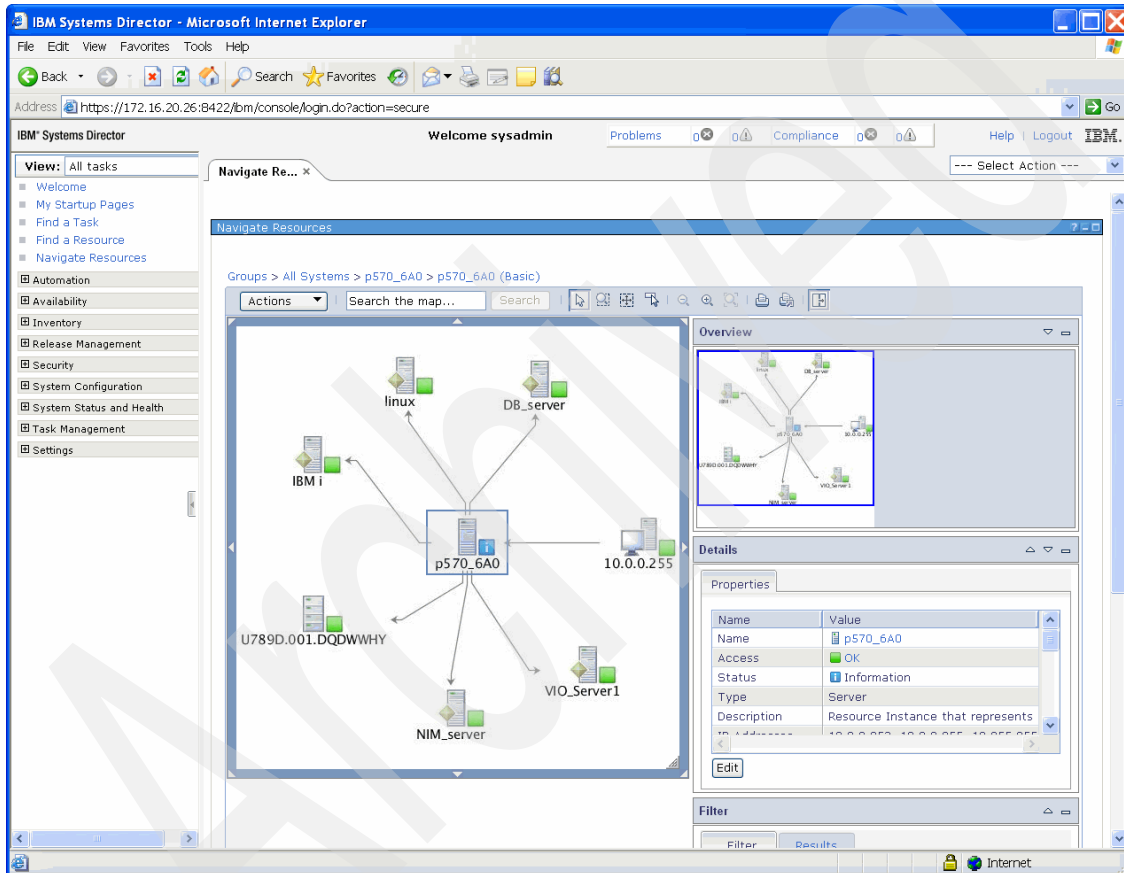


Figure 3-8 Topology Map view

3.3 Command-line interface

The IBM Systems Director provides the systems management command-line interface, referred to as **smcli**, for issuing commands. You can run **smcli** commands locally from SDMC or remotely by accessing the SDMC using a remote access utility, such as secure shell (SSH).

SDMC provides all the commands that were available in HMC. You can run the same command as in HMC, but using the **smcli** prefix. So the HMC command **lssyscfg -r sys** becomes **smcli lssyscfg -r sys**.

Note that the **smcli** is prepended to the HMC command, and you can execute all the HMC commands with the same parameters and values. Note that you do not need to prepend **smcli** when you look up the man page of a command. When looking up the man page of a command that is related to managed Power resources, you should issue the following command:

```
man psm.<command_name>
```

The commands related to console management and user management are discontinued in SDMC. There are some commands that exist both in the HMC and IBM Systems Director, such as **lsled**. If you issue the command with the **smcli** prefix, SDMC executes the command belonging to IBM Systems Director. If you want to execute the same command that existed in HMC, you have to include the bundle name **psm** in the command, as shown below:

```
smcli psm lsled
```

This command executes the **lsled** command as executed in the HMC. For further information, see Chapter 10, “Command-line interface” on page 275.

Making the transition to the IBM Systems Director Management Console

This chapter describes the various ways of how you can transition your managed systems from the Hardware Management Console (HMC) or Integrated Virtualization Manager (IVM) environment to the IBM Systems Director Management Console (SDMC) environment.

4.1 Concepts

Transition is a new feature that is available to transition systems from the HMC or IVM environment to the SDMC environment. This feature helps you transition one or more systems that are currently being managed by HMC or IVM to being managed by SDMC.

SDMC supports the following two types of transition:

- ▶ IVM to SDMC
- ▶ HMC to SDMC

With regards to an HMC transition, you can use either the command-line interface or the graphical user interface to perform an interactive transition or an offline transition. Use interactive transition when your HMC is running and offline transition when your HMC is shutdown. During transition, SDMC discovers the managed systems and you have to request access to each managed system by supplying the password. Transition is complete only after successful authentication to the managed system. The state of the managed system changes to Available and you can start managing your system and its Virtual Servers, which appear automatically.

The SDMC transition process does not remove the managed systems connection from the HMC. The managed systems stay connected to the HMC even after transition. A maximum of two management console connections are allowed per managed system (two HMCs and two SDMCs, or one HMC and one SDMC). Ensure that a connection for the management through the SDMC console is available and not in use during the request access phase of the SDMC transition process.

4.2 IVM to SDMC transition

This section describes how you can transition a managed system from an IVM to an SDMC.

You have to perform the transition process manually for the IVM to SDMC transition. You cannot use the transition wizard to transition managed systems from IVM to SDMC. The managed system has to be in an IVM Managed state. After the transition is complete, you are not able to use the IVM user interface, because the Virtual Management Channel (VMC) is deactivated. The VMC is the device on the Virtual I/O Server that enables a direct hypervisor configuration. This device is activated only when the Virtual I/O Server detects that the environment has to be managed by IVM.

4.2.1 What is transitioned

When you transition managed systems from IVM to SDMC, only the following information is transitioned:

- ▶ Managed system information.
- ▶ Virtual Server information is automatically retrieved from the managed system after a request access to the managed system is successful.

4.2.2 How to transition

Perform the following steps to transition a managed system from IVM to SDMC:

1. Discover the managed system in SDMC using the [System Discovery page](#).
2. Request access to the managed system. The request access task fails and the Operating State of your managed system changes to [Waiting for Input](#) and the Detailed State is [Pending Authentication - Password updates required](#).
3. Update the ASM general and ASM admin passwords for the managed system using the **Update Password** task.

The Access state of the system changes to OK and additional tasks are now available on the context menu for managing the system. The Virtual Servers hosted by the system are retrieved and listed on the [Welcome page](#).

This transition performs the following operations internally:

- ▶ Fetches the Virtual Server configuration information from the hypervisor.
- ▶ Updates the SDMC with the managed system information from the hypervisor.
- ▶ The virtual slots ranging from 2 to 10 are reserved in SDMC. The IVM does not have such restrictions, and it is possible that you were using some virtual slots in the reserved range in the IVM environment. The transition process looks for such virtual slots and dynamically adjusts the virtual slots range to a new available range within the maximum slots value specified.

Note: If the automatic readjustment of reserved virtual slot range is unsuccessful, then you have to shut down and activate the Virtual I/O Server again to use the advanced PowerVM features. The shutdown and reboot are needed only when you want to use the advanced PowerVM features. But the Virtual Servers continue to run normally even without the shutdown and reboot.

- Creates default profiles based on Virtual Server current configuration read from PHYP, as IVM does not support profiles.

4.2.3 Messages

By default, all success and failure messages are listed in the Event Log page. The Event Log page is available under the System Status and Health category in the navigation area. Check the Event Log page for the success or failure of the transition process. When the transition completes successfully, the following message is posted in the Event Log:

The IVM to SDMC transition completed successfully.

The Status Manager displays the Alert and the Resolution messages. Clicking the **Health and Summary** link under the System Status and Health category shows the messages in the Status Manager. An Alert message (error) is displayed first, followed by a Resolution event.

An alert message is displayed in the Status Manager to flag a problem. A Resolution event is received by the Status Manager when the problem is resolved. Thus, the Resolution event removes the corresponding alert that it has resolved from the Status Manager.

Table 4-1 shows the Alert and Resolution events related to the IVM to SDMC transition.

Table 4-1 Status Manager Error/Resolution messages

| Alert | Resolution |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Virtual I/O Server Slot Range Adjustment Failed (Error). | Virtual I/O Server Reactivated & Slot Adjustment Completed Successfully (Resolution). |
| The Virtual I/O Server Slot adjustment did not complete successfully. You have to reactivate the Virtual I/O Server Virtual Server before attempting LPM or AMS operations. | The Virtual I/O Server Slot Adjustment completed successfully. |

4.3 HMC to SDMC transition

This section describes how you can transition a managed system from an HMC environment to an SDMC environment. This section is applicable only when the managed systems are in a public network and SDMC is not the Dynamic Host Configuration Protocol (DHCP) server. If your managed systems are in a private network, refer to 4.4, “Transition in a private network” on page 72.

4.3.1 What is transitioned

The following items are the major items that are transitioned:

- ▶ List of managed systems along with their information, such as MTMS name and IP address.
- ▶ Virtual Server and profile information are not lost during transition and are retrieved from the managed system after transition.

4.3.2 What is not transitioned

The following items are the major items not transitioned:

- ▶ Dump data, system, and error logs stored on the HMC.
- ▶ Custom users and roles created on the HMC.

4.3.3 Interactive transition using graphical user interface

SDMC provides a wizard for interactive transition. Using the wizard, you can connect to a live HMC and stream in the configuration data directly from it.

Perform the following steps to perform an online transition:

1. Launch the transition wizard using the **Common Tasks** menu in the SDMC welcome page (Figure 4-1).

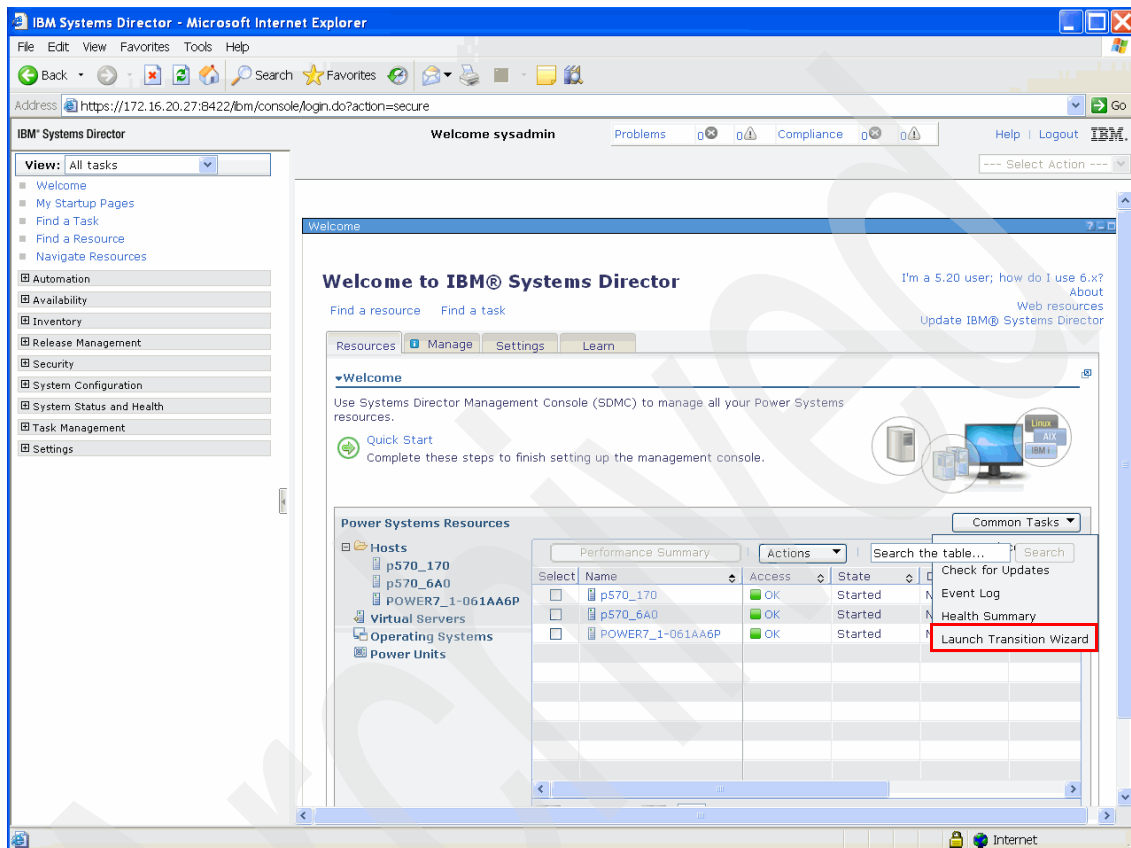


Figure 4-1 Launch Transition wizard

2. Click **Next** on the Welcome page of the transition wizard.
3. Select **Connect to the HMC to interactively transition to SDMC**. Enter the user name, password, and the IP address or host name of the HMC and click **Next**.

4. You should now see a list of managed systems (Figure 4-2) that are available in the HMC that can be transitioned to your SDMC. Select the managed systems that you want to transition and click **Next**.

Note: If the SDMC is already managing some managed systems that are being managed by the HMC currently, those managed systems will not be listed for transition.

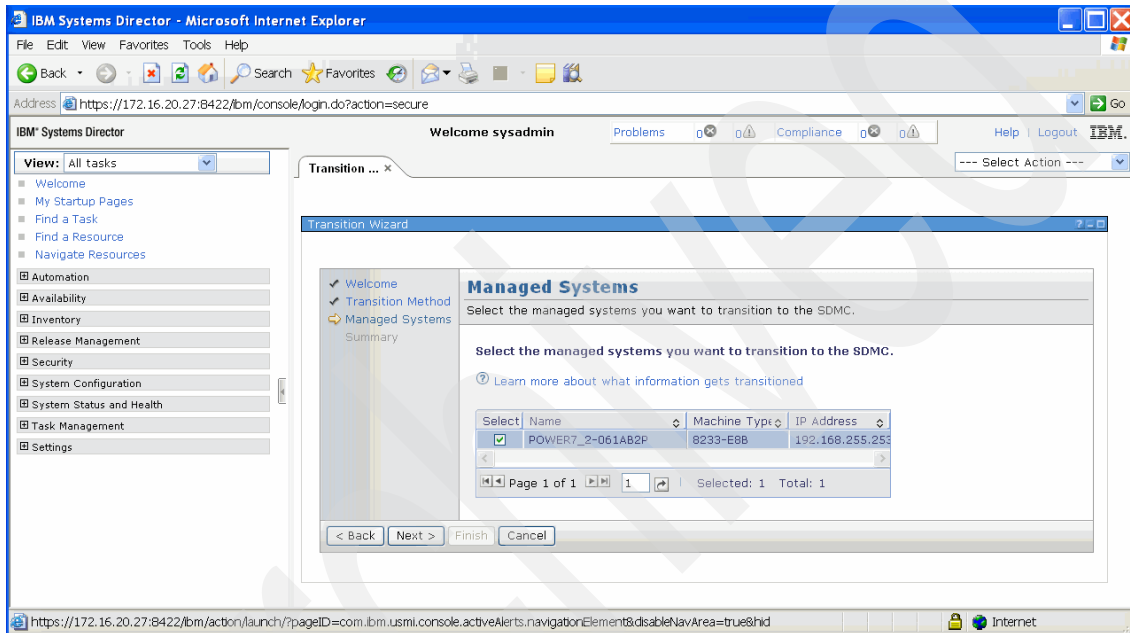


Figure 4-2 Managed systems in the Transition wizard

5. You should now see the summary page of the Transition wizard. It shows you the IP address or the host name of the HMC and the managed systems that you have selected for transition. Click **Finish** to complete the transition.
6. You can see the transitioned managed systems in the Welcome page in the No Access state. Request access to the managed system. The user ID field in the Request Access page will be pre-populated and disabled. You only need to enter the password.

After successful authentication, the Access state of the managed system changes to OK. The tasks for managing the system are now available in the context menu of the system. The Virtual Servers hosted by the managed system are retrieved automatically and can be seen in the Welcome page or the Navigate Resources page.

4.3.4 Interactive transition using the command-line interface

Perform the following steps to perform an online transition using the command-line interface:

1. Execute the **impdata** command using the following options on the SDMC:

```
smcli impdata -h <system_name> -u <user>
```

Where:

system_name The host name or IP address of the remote HMC from which to import configuration data

user The name of the remote HMC

2. Enter the name of the remote HMC user.
3. Enter the password for the name of the remote HMC user when prompted. SDMC identifies the managed systems to transition and discovers them.
4. The transitioned systems are in the No Access state. You can request access to the managed systems using the **accesssys** command.

After successful authentication, you can start managing the system with the tasks available on the context menu of the system, and the Virtual Servers hosted by the managed system are retrieved automatically.

4.3.5 Offline transition using the graphical user interface

Perform the following steps to perform an offline transition using the graphical user interface:

1. Execute the **expdata** command using the following option on the HMC:

```
expdata -f <file>
```

Where *file* is the name of the file where the HMC configuration data is written on the HMC. If the file is not fully qualified, it will be written to the `/dump/expdata` directory on the HMC.

If the file already exists, this command will fail unless the `--force` option is specified. To export the 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 you issue this command.

All serviceable events must be closed before you can execute this command. If there are any open serviceable events at the time of issuing this command, you will get a warning message and you have to close all of them before executing the command again.

Note: The **expdata** command only exports HMC configuration information that is required for transition. The exported data cannot be used as HMC backup data.

2. Launch the transition wizard. Note that the export is run on the HMC, and the wizard is launched on the SDMC. The SDMC imports the data from the HMC export.
3. Click **Next** to go to the Transition Method page in the wizard.
4. Select **Use an exported data file** in the Transition Method page.

5. Browse to and select the exported configuration data file from step 1 (Figure 4-3). You can also select a file that is available on a connected system in the network. Click **Next**.

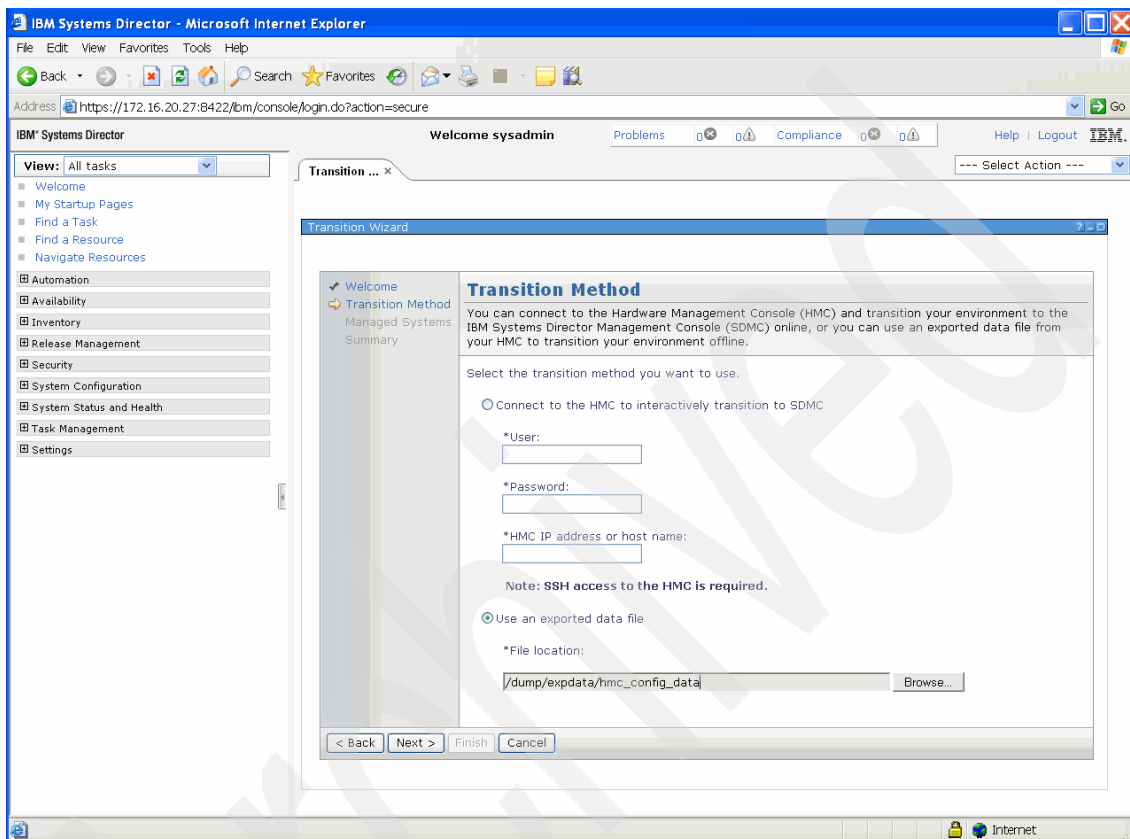


Figure 4-3 Transition method using an exported data file

6. You should now see the summary page of the transition wizard. It shows you the IP address or the host name of the HMC and the managed systems that you have selected for transition. Click **Finish** to complete the transition.
7. You can see the transitioned managed systems in the welcome page in the No Access state. Request access to the managed system. The user ID field in the Request Access page will be pre-populated and disabled. You only need to enter the password.

After successful authentication, you can start managing the system. The Virtual Servers hosted by the managed system are retrieved automatically.

4.3.6 Offline transition using the command-line interface

Perform the following steps to perform an offline transition using the command-line interface:

1. Execute the following **expdata** command on the HMC:

```
expdata -f <file>
```

2. Execute the **impdata** command using the following option in the SDMC:

```
smcli impdata -f file
```

Where *file* is the name of the file containing the HMC configuration data imported from your HMC in step 1.

This command carries out a discovery process of the managed systems that are eligible for transition from your HMC. The managed systems are discovered by the SDMC and will be in the No Access state.

3. Request access to the managed systems using the **accesssys** command:

```
smcli accesssys <managed system name>
```

Enter the user ID and password for the managed system when prompted.

After successful authentication, you can start managing the system. The Virtual Servers hosted by the managed system are retrieved automatically.

The flow chart in Figure 4-4 shows a snapshot of the complete transition process.

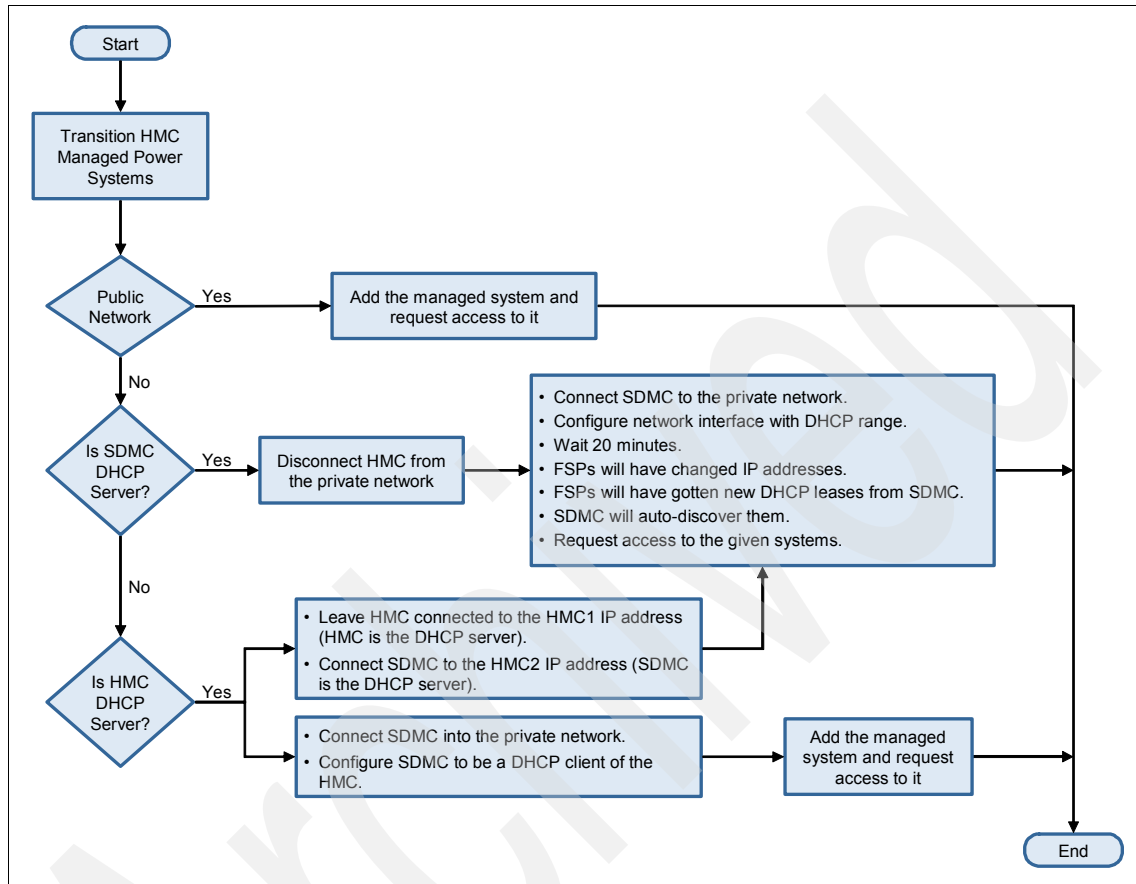


Figure 4-4 Transition workflow

4.4 Transition in a private network

This section describes how to perform that transition of managed systems that are in the private network. In this scenario, either the SDMC or the HMC can be the DHCP server. The steps for transitioning when the SDMC is the DHCP server is different from the steps when the HMC is the DHCP server.

4.4.1 SDMC as the DHCP server

Perform the following steps to perform a transition of managed systems in the private network with the SDMC as the DHCP server:

1. Disconnect the HMC from the private network.
2. Connect the SDMC to the private network.
3. Configure the network interface of the SDMC with the correct DHCP range.

The IP addresses of the managed systems might change after the renewal of the DHCP leases from the SDMC. SDMC then auto-discovers the managed systems.

4. Request access to the managed systems.

After successful authentication, you can start managing the systems using the tasks available on the context menu of the system. The Virtual Servers hosted by the managed system are retrieved automatically.

4.4.2 HMC as the DHCP server

When the existing HMCs are currently the DHCP servers and SDMC will replace one HMC as the DHCP server on the same DHCP range used by the HMC, you have two methods of transitioning systems.

For the first method, perform the following steps to perform a transition of managed systems:

1. Connect the SDMC to the HMC2 port of the managed system. Leave the other HMC connected to the HMC1 port of the managed system.

Now, the HMC is the DHCP server for the managed systems on the network to which the HMC1 port is connected. The SDMC will be the DHCP server for those systems on the network to which the HMC2 port is connected, replacing the other HMC that used to perform this function..

2. Configure the network interface with the same DHCP range as the HMC that used to be attached to the HMC2 of the managed system.

The IP addresses of the managed systems might change after renewal of the DHCP leases from the SDMC. SDMC then auto-discovers the managed systems.

3. Request access to the managed systems.

After successful authentication, you can start managing the systems using the tasks available on the context menu of the system. The Virtual Servers hosted by the managed system are retrieved automatically.

For the second method, perform the following steps to perform a transition of the managed systems:

1. Connect the SDMC to the private network.
2. Configure the SDMC to be a DHCP client of the HMC.
3. Discover the HMC managed system using the IP address or the host name of the managed system.
4. Request access to the managed system.

After successful authentication, you can start managing the systems using the tasks available on the context menu of the system. The Virtual Servers hosted by the managed system are retrieved automatically. Because the resulting environment remains dependent on the HMC to be the DHCP server and hinders a complete transition to an SDMC-only setup, this method should only be used as a temporary solution.



System management

This chapter contains information about how to discover managed systems and perform life cycle management operations on the managed systems. This chapter also contains information about how to perform Capacity on Demand operations using the IBM Systems Director Management Console (SDMC).

5.1 System discovery

Discovery is the process by which IBM Systems Director identifies and establishes connections with the network-level resources that the SDMC can manage. You can use system discovery or advanced system discovery to identify resources within your environment, collect data about the resources, and establish connections with the resource.

SDMC uses the Service Location Protocol (SLP) for discovering resources in the network. SDMC supports the discovery of servers or Flexible Service Processors (FSP), frames or Bulk Power Controllers (BPC), and operating systems. Discovery of operating systems is not necessary if you want to manage only Power resources. SDMC discovery also supports FSP and BPC redundancy.

The discovery in SDMC is a two step process compared to the one step process in HMC. In HMC, you can perform a single step of “Add Managed System” task to discover, where as in SDMC, you have to perform the following two steps:

1. System discovery
2. Request access

After a system has been discovered, it is displayed under Hosts on the Resources tab of the Welcome page. You can manage a system only after discovering it and successfully requesting access to it.

5.1.1 System discovery functions

System discovery is useful when you want to discover a resource for a single IP address or host name, discover resources of the same type for a range of IP addresses, or use a discovery profile. Discovery profiles enable you to customize discoveries, including importing IP addresses and requesting access to discovered resources.

System discovery provides the following functions:

- ▶ Discovery based on a single IP address (IPv4 or IPv6)
- ▶ Discovery based on a range of IP addresses (IPv4 or IPv6)
- ▶ Discovery based on a host name
- ▶ Discovery based on a resource type
- ▶ Scheduling discovery to run on recurring basis

You can launch the System Discovery tool by selecting the **Common Tasks** menu in the Welcome page or by clicking the **System Discovery** link available under Inventory in the navigation area. This should launch the System Discovery page (Figure 5-1).

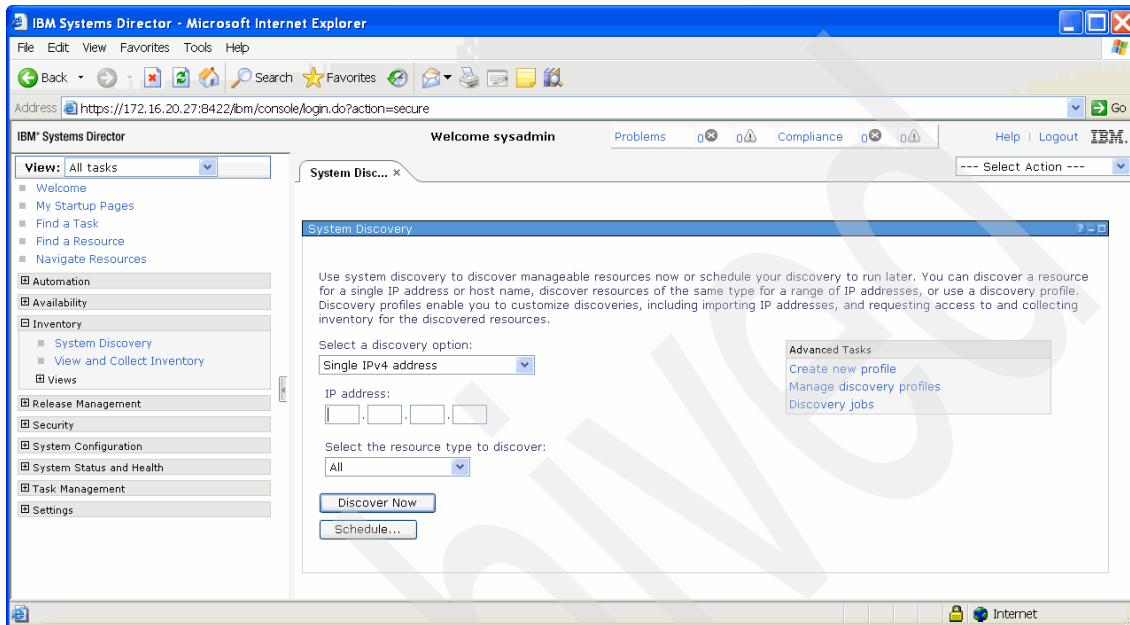


Figure 5-1 System Discovery page

The discovered resources are displayed in the Discovered Manageable Systems table. The Discovered Manageable Systems table displays only the manageable resources that are discovered during the current discovery. System discovery discovers only systems and other types of resources that can be managed by SDMC. The discovered systems are listed on the Resources tab of the Welcome page and the Navigate Resources page with an Access state of Unknown. The Access state of the discovered system is Unknown. The Access changes to No Access after a while and you can perform a Request Access State task on the discovered system. You can also perform a Verify Connection task on the discovered system when it is in the Unknown Access state, which changes the Access state to OK if it was successful.

Verify Connection page

The Verify Connection page validates the connection between SDMC and the system. It also ensures that the state of the system is correctly represented. You can verify the connection to your system at any time. You can launch this task from the context menu by right clicking the system and selecting **Security** → **Verify Connection**. You should see the Verify Connection page (Figure 5-2). This task is launched automatically when you click the **Access** state of the system when the Access state of the system is Unknown.

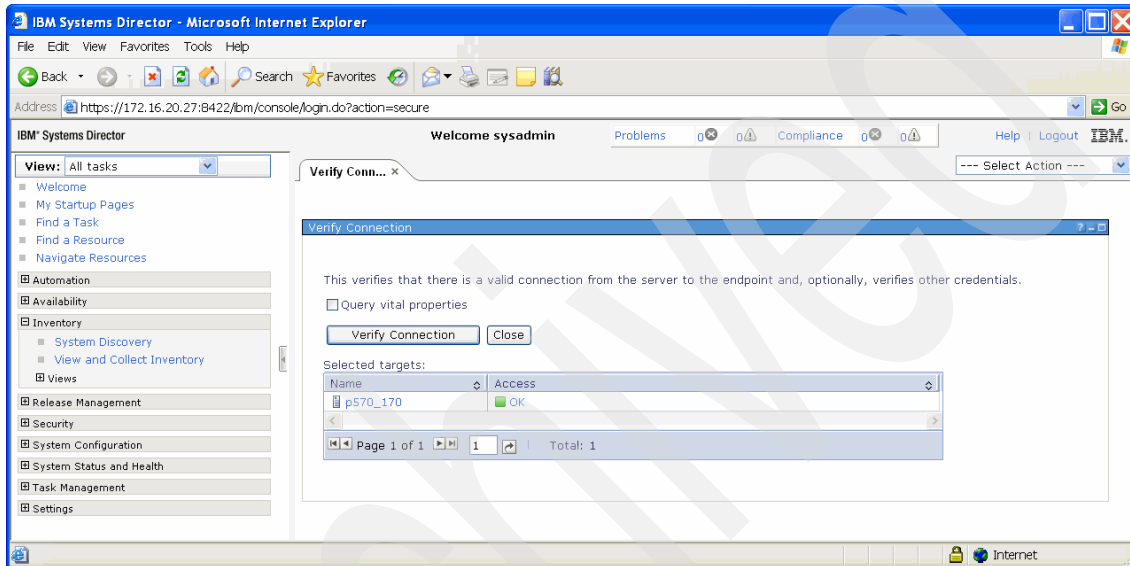


Figure 5-2 Verify Connection page

The Verify Connection task runs in the back ground every 15 minutes. You can change the time interval in the Settings section in the navigation area of the Server Preferences page. The Access state of the discovered systems changes to No Access on successful verification of the connection. You have to request access to the system after verifying the connection to continue with the discovery process.

Request Access page

Use the Request Access page to request access to a system to which your SDMC has not yet authenticated. Ensure that you have the correct authorization to access the system. You can launch this task only when the **Access** state of the system is No Access. This task is launched automatically when you click the **Access** state of the system when the Access state of the system is No Access. You can also launch it from the context menu of the server by right-clicking the system and selecting **Security** → **Request Access**. You should see the Request Access page (Figure 5-3).

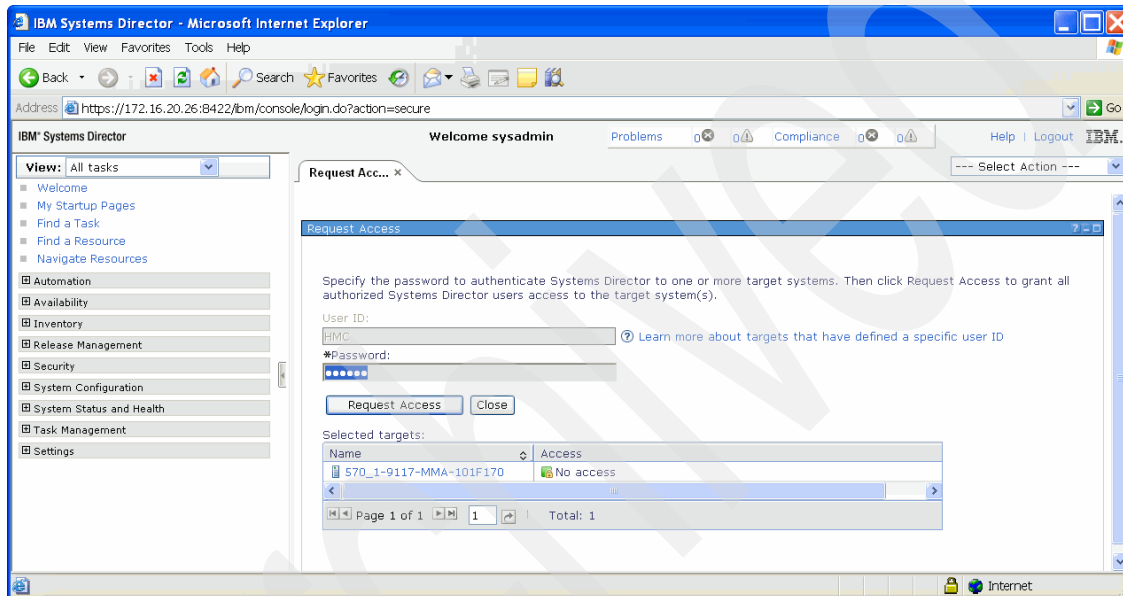


Figure 5-3 Request Access page

The User ID field is pre-filled with the value HMC and is disabled. The password is the same as the Access Password on the Add Managed System panel of the HMC. On successful request access, the Access state of the system changes to OK, which means you have access to the system. After a system is accessed, additional tasks for managing the system are available. The Virtual Servers belonging to the system are populated after a successful request access only.

Configure Access page

Use the Configure Access page to view the status of Remote Service Access Points (RSAP) on a selected resource. RSAP is a logical address that a system uses to route data between a remote device and the appropriate communications support. RSAP credentials incorporate both source and targeted credentials and mappings between the credentials.

The Access states of individual RSAPs are used to evaluate the overall access state for the system. If one or more RSAP is in No Access state, then the overall Access state of the system is Partial Access. The NETC RSAP is used for accessing the FSP. NETC is an IBM proprietary protocol to connect to an FSP from a management console.

The POWER6 system has only NETC RSAPs configured. The POWER7 system has both NETC RSAP and CIM RSAP configured. The Power Unit has only the NETC RSAP configured.

You can configure access to the individual RSAPs from the Configure Access page. If different RSAPs have different credentials, you can use this page to configure each of them. You can also remove RSAPs for a system from this page. You can use the same FSP access password on both the NETC and CIM RSAPs. If any one of the RSAPs was in the No Access state, you just have to request access again.

Revoke Access page

Use this page to remove the connection of SDMC with the system. Use this task when you are not going to manage the system any longer. Right-click the system and select **Security** → **Revoke Access** to perform this task. The state of the system changes back to No Access. You have to request access to the system again if you want to manage the system again.

The Revoke Access task does not remove the system from the SDMC Welcome page or Navigate Resources page. You have to remove the system from SDMC if you no longer want to have it discovered by the SDMC. Right-click the system and select **Remove** to remove the system from SDMC. The Revoke Access task only removes the access to the system and does not remove the managed system from the SDMC inventory. You can access the system again by requesting access to it. However, the Remove task removes the details of the system from the SDMC inventory. The system is no longer listed on the Welcome page or Navigate Resources page. If you want to manage the system again, you have to discover the system again. The Remove task implicitly performs a revoke access task also, and the connection to the FSP is revoked.

5.1.2 Discovery of POWER processor-based blades

A POWER processor-based blade can be managed in very much the same way that a rack-mount Power System is managed from a SDMC, that is, it is managed directly through the service processor (FSP).

By default, the service processor is not available on the network. You must explicitly go into the Advanced Management Module (AMM) and enable this configuration. Make sure you have the latest AMM firmware and blade firmware and select **Blade Tasks** → **Configuration** → **Management Network Configuration**. Enable the FSP on your network.

At this point, you want to remove the blade altogether from SDMC. You are currently managing it through IVM, but you should change that configuration by removing the VIOS OS object, all the Virtual Server objects, and the server object. Remove all objects associated with the blade and chassis from the SDMC. Then, *discover* the FSP directly and request access to it (you need to supply a password here and set the Admin and General passwords. Note that performing this task disables the IVM interface.

To discover a blade server, perform the following steps:

1. Open the System Discovery page.
2. Supply the IP address or the host name of the blade server and choose the resource type as **Server**. The discovery process should discover the blade server as a Server.
3. Request access to the blade server with the correct credentials.

The blade server is now connected to the SDMC and is listed in the Resources tab of the Welcome page. The model type and serial number of the Server indicates that it is a blade server. You can perform all management tasks on the blade server of which it is capable.

Discovery through the Advanced Management Module

Advanced Management Module (AMM) is a management console that provides system management functions and keyboard/video/mouse (KVM) switching for all the blade servers in a BladeCenter® chassis that support KVM. SDMC can also manage the blade servers that are connected to an AMM.

You have to discover the AMM on the System Discovery page and request access to the AMM using the credentials for AMM. The blade servers that are managed by the AMM are now listed as servers in the Navigate Resources page. These managed systems are not listed in the Resources tab of the Welcome page. The SDMC management tasks are not available on these managed systems.

The blade servers discovered directly and the blade servers that are discovered through an AMM can coexist in the SDMC environment. SDMC can manage both these blade servers at the same time.

5.1.3 Using the command-line interface

You can also use the command-line interface to perform the System Discovery and Request Access tasks. To perform system discovery, run the following command:

```
smcli discover -i <IP Address>
```

The IP address of the system can be either an IPv4 or IPv6 address. The command has other options that help discover systems based on host name, a range of IP addresses, or the resource type.

Important: If you issue the **smcli discover** command without any options, SDMC discovers all the resources on the subnet, including resources that you do not want to manage. You might have to manually remove all the resources that you do not want to manage.

To request access to the system, run the following command:

```
smcli accesssys <system name>
```

The system name is the name of the discovered system. You can use the **lssys** command to discover the name of the discovered system.

Enter the user ID and password when you are prompted after executing this command. The Access State of the system changes to OK after successful authentication. You can now start managing the system.

5.1.4 Auto discovery

The auto discovery feature works very similar to how it works on the HMC. If the Dynamic Host Configuration Protocol (DHCP) server is already configured on SDMC, it parses the IP addresses from the lease database and discovers the systems located in the IP addresses automatically.

You still have to request access to the auto-discovered systems with the right credentials to start managing it.

The DHCP service starts after the SDMC installation is completed. You can also manually start or stop the DHCP service by using the following commands:

| | |
|-----------------------------------|--------------------------|
| chnetcfg -c dhcp -s enable | Starts the DHCP service. |
| chnetcfg -c dhcp - disable | Stops the DHCP service. |

If you removed a system from the SDMC previously, SDMC places the IP address of the removed system in a file. Any IP address in this file is not automatically discovered by SDMC. When you run the `smcli mksysconn -o auto` command, it removes all the IP addresses from that file. If you want to rediscover a specific system that you had previously removed, you can do that by executing the following command:

```
smcli rmsysconn -o rediscover {-m managed-system | -e managed-frame}
```

The change in IP addresses are automatically handled in a DHCP and auto discovery setup, but this does not apply to systems that were manually discovered. In that case, you have to remove the system from SDMC and rediscover it to reflect the change in the IP address.

5.1.5 IP address rules

System discovery in SDMC supports both the IPv4 and IPv6 protocols. The IP addresses specified in the System Discovery page must adhere to the following rules:

- ▶ The maximum permitted range of IP addresses is 256.
- ▶ For IP address ranges, the starting IP address must be less than the ending IP address, where only the last piece of the starting and ending IP addresses are unique.
- ▶ All IP addresses in a valid IPv4 address range must occur in the same class C subnet.
- ▶ The IPv6 address compression can be used to replace one or more consecutive instances of "0" in an IP address.
- ▶ The IPv6 loopback address (0:0:0:0:0:0:1 or ::1) is not supported.
- ▶ The prefix length and scope ID for IPv6 addresses are not supported.
- ▶ Use the smallest range possible when discovering with a range of IP addresses.

5.2 System discovery using the HMC

You can also discover and manage systems that are connected to an HMC using SDMC. To accomplish this task, perform the following steps:

1. Open the System Discovery page.
2. Provide the IP address or the host name of the HMC and choose the resource type as **All**. The discovery process should discover the HMC as a Hardware Management Console.
3. Request access to the discovered HMC by entering the correct credentials for the HMC.

The managed systems connected to the HMC are now available in the SDMC. These systems are not displayed in the Resources tab of the Welcome page. You can see these systems listed in the Navigate Resources page. Right-click any of the systems and select **Extended Management** to see all the management tasks that you can perform on these systems.

The context menu is shown in Figure 5-4.

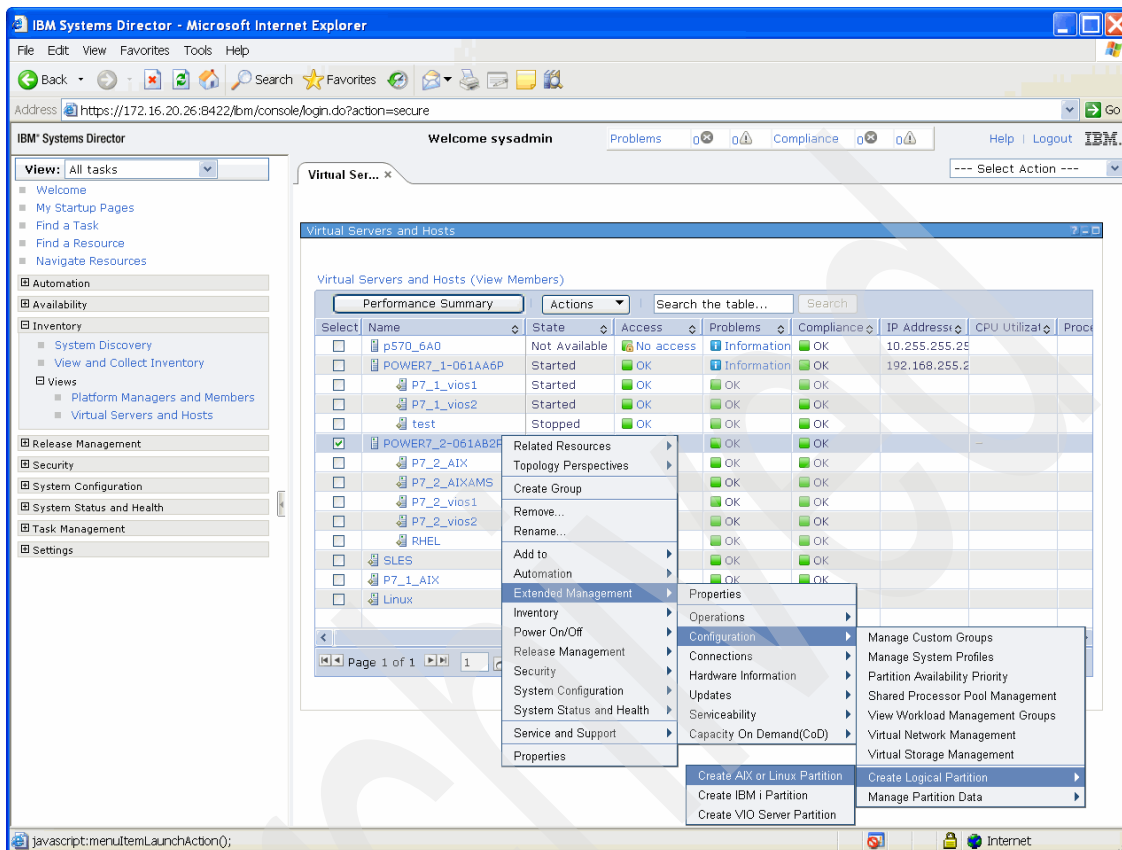


Figure 5-4 Extended management

SDMC does not directly manage the systems connected to the HMC in this setup; they are managed using the HMC user interface. If you want the SDMC to manage the system directly, you must remove the connection of the system from the HMC and discover it from SDMC. The same is true if you want to change an SDMC managed system to being managed by an HMC, that is, you have to remove the connection from the SDMC and add it to the HMC directly.

The PlatformManagerType attribute of the system defines who is managing the system currently. If you want to list the systems on the SDMC that are managed using the HMC, run the following command:

```
smcli lssys -w "PlatformManagerType=HMC"
```

If you want to list the systems on the SDMC that are being directly managed, use the following command:

```
smcli lssys -w "PlatformManagerType=SDMC"
```

5.3 System management operations

After you successfully discover system and request access, you can start managing the system. The managed systems are listed in the Resources tab of the Welcome page. You can also find the managed systems listed in the Navigate Resources page. All the management tasks are available in the context menu of the managed system or in the **Actions** menu. The available tasks available are shown in Figure 3-3 on page 53.

5.3.1 Edit Host page

Servers are referred to as *hosts* in the SDMC environment, as they host Virtual Servers. You can view and edit the properties of a host using the Edit Host page. Right-click a managed system and select **System Configuration** → **Edit Host** to launch the Edit Host page (Figure 5-5 on page 87).

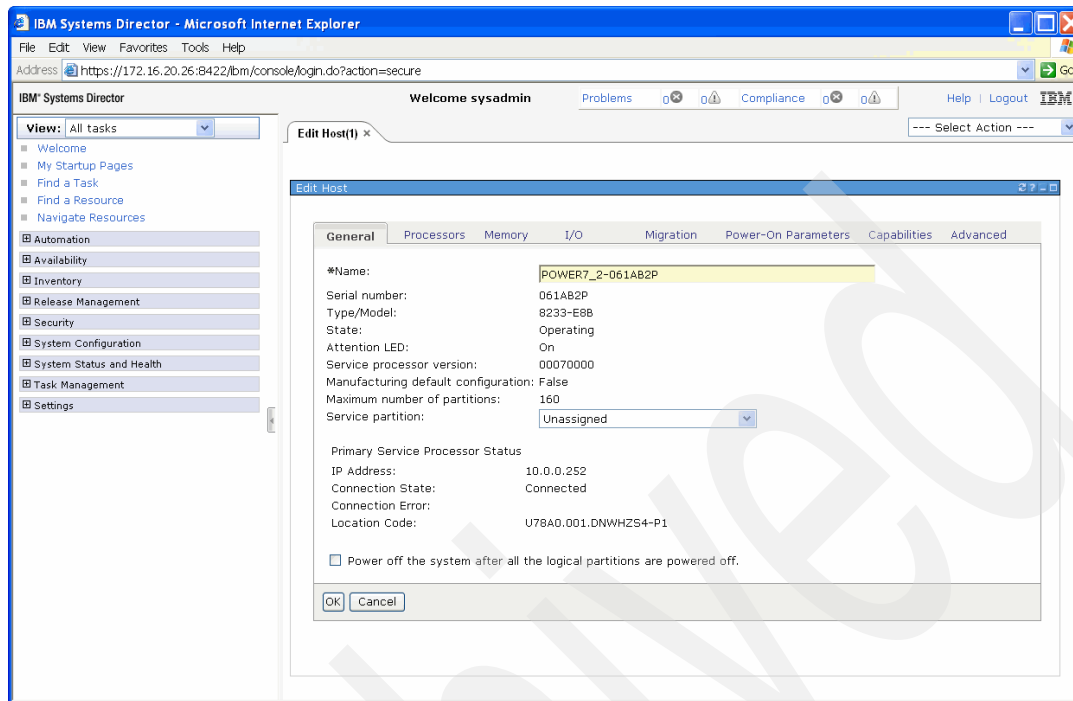


Figure 5-5 Edit Host page

5.3.2 Operations page

The Operations page includes the tasks for server operations. Right-click the server and select **Operations**, where you can see the following items:

- ▶ Power On
- ▶ Power Off
- ▶ Change Password
- ▶ Update Password
- ▶ Power Management
- ▶ Launch Advanced System Management
- ▶ Rebuild Managed System
- ▶ Schedule Operations
- ▶ Utilization Data

These tasks are similar to the ones in HMC except for Schedule Operations. The Schedule Operations task makes use of the scheduling facilities provided by IBM Systems Director. For more information about Schedule Operations, see Chapter 11, “Schedule operations” on page 289.

The tasks are available based on the current operating state of the managed system. The Update Password task is available only when the state of the managed system is Waiting for Input and the detailed state is Pending Authentication - Password Updates Required.

5.3.3 System Configuration page

The System Configuration page includes tasks for configuring your managed system. The tasks include:

- ▶ Create Virtual Server
- ▶ Edit Host
- ▶ Manage System Plans
- ▶ Manage System Profile
- ▶ Workload Management Groups
- ▶ Virtual Server Availability Priority
- ▶ Capacity on Demand
- ▶ Manage Partition Data

The Create Virtual Server task provides a wizard that lets you create a Virtual Server; it is different in SDMC than in HMC. For more information about creating a Virtual Server, see 8.1, “Virtual Server creation” on page 132. Capacity on Demand has also been simplified in SDMC (refer to 5.5, “Capacity on Demand” on page 94 for more information). The other tasks look and function similar to how they looked and functioned in HMC.

5.3.4 Virtual Resources page

The Virtual Resources page includes tasks for configuring virtual resources, such as processors, memory, storage, and networks on your managed system. These virtual resources are used by the Virtual Servers hosted by the managed system. The tasks include:

- ▶ Reserved storage device pool management
- ▶ Shared memory pool management
- ▶ Shared processor pool management
- ▶ Virtual network management
- ▶ Virtual storage management

5.3.5 Hardware page

The Hardware page includes the tasks for configuring your Host Ethernet Adapter (HEA) and Host Channel Adapter (HCA), and for viewing RIO Topology.

5.3.6 Release Management page

The Release Management page includes tasks for updating the firmware level of the managed system. It includes the following tasks:

- ▶ Import Updates by FTP
- ▶ POWER Firmware Management
- ▶ Readiness Check
- ▶ Check for Updates
- ▶ Show Needed Updates
- ▶ Show Installed Updates

These tasks are explained in detail in 7.1.3, “Power Firmware Management tasks” on page 126.

5.3.7 System Status and Health page

This page includes tasks that provide health information about the managed system. The tasks include:

- ▶ Performance Summary
- ▶ Active Status
- ▶ Event Log
- ▶ Monitors
- ▶ Thresholds

These tasks are also available under the System Status and Health section of the navigation area of the web interface.

5.3.8 Service and Support Manager page

The Service and Support Manager page includes the tasks for automatically detecting serviceable hardware problems, collecting supporting data, and transmitting them to IBM. The tasks include:

- ▶ Check Eligibility
- ▶ Dump Settings
- ▶ Electronic Service Agent Send Service Information
- ▶ Reference Code History
- ▶ Reset Other Management Console Connection
- ▶ Send a Test Service Request to IBM
- ▶ Submit Service Request
- ▶ Control Panel Functions
- ▶ FSP Failover
- ▶ Hardware

The tasks are explained in detail in Chapter 14, “Service and support” on page 335.

5.3.9 State mappings between HMC and SDMC

Table 5-1 presents a mapping of the managed system states of HMC to SDMC. The SDMC has three states that are shown in three different columns.

Table 5-1 State mapping

| HMC state | SDMC operating state | SDMC detailed state | SDMC health state |
|----------------------------|----------------------|----------------------------|-------------------|
| Operating | Started | N/A | OK |
| Standby | Standby | N/A | OK |
| Power Off | Stopped | N/A | OK |
| Service Processor Failover | Started | Service Processor Failover | Degraded/Warning |
| Power Off In Progress | Stopping | N/A | OK |
| Initializing | Starting | N/A | OK |
| No Connection | Not Available | Unknown | Unknown |
| Pending Authentication | Waiting For Input | Password Updates Required | Degraded/Warning |
| Failed Authentication | Not Available | Unknown | Unknown |
| Error | Error | Unknown | Critical Failure |
| Error - Terminated | Error | Terminated | Critical Failure |
| Error - Dump In Progress | Error | Dump In Progress | Critical Failure |
| Recovery | Error | Recovery | Critical Failure |
| Incomplete | Error | Incomplete | Critical Failure |
| Version Mismatch | Error | Version Mismatch | Major Failure |

5.4 Hierarchical management

Hierarchical management is a feature available in IBM Systems Director that enables you to configure one IBM Systems Director to be a control point over other IBM Systems Directors. Hierarchical management enables an IBM Systems Director to act as a *global server* that can discover and manage one or more IBM Systems Director, referred to as *domain servers*. The global server also manages the data and status for the resources under each domain server by aggregating the management data from each domain server. The global server can be used for cross-domain and cross-appliance administration in large data centers. In hierarchical management, systems managed by the domain servers are referred to as *remote managed systems*. SDMC can be used both as a global server or a domain server in a hierarchical management setup.

Note: In production environments, use the SDMC as a local or domain server, and use IBM Systems Director as a global server.

Hierarchical management provides greater scalability through aggregation. A global server can effectively help manage IBM Systems Director servers and act as a centralized data center level aggregation point. Hierarchical management provides a single complete data center view. When the data center uses multiple systems management appliances, hierarchical management can be used for a single point of control over all appliances. Hierarchical management is also similar to the environment where the SDMC manages the systems under a HMC after discovering the HMC. At the time of writing, Advanced Managers of IBM Systems Director, such as Active Energy Manager or VMControl, are not supported in a hierarchical management setup.

5.4.1 Enabling hierarchical management

To enable hierarchical management on the SDMC web interface that you want to act as the global server, perform the following steps:

1. Select **Settings** → **Server Preferences** in the SDMC navigation area. The Server Preferences page opens (Figure 5-6).

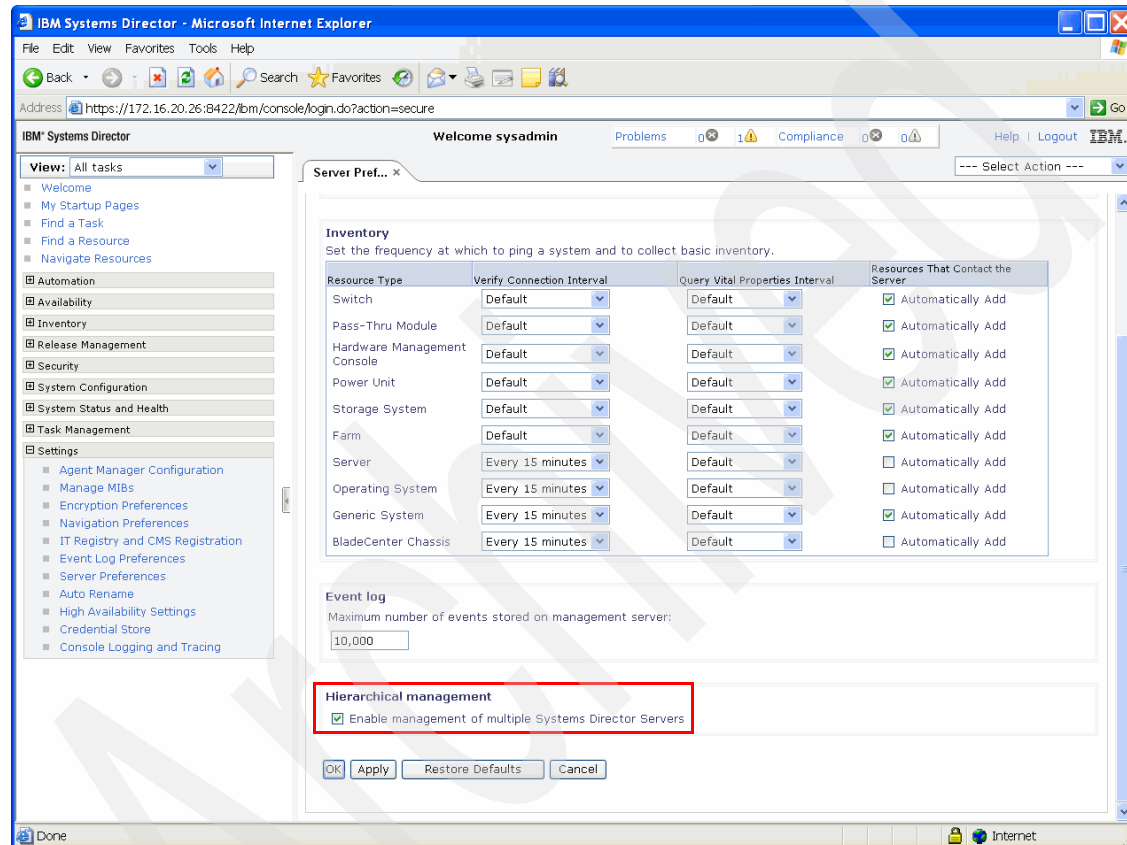


Figure 5-6 Server Preferences page

2. On the Server Preferences page, check the **Enable management of multiple Systems Director Server** check box and click **OK**.

From the command-line interface, enter `smcli hms/confighms -r` to enable hierarchical management. To verify whether its already enabled or not, issue `smcli hmc/confighms -s` on the command-line interface.

3. Discover the domain server (another SDMC that is connected to managed systems) from the System Discovery page. The domain server is discovered as the Operating System type.
4. Request access to the discovered domain server by right-clicking the server and selecting **Security** → **Request Management Access**.

Note: If you see Request Access instead of Request Management Access, the domain server has not been discovered using the Representational State Transfer (REST) protocol. You need to rediscover the domain server.

5. Enter the credentials for the domain server and click **Request Access**.

The remote managed systems of the domain server are now listed on the Navigate Resources page.

5.4.2 Using hierarchical management

After the hierarchical management is set up, you can view and run tasks on the the remote managed resources from the global server. To view and run tasks on a remote managed system, right-click the remote managed system in the **Navigate Resources** page and select a task to run. The global server opens a new browser page and starts the selected task on the domain server. A new browser page opens for each task that you run.

5.4.3 Hierarchical management security

Access to systems managed by the domain servers is controlled by a one-to-one (1:1) user mapping between the global server and the domain server. A 1:1 mapping is a mapping that is created for each user on the global server to a user on the domain server. Each user who accesses the global server will only be able to manage the remote managed systems that the user is authorized to manage on each domain server. Users on the global server do not have complete access to all remote managed systems across all domain servers.

When a user unlocks a domain server by entering the correct credentials, a 1:1 mapping is automatically created for that particular user. This mapping is used for further interactions of that user with the domain server. The user can change the mapped credentials (user ID and password) for the targeted domain server at any time through the Configure Single Sign On UI. Other users who log on the global server to manage remote managed systems from a domain server should use the Configure Single Sign On UI to create their own 1:1 mappings to access that domain server.

5.5 Capacity on Demand

Capacity on Demand (CoD) offerings allow you to dynamically activate one or more resources on your server as your business peaks dictate. You can activate inactive processors or memory units that are already installed on your server on a temporary or permanent basis.

This section also includes information about how to activate Advanced Functions using SDMC.

5.5.1 Launching the CoD task

You can launch the CoD task only on managed systems capable of performing CoD operations. You can check the capabilities of the server by clicking the **Capabilities** tab of the Edit Host page of the server. The name of the capability to perform CoD operations is called CoD Capable.

Right-click the managed system and select **System Configuration** → **Capacity on Demand (CoD)** to launch the CoD page. The CoD page opens (Figure 5-7). You can perform all CoD operations from this page.

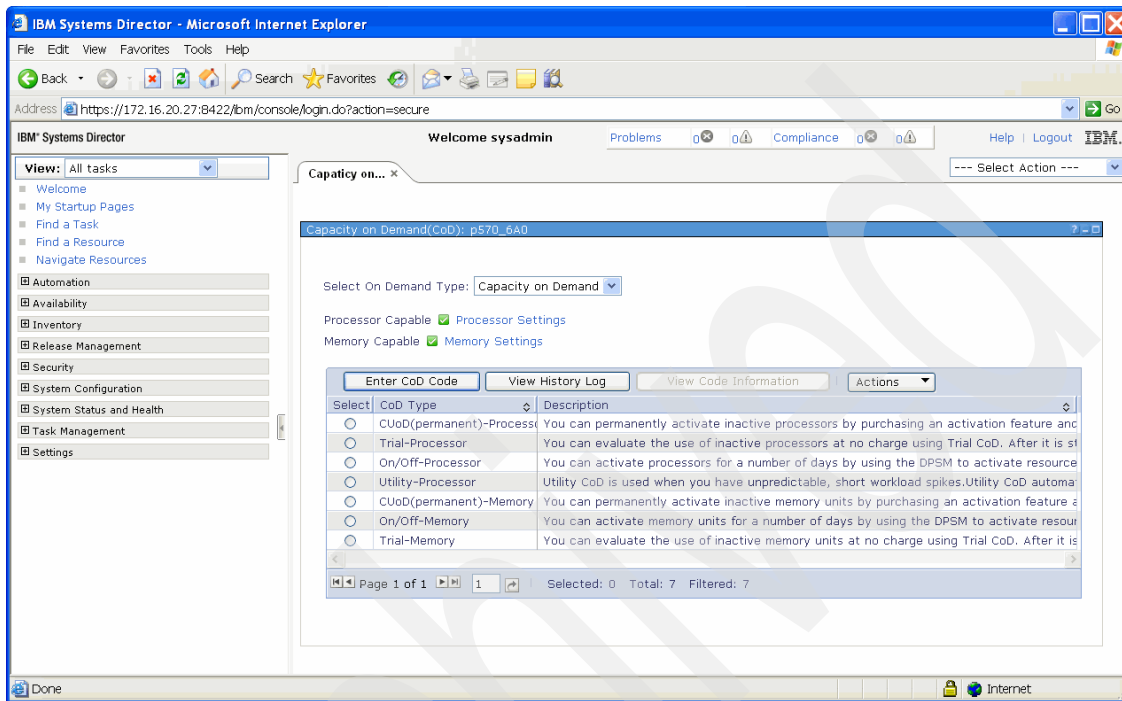


Figure 5-7 CoD page

The On Demand Type menu has two options: Capacity on Demand and Advanced Functions.

5.5.2 Capacity on Demand

Select **Capacity on Demand** from the **Select On Demand Type** menu if you want to activate or deactivate CoD processors and memory on your managed system. The following CoD types are available:

- ▶ CUoD (permanent)-Processor
- ▶ Trial-Processor
- ▶ On/Off-Processor
- ▶ Utility-Processor
- ▶ CUoD (permanent)-Memory
- ▶ On/Off-Memory
- ▶ Trial-Memory

Processor Settings and Memory Settings are hyperlinks and clicking any of them takes you to the CoD processor settings and CoD memory settings page, respectively. These hyperlinks are enabled only if the server is CoD Processor Capable and CoD Memory Capable, respectively.

The Enter CoD Code, View History Log, and View Code Information tasks are global tasks and are available at top of the table. You can launch the Enter CoD Code and View History Log tasks without selecting any CoD type. You have to select a CoD type before launching the View Code Information task, which provides the code information for the selected CoD type. The Actions menu provides the list of tasks that you can perform on the various CoD types. The list of tasks vary depending on the selected CoD type.

5.5.3 Advanced Functions

Select **Advanced Functions** from the **Select On Demand Type** menu if you want to activate advanced functions on your managed system. The available types are:

- ▶ PowerVM
- ▶ Enterprise Enablement
- ▶ Active Memory Expansion
- ▶ Trial Active Memory Expansion
- ▶ Trial Live Partition Mobility
- ▶ WWPN Renewal
- ▶ LPAR Expansion > 128-core

Click the **Enter Activation Code** button to enter the activation code that you obtained from IBM to activate any of the advanced functions.

Note: The Enter CoD Code button, when you select the **Capacity on Demand** option from the Select On Demand Type menu, is different from the Enter Activation Code button when you select the **Advanced Functions** option from the Select On Demand Type menu. The former refers to activation of CoD processors and memory and the latter refers to the activation of advanced functions.

The PowerVM type includes PowerVM Express Edition, PowerVM Standard Edition, and PowerVM Enterprise Edition.

5.5.4 CoD operations

You can perform all CoD related operations from the CoD page. These operations are exactly the same as they were on the HMC. The operations include:

- ▶ Enter CoD Code
- ▶ View Code Information
- ▶ View History Log
- ▶ View Capacity Settings
- ▶ Stop Trial
- ▶ View Shared Processor Utilization
- ▶ Manage

Archived

Power Unit management

This chapter describes how the IBM Systems Director Management Console (SDMC) handles Power Units, formerly called frames or Bulk Power Assemblies (BPAs). A Power Unit is a power assembly for processor, memory, flexible service processor (FSP), and I/O enclosures.

6.1 Power Unit management

When a host is discovered, so are the Power Units. The Power Units are listed in the Resources tab of the Welcome page under the Power Units menu (Figure 6-1). You can also find the Power Units listed in the Navigate Resources page. All the management tasks are available in the context menu of the Power Unit or in the Actions menu.

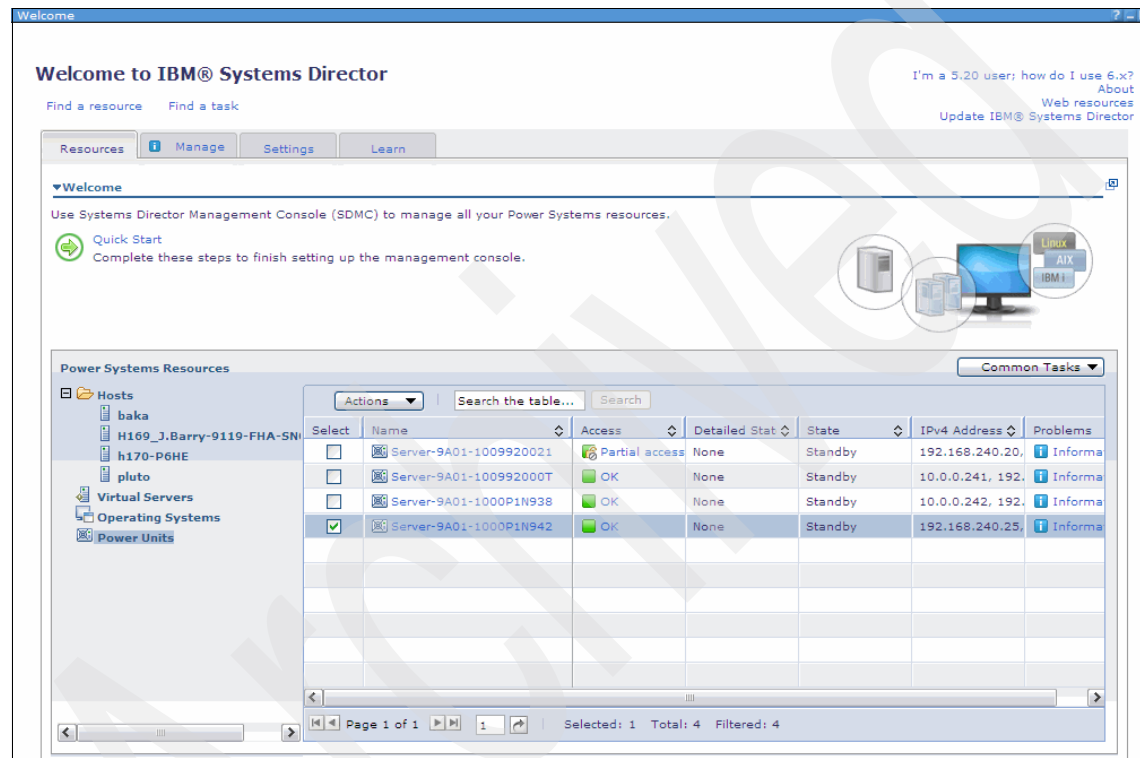


Figure 6-1 Available Power Units

6.1.1 Edit Power Unit page

You can view and edit the properties of a Power Unit using the Edit Power Unit page. Right-click a Power Unit and select **Edit Power Unit** to launch the Edit Power Unit page (Figure 6-2).

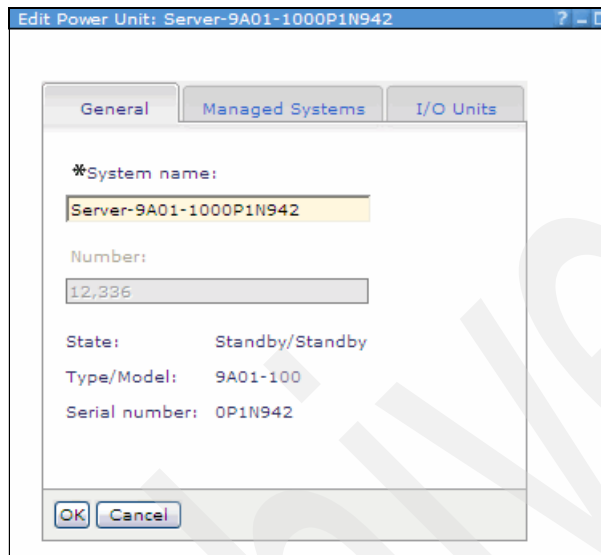


Figure 6-2 Edit Power Unit page

The only change you can make to the Power Unit from this page is to give it a new system name.

6.1.2 Bulk Power Assembly (BPA) Status page

You can view the state of the connection from the SDMC to side A or side B of the Power Unit by right-clicking a Power Unit and selecting **Connections** → **Bulk Power Assembly(BPA) Status**. The Bulk Power Assembly(BPA) Status page opens (Figure 6-3).

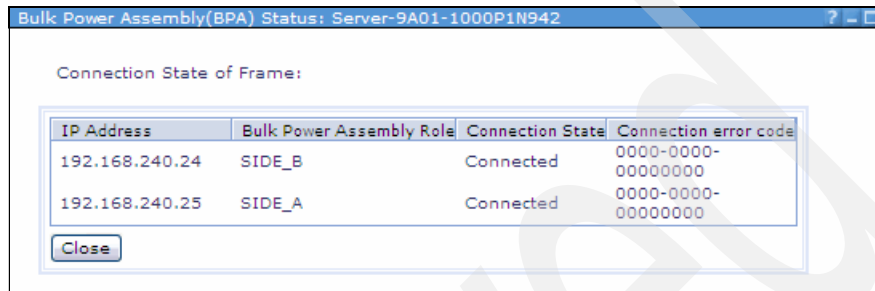


Figure 6-3 Bulk Power Assembly (BPA) Status page

The SDMC operates normally with a Connected connection state to either side A or side B. However, for code update operations and some concurrent maintenance operations, the SDMC needs Connected state connections to both sides.

6.1.3 Change Password page

You can change the password for a Power Unit by using the Change Password page. Right-click a Power Unit and select **Operations** → **Change Password** to launch the Change Password page (Figure 6-4).

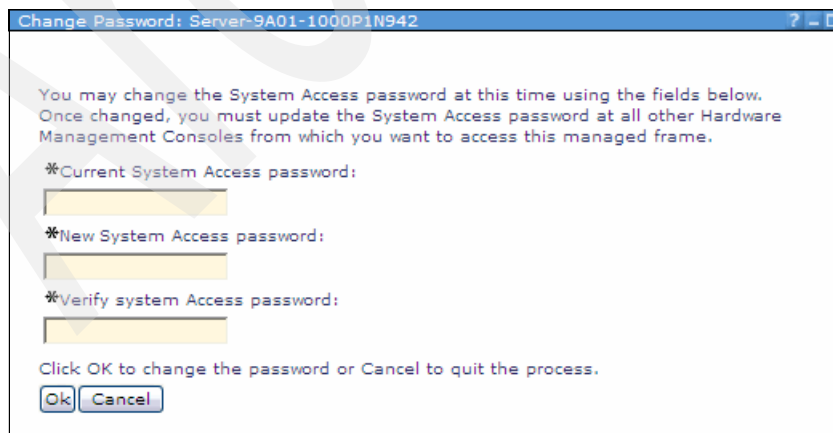


Figure 6-4 Change Password page

You have to enter the current password, then a new password, and verify it by entering it again.

If you change the password, you have to update the password on any other SDMCs from which you want to access this Power Unit.

6.1.4 Initialize Frame page

You can initialize a Power Unit by right-clicking a Power Unit and selecting **Operations** → **Initialize Frame**. The Initialize Frame page opens (Figure 6-5).

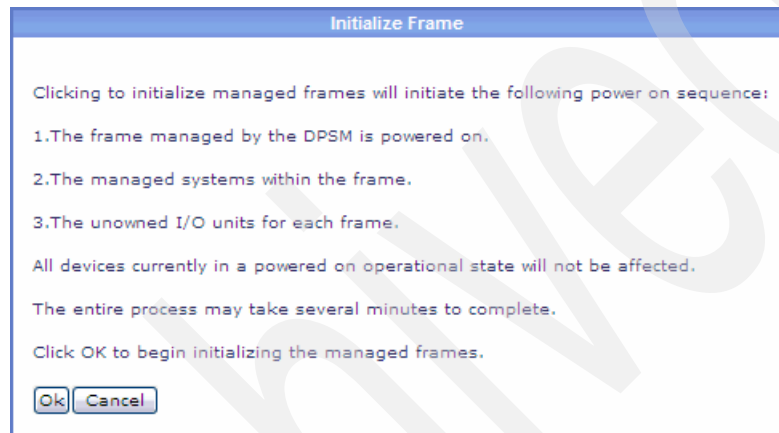


Figure 6-5 Initialize Frame page

If you select **OK**, the frame will be powered on, but only if it is not initialized. All devices that are currently powered on and are in an operational state will not be affected.

When you initialize a managed frame, all of the systems that are contained within a frame managed by the SDMC are powered on. As each individual frame is powered on, the I/O units that are contained within the frame are powered on, then the managed systems that are contained within the frame are powered on as well. When all 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 can take several minutes to complete.

6.1.5 Launch Advanced System Management page

You can open the Advanced System Management Interface (ASMI) page for a Power Unit by right-clicking the Power Unit and selecting **Operations** → **Launch Advanced System Management (ASMI)**. For further instructions, refer to Chapter 13, “Advanced System Management Interface” on page 325.

6.1.6 Power Off Unowned IO Units page

An unowned Power Unit can be powered off by right clicking the Power Unit and selecting **Operations** → **Power Off Unowned IO Units**. The Power Off Unowned IO Units page opens (Figure 6-6) and prompts you to continue. If you click **OK**, then the unowned Power Units will be powered off.

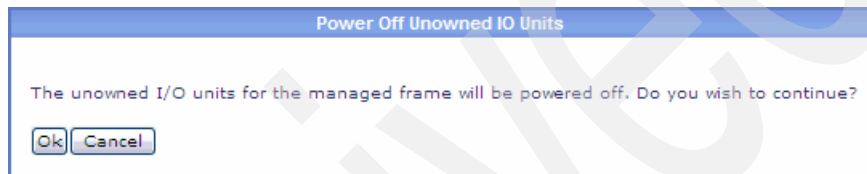


Figure 6-6 Power Off Unowned IO Units page

6.1.7 Rebuild page

You can rebuild the SDMC internal representation of a Power Unit by right clicking the Power Unit and selecting **Operations** → **Rebuild**. The Rebuild page opens (Figure 6-7) and prompts you to continue. If you click **OK**, then the Power Unit will be rebuilt, which can take several minutes, during which no other task can be performed.

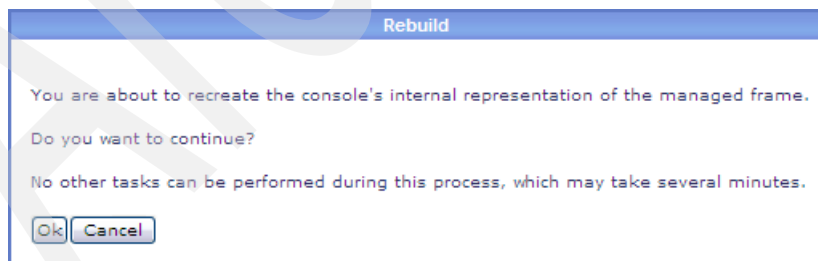


Figure 6-7 Rebuild of a Power Unit

Rebuilding, or recreating, the managed frame acts much like a refresh of the frame information. Rebuilding a frame is useful when the systems state indicator of a Power Unit is shown as Incomplete, which means that the SDMC cannot gather complete resource information from the host within the Power Unit.

Archived

Archived

Firmware updates

This chapter cover installing and managing firmware on Power Systems from the IBM Systems Director Management Console (SDMC). Although Power Systems are used for the examples in this chapter, the installation and update process is much the same when it is used to update other managed target systems, including the SDMC appliance itself (see 9.5, “SDMC appliance update” on page 271).

7.1 Update Manager

The Update Manager is the component of SDMC used to perform update installation and maintenance operations on the SDMC managed system environment. This includes the SDMC appliance itself and managed Power Systems. These operations can be accessed from the Update Manager page, which is linked from the Manage tab of the Welcome page of the SDMC GUI (Figure 7-1). Alternatively, individual update tasks can also be initiated by clicking the **Action** menu on the Resources page.

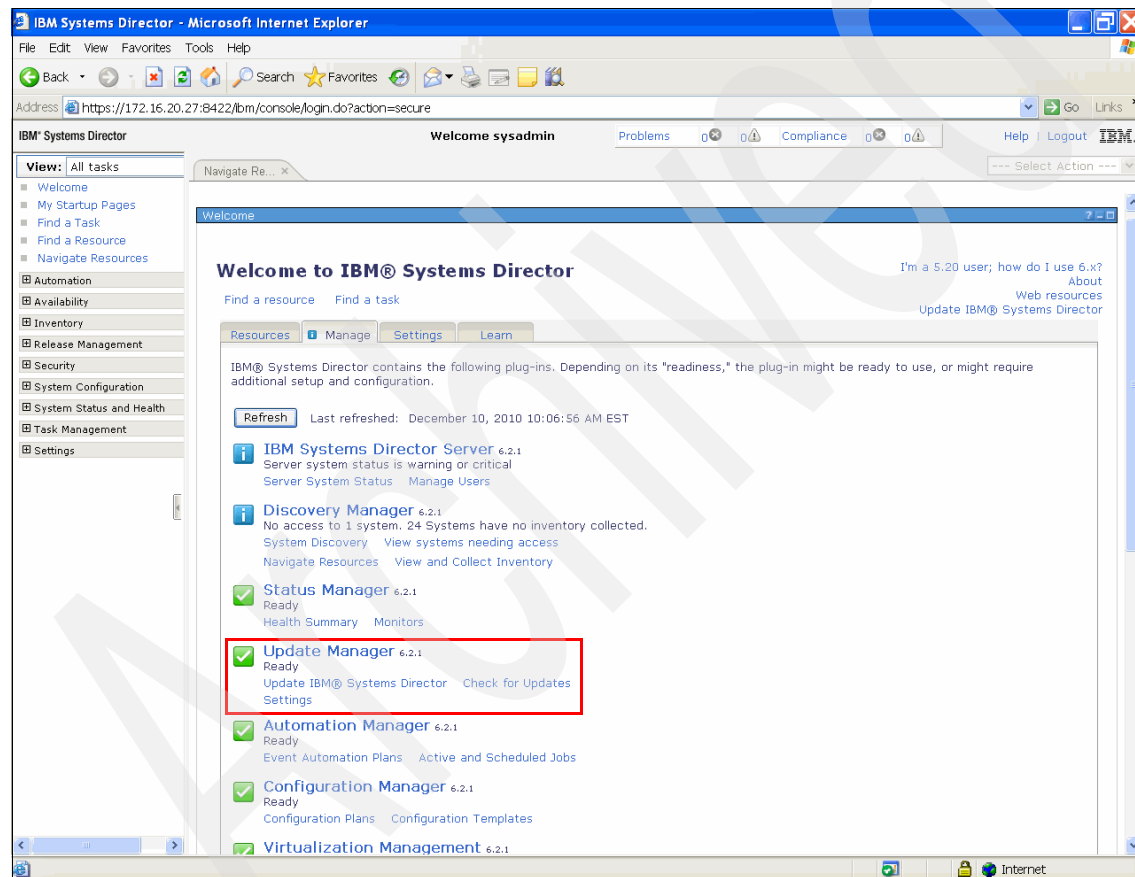


Figure 7-1 Accessing the Update Manager page

All of the available update operations are shown in the Update Manager page (Figure 7-2 on page 109). An in-depth guide for configuring and customizing the Update Manager and all of the available update operations can be found in

Chapter 10, “Update Manager”, in *Implementing IBM Systems Director 6.1*, SG24-7694.

In this chapter, we focus on only the basic steps needed for updating and managing the Power Systems firmware and the SDMC appliance itself. However, the steps for installing and managing updates for other selected managed targets (other types of hardware, operating systems, and so on) by using the GUI are actually very similar, with only some minor differences and considerations.

From the Resources tab on the Welcome page on the SDMC GUI, perform the following steps to perform a readiness check in preparation for an update operation to a managed system:

1. Select system target(s) and select **Release Management** → **Readiness Check** from the Action menu (Figure 7-2).

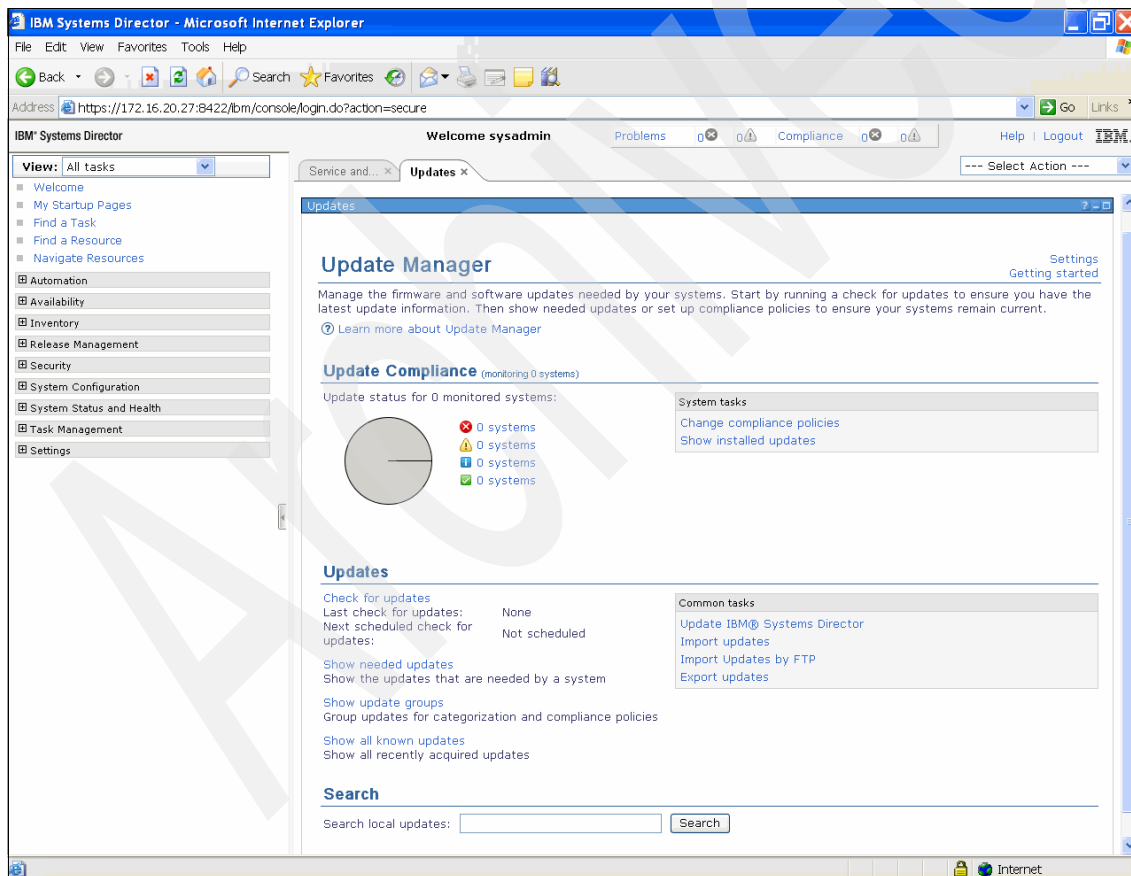


Figure 7-2 Update Manager page

7.1.1 Readiness Check page

Before performing any of the installation or management operations on a system, the user should perform a Readiness Check from the SDMC.

The Readiness Check page is used to detect whether the system is in a good state before a code update operation is performed. This check alleviates the trouble of starting an installation only for it to fail during the process because of an error that could have been detected before the process started. The types of issues detected are:

- ▶ There are connectivity issues.
- ▶ The system is in the non-operational state.
- ▶ There are open serviceable events.

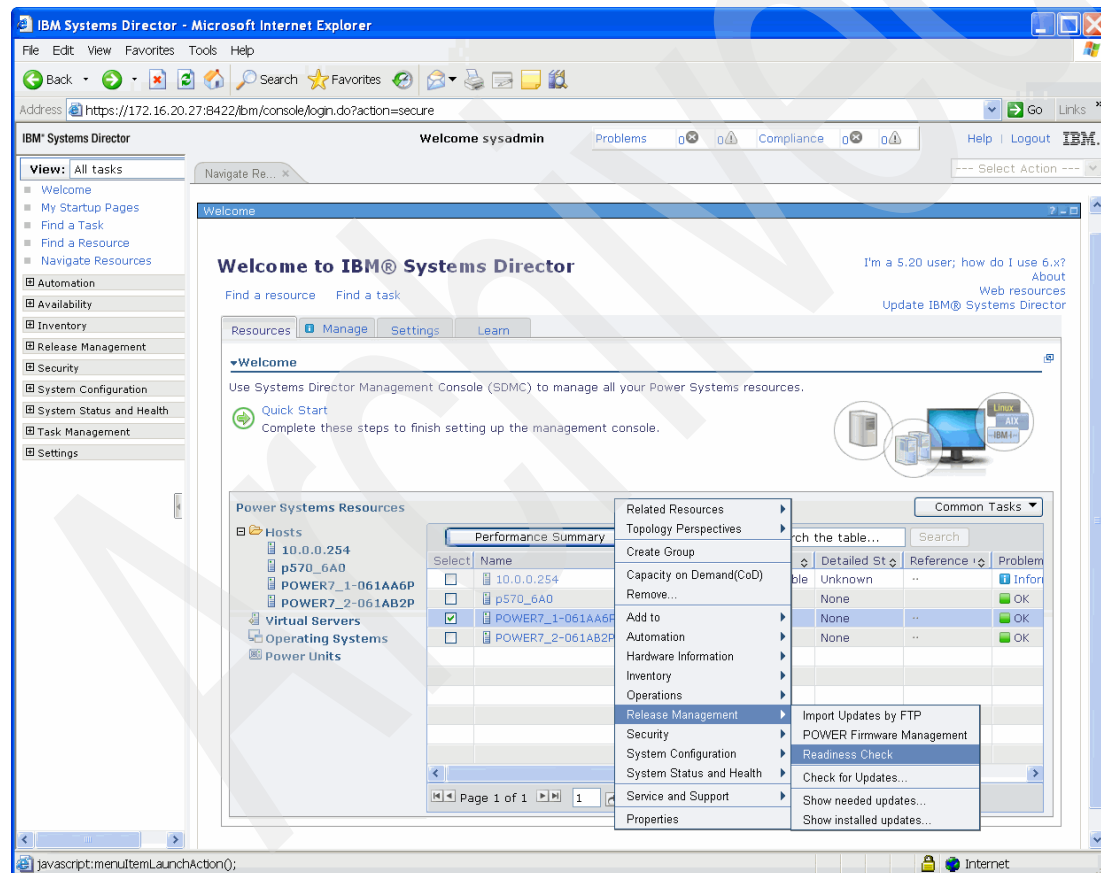


Figure 7-3 Readiness Check page

Click the **Gather Target Information** button on the Readiness Check page to run the Readiness Check on the target systems (Figure 7-4).

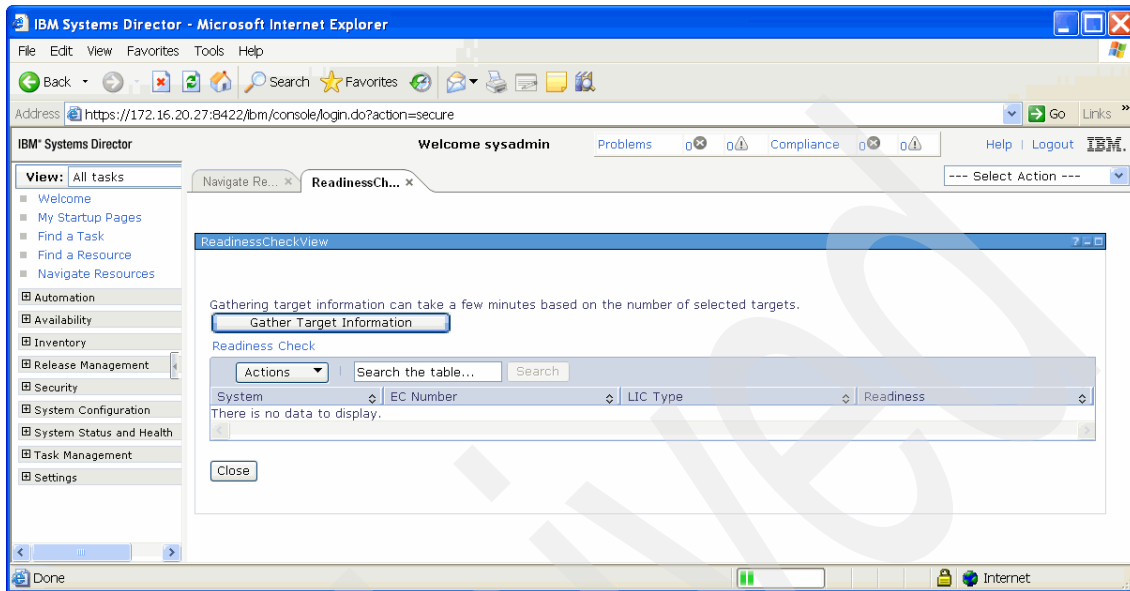


Figure 7-4 Gather Target page

If the selected system pass the Readiness Check, the Readiness column shows as Passed, and the system has been validated for an update install operation (Figure 7-5). If there is a failure, the reason is displayed and the Readiness column will contain a link to the Problems tab.

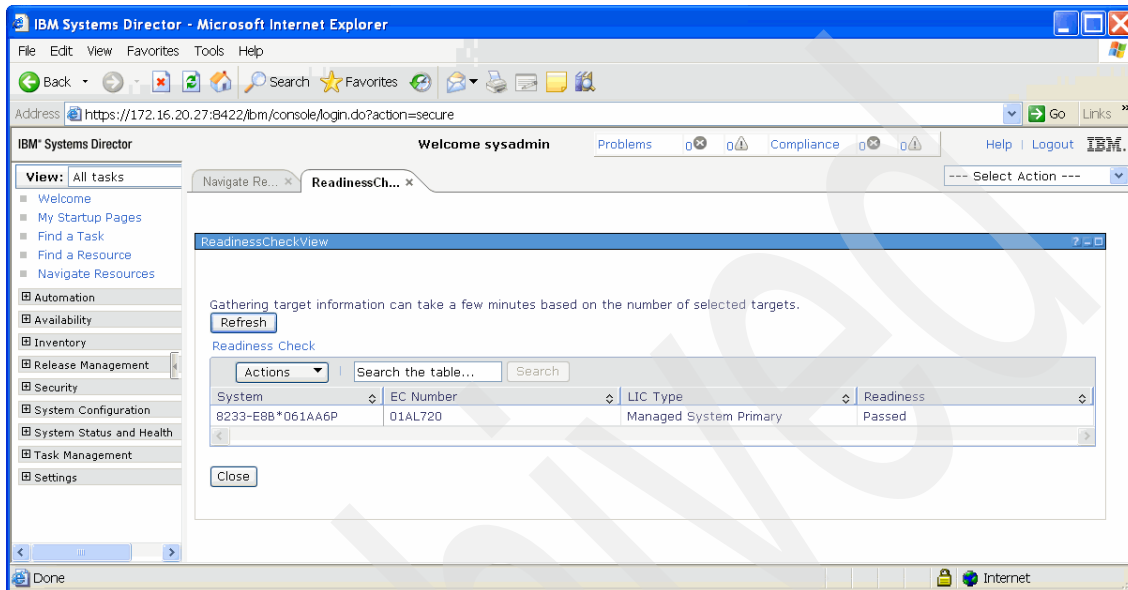


Figure 7-5 Readiness Check passed

7.1.2 Installing updates

The process for installing new updates to Power Systems consists of the following procedures:

- ▶ Getting the updated images
- ▶ Collecting the inventory
- ▶ Installing the updates
- ▶ Checking the results

Main differences from HMC

For users familiar with doing updates using the HMC, here is a list of the main differences when using the SDMC to perform update operations on Power Systems:

- ▶ Updates and upgrades are done through the same page and installation flow.
- ▶ Management operations such Accept and Reject are performed through different page flows than installations, as noted in the procedures outlined in this chapter.

- ▶ SDMC requires more update files for an image than just the .xml and .rpm files; it also requires the .dd.xml, .pd.sdd, and the .readme.txt files.
- ▶ User-controlled timing of an initial program load (IPL) and activation during a disruptive installation is not offered on SDMC. If the user chooses to perform an installation that is disruptive, the IPL (shutdown and reboot) and activation happens in real time during the installation process. The process does not pause for user interaction. If the user wants to delay the IPL and activation, they must choose to fully defer the disruptive action. The installation still occurs, but is not activated until the user clicks **Disruptive Activate** in the Power Firmware Management page. The deferred fixes will not activate until the next IPL.
- ▶ The connection status on the target system must be OK before processing an operation.
- ▶ The target system must be associated with the desired firmware package. If this relationship is not present, the Install button will not enable when attempting to launch the install. Running an inventory collection runs this relation processing.
- ▶ Import the firmware package after the target system has been discovered.
- ▶ Run inventory collection on the target system.

Getting updates

The easiest way to check for and download the latest updates is to configure the Update Manager connection settings (the default is for a direct connection, but a proxy server can also be specified) and then click the **Check For Updates** link from the Update Manager page to auto-check and download applicable updates (Figure 7-6).

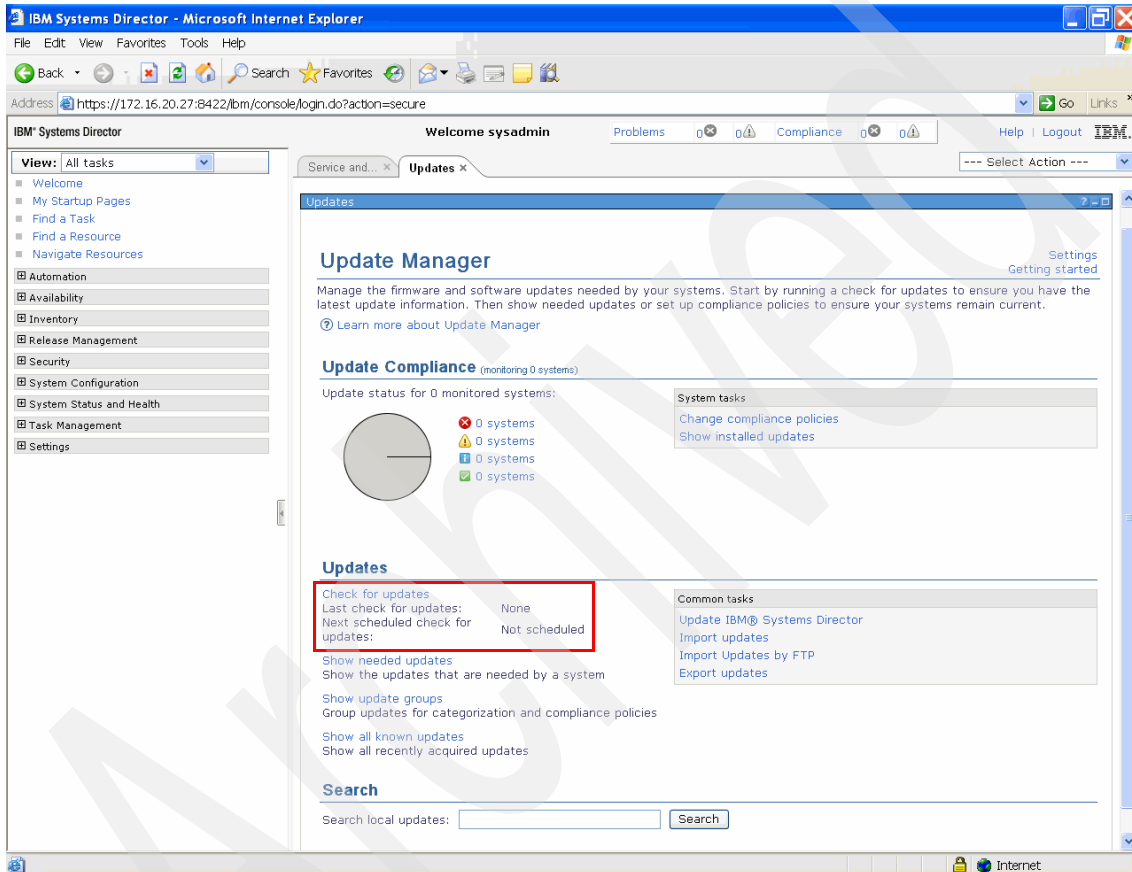


Figure 7-6 Update Manager: Settings and Check for Updates link

The user can then select the type of updates to check for on the Check for Updates page (Figure 7-7) and continue through the wizard to run a check for updates.

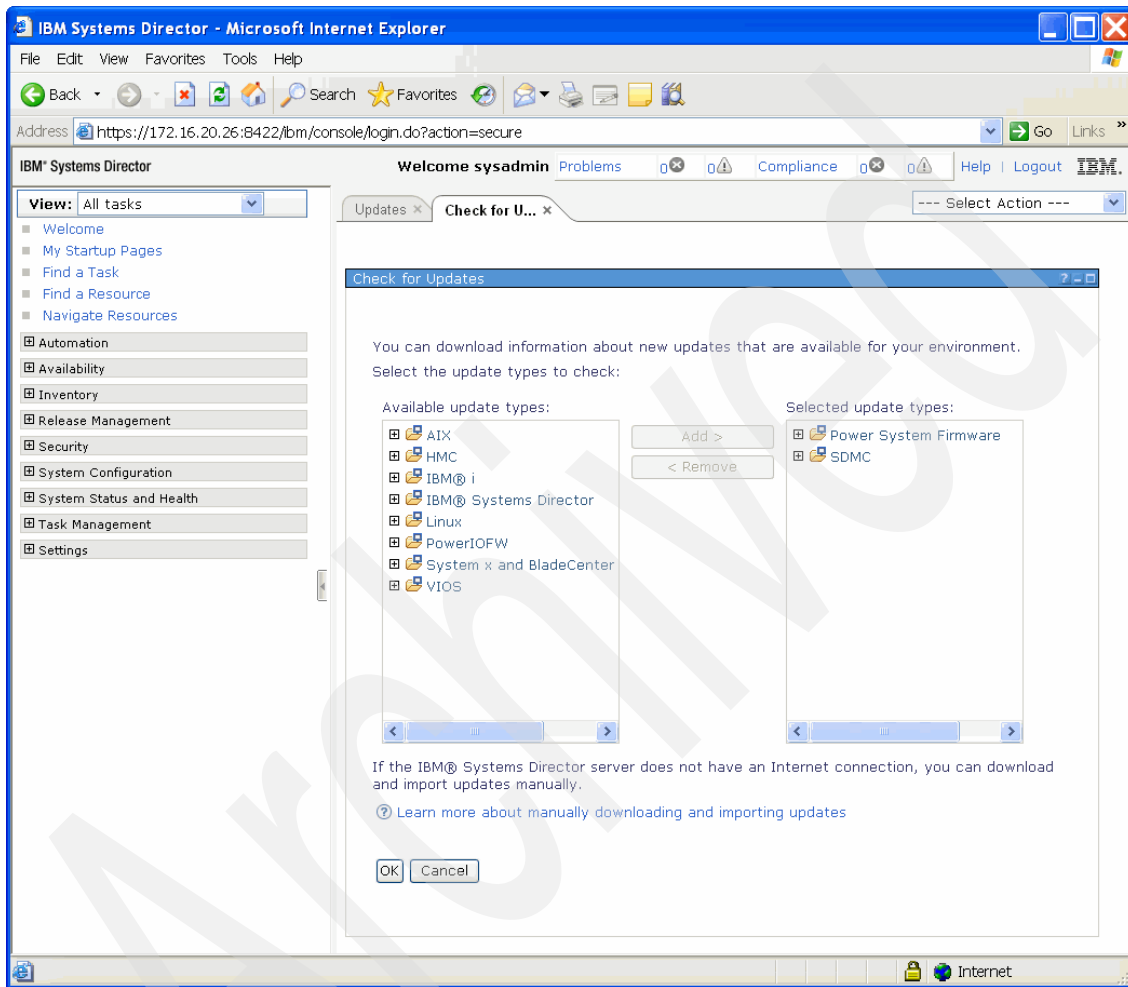


Figure 7-7 Check for Updates page

If the SDMC does not have access to the Internet and cannot be configured to access the IBM Fix Central site automatically, the updates can also be manually downloaded or ordered on DVD media and then imported into the SDMC. The user can import the update files from a specified local file system directory or through an FTP server.

The updates for any IBM hardware managed by the SDMC (including Power Systems and the SDMC appliance itself) can be downloaded from the IBM Fix Central website at the following address:

<http://www.ibm.com/support/fixcentral/>

If you want to run the import operation from the command line, run the **smcli importupd** command. Run **smcli importupd --help** to view the command's details and examples.

Run **mount --help** to view instructions about using the **mount** command.

After the DVD is mounted, the path to use when importing the updates is the mounted directory followed by the path on the DVD containing the update images.

Note: When using a USB device, run the **lsmediadev** command to find the device to mount.

Note: The following discussion assumes that the CD/DVD is always at `/dev/cdrom` and the USB is always at `/dev/sda1`

To mount the CD or DVD on Linux operating systems, insert the CD or DVD in the drive and enter the following commands, where `/mnt/cdrom` represents the location on the file system from which the files will be accessed:

- **mkdir /mnt/cdrom**
- **mount -t iso9660 -o ro /dev/cdrom /mnt/cdrom**

You can now specify the path entered above as the target directory using the Import Updates window or by using the **smcli importupd** command. Note that you must specify the full path to the install image files on the media, for example, `/mnt/cdrom/path/to/install/files`.

When mounting a USB device, the mount location is typically `/dev/sda1`. You can verify this location by running the **fdisk -l** command after plugging in the USB device. If `/dev/sda1` is present, that should be the USB device. When running the **mount** command, a path other than `/cdrom` should be used, such as `/mnt/usb`.

To mount the USB device, run the following command:

```
mkdir /mnt/usb
```

If the USB is formatted for an NTFS file system, run the following command:

```
mount -t ntfs /dev/sda1 /mnt/usb
```

If the USB is formatted for a vFAT file system, run the following command:

```
mount -t vfat /dev/sda1 /mnt/usb
```

The simplest version of **importupd** to run is:

```
smcli importupd /mnt/cdrom/path/to/install/files
```

Some common options for the **importupd** command are:

- v** Verbose output.
- r** Recurse to find all installable images available under the specified directory.
- help** Displays the importupd help text.
- s** Required for CDROM media

For example, if you are using the **-r** option, only the **/mnt/cdrom** path would be needed, for example, **smcli importupd -r /mnt/cdrom**. This command imports *all* the images available on the media device.

On the Update Manager page, the Common tasks section has links to the Import updates page, where the user can specify a local directory path to the update files (Figure 7-8).

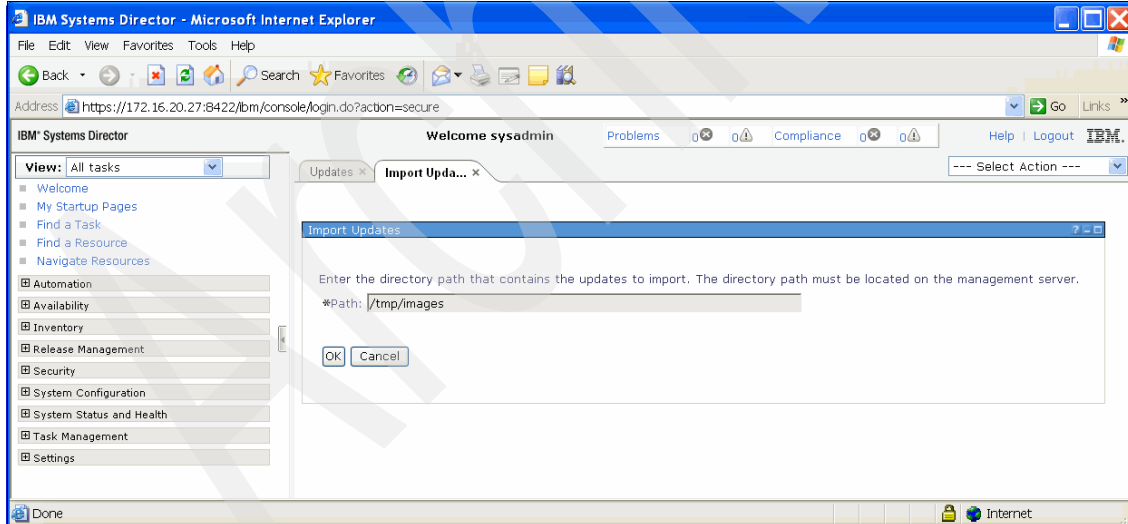


Figure 7-8 Import Updates from the local SDMC directory

In the same Common tasks section, there is also a link for Import Updates by FTP, where the user can specify a remote FTP address, directory path, and login information (Figure 7-9).

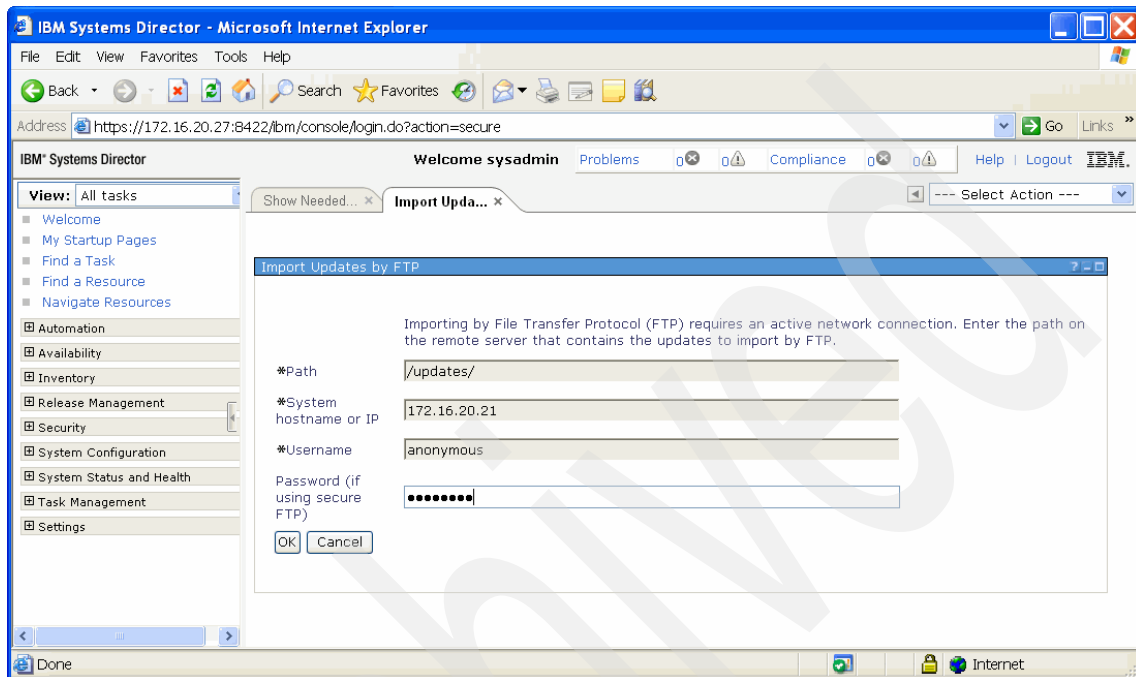


Figure 7-9 Import Updates using FTP

Updating target systems

On the Update Manager page, you can start an installation from the Show needed updates, Show all known updates, or Show update groups pages (Figure 7-10). Make sure to collect inventory on all the target systems that need to be updated before starting the update operations (if not, a message appears before the update starts that provides a button that the user can use to collect inventory before starting the update).

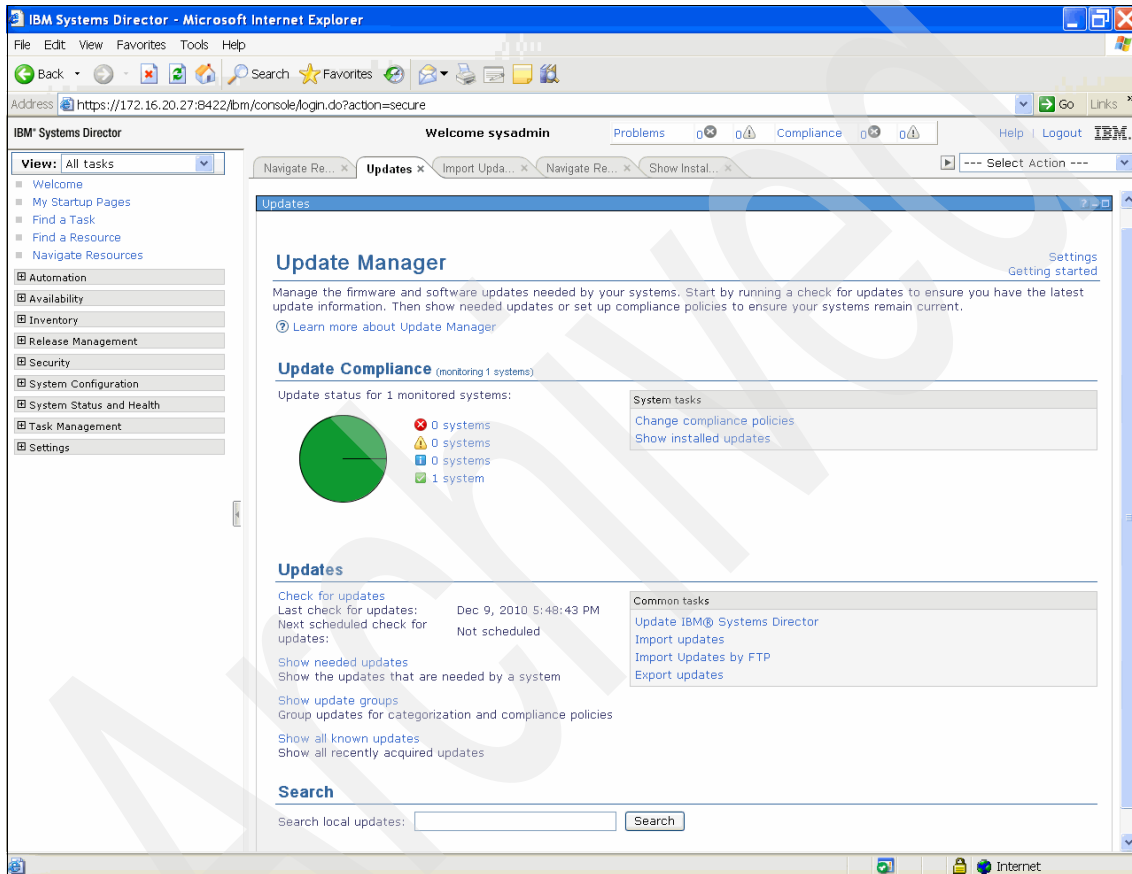


Figure 7-10 Installation links from Updates page

To update the target systems, perform the following steps:

1. To install the latest downloaded updates, start by clicking **Show needed updates** from the Update Manager page. The Show Needed Updates page opens and shows the Context Chooser dialog box (Figure 7-11).

Select the target systems for the installation operation and click **Add** to add the systems to the Selected list panel on the right. Click **OK** after making the selections to return to the Show Needed Updates page.

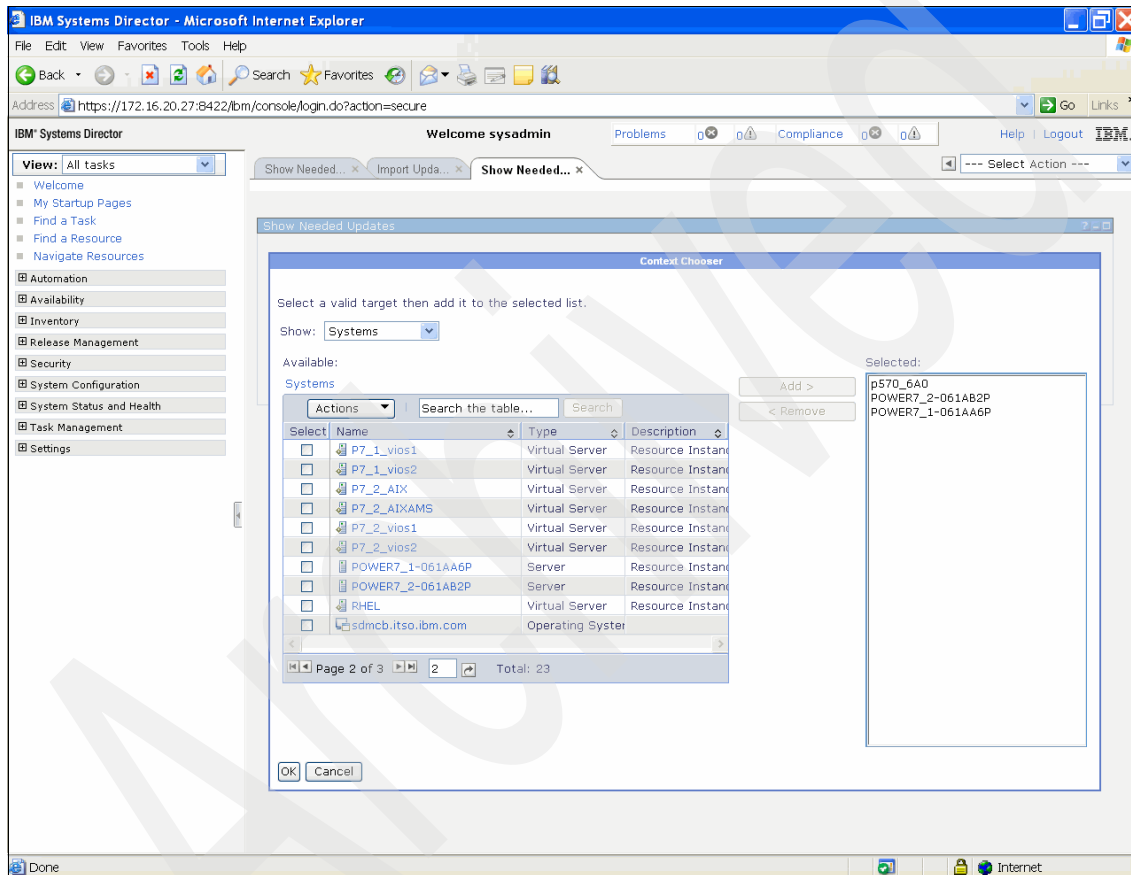


Figure 7-11 Target systems selection on the Show Needed Updates page

- The **Show Needed Updates** page opens and show the system(s) from the selected list. Click the **Show Needed Updates** button and a table that shows the updates needed by the selected system(s) opens and is populated with the applicable update code (Figure 7-12).

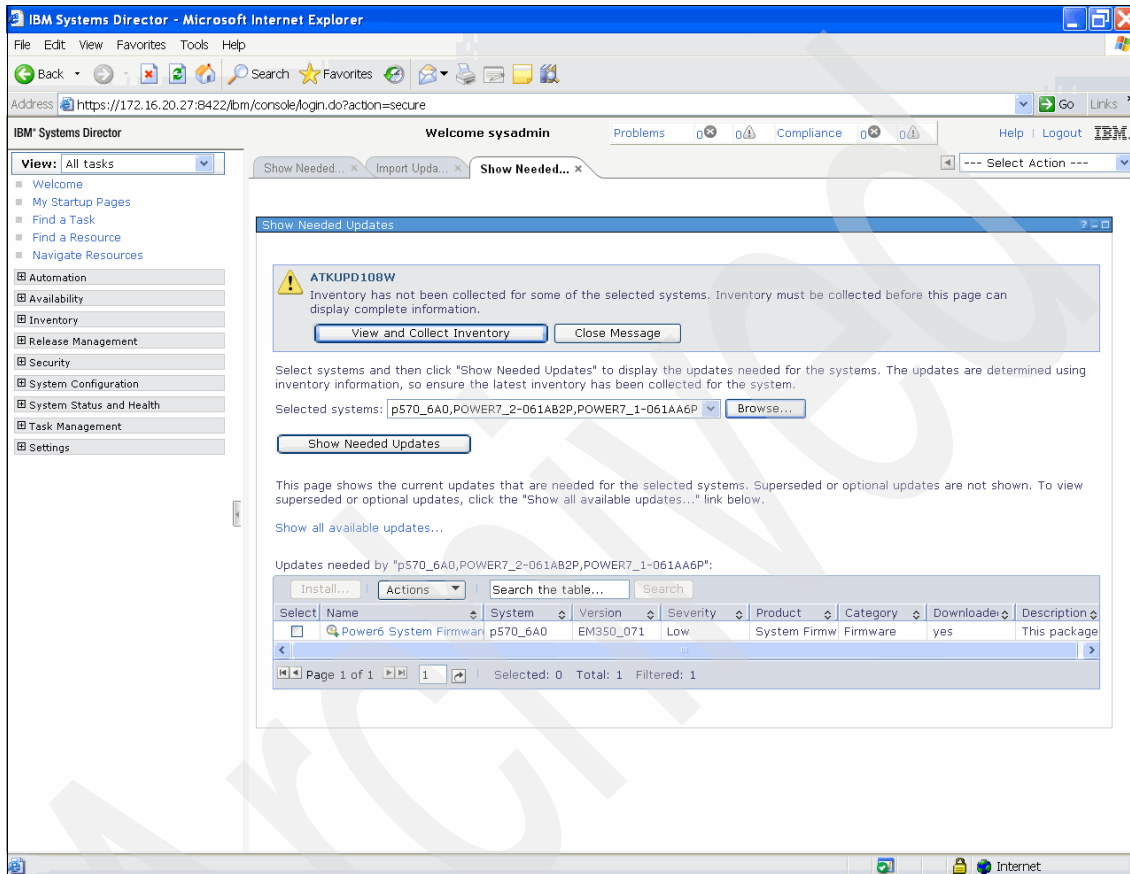


Figure 7-12 Show Needed Updates page

If no updates are listed in the Show Needed Updates page, click the **Show all available updates** link to view all updates that have been imported. Please note that any updates listed on the Show all available updates page will likely be older than what is currently installed on the target.

Verify the level of any updates listed on the Show all available updates page in relation to what is currently installed on the target before choosing to install them.

Also note the error message that appears at the top of the page stating that an inventory collection has not been completed for some of the selected systems. You need to collect inventory before performing the update process on the target servers. You can accomplish this task by going through the SDMC menus for inventory collection or by simply clicking the **View and Collect Inventory** button inside the error message.

3. After inventory collection has completed for all selected servers, the error message should disappear. Check the check box next to each of the needed updates listed in the table. The Install... button should now be available. Click this button to launch the Welcome page for the Install Wizard (Figure 7-13). Click **Next**.

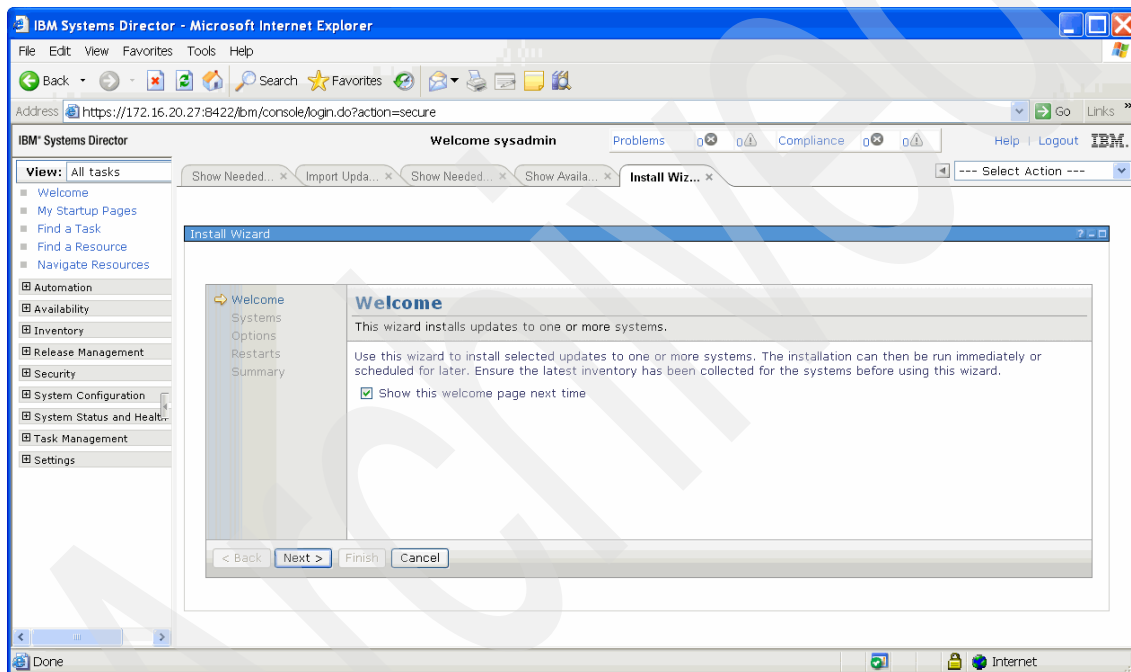


Figure 7-13 Install Wizard Welcome page

4. On the Systems page that opens (Figure 7-14), select the target system to which you want to apply the previously selected code update and add the system to the Selected list. Click **Next**.

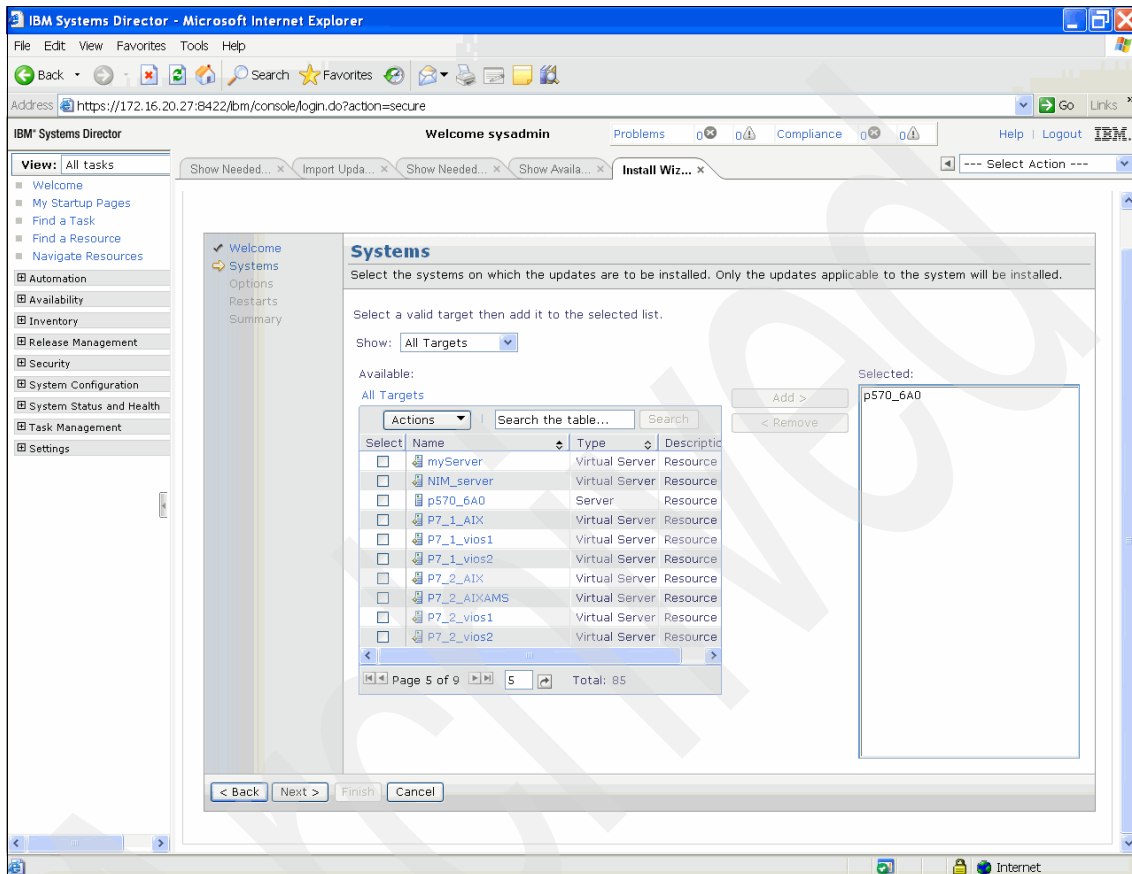


Figure 7-14 Select target systems

5. The Options page shows any applicable installation options or any additional required updates (Figure 7-15). Click **Next**.

Note: If the Options page reports that the advanced options could not be retrieved and are unavailable, simply continue with the install wizard.

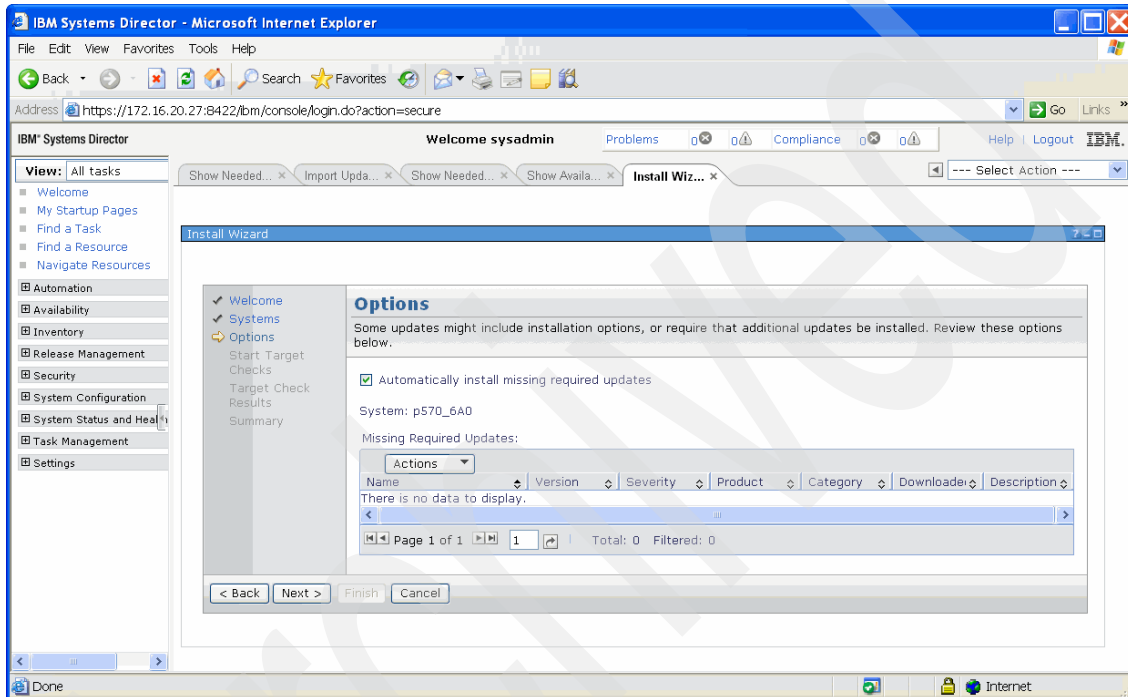


Figure 7-15 Select systems from install wizard

6. From the Start Target Checks page, initiate readiness and concurrency checks for the selected targets. These checks can take a few minutes depending on the number of targets selected. Click **Next** to continue. The Target Check Results page (shown in Figure 7-16) opens and shows the results of the checks.

An Information message box at the top of the page also shows the estimated time for the selected update task to complete. Here the user also selects whether to auto-accept the current firmware level on the temporary side of the FSP. Accepting this image copies the contents of the temporary FSP side to the permanent FSP side. Additionally, if the update is disruptive, the user is given the choice to either concurrently install with deferred activation or disruptively install and activate.

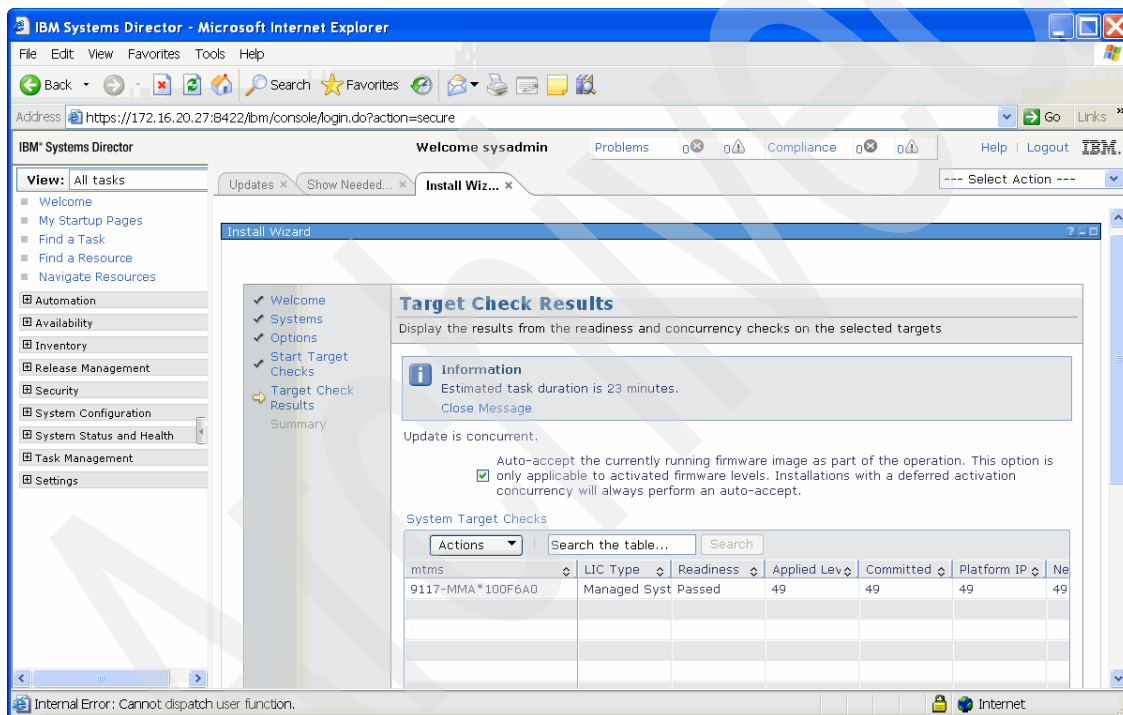


Figure 7-16 Target Check Results page

7. On the Show Needed Updates page, click the **Install...** button that becomes available. The Task Launch dialog box opens, which allows you to run the installation task now or to schedule it for later. Click **OK** to run the task now and the Active and Scheduled Jobs page opens and show the task progress. The status shows as Complete after the installation operation has been successfully run.

7.1.3 Power Firmware Management tasks

You can manage firmware on Power Systems using the Resources tab on the Welcome page of the SDMC GUI.

Power Firmware Management: Definitions

Before start out discussion of Power Firmware Management tasks, we need to define some terminology:

| | |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| T/P-side | An FSP has two flash sides: Temporary (T) and permanent (P). They are used in conjunction to perform a backup of a firmware level deemed to be stable and accepted by the customer. During a normal installation, the user writes the new firmware to the T side of the FSP. If this new version is not acceptable, the user can then revert back to the saved firmware that exists on the P side. |
| Accept | Copies the current T side of the FSP to the P side so that it acts as the new backup version of firmware. |
| Reject | Copies the saved P side of the FSP to the T side so that it acts as a restore operation. This function is available when you perform an IPL of the FSP on the P side. |
| Synchronize | For systems with redundant FSPs, copies the contents of the active FSP to the non-active redundant component. |
| Remove and Activate | This operation is similar to the Reject operation, but is available when the FSP is running on the T side. The difference is that for a Remove and Activate, the new code level being restored is also activated, because the user is currently running on the FSP side that is being restored. For a Reject, the user is not running on the FSP side that is being restored, so no activation needs to be done. |
| Disruptive Activate | Performs an IPL (system reboot) and activation of the code on the FSP side that is set as the next IPL side. This operation also activates any updates that were deferred from a previous installation. |
| Set Next IPL Side | Toggles which FSP side (T or P) becomes active on the next IPL. |

Procedures for Power Firmware Management operations

From the Resources tab on the Welcome page on the SDMC GUI, perform the following steps to perform management operations of a Power Systems firmware update:

1. Select the target system(s), and then select **Release Management** → **Power Firmware Management** from the Action select button (Figure 7-17).

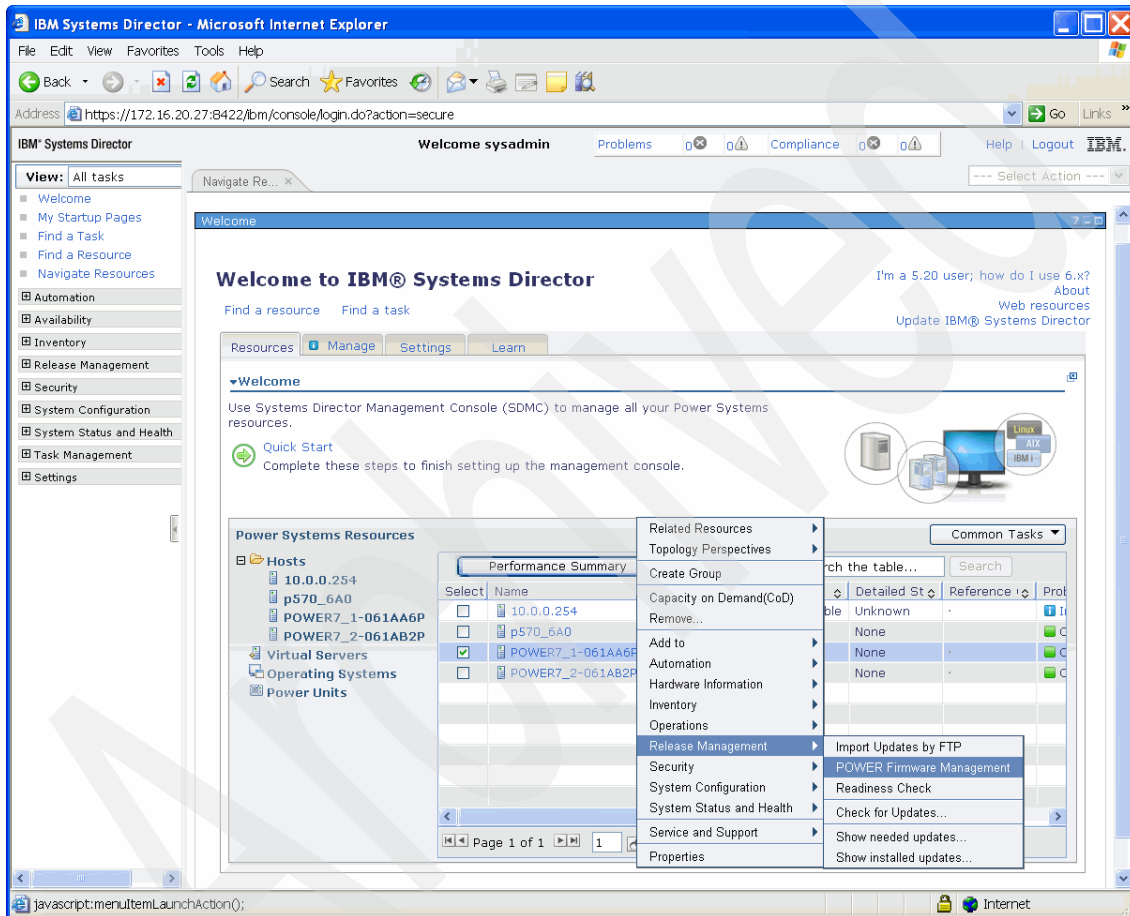


Figure 7-17 Power Firmware Management

The **Power Firmware Management** page opens (Figure 7-18). As with the readiness check, click **Gather Target Info** to gather the target information, which populates the table with the selected target system information. The Readiness state of the system must show Passed to proceed with firmware management operations.

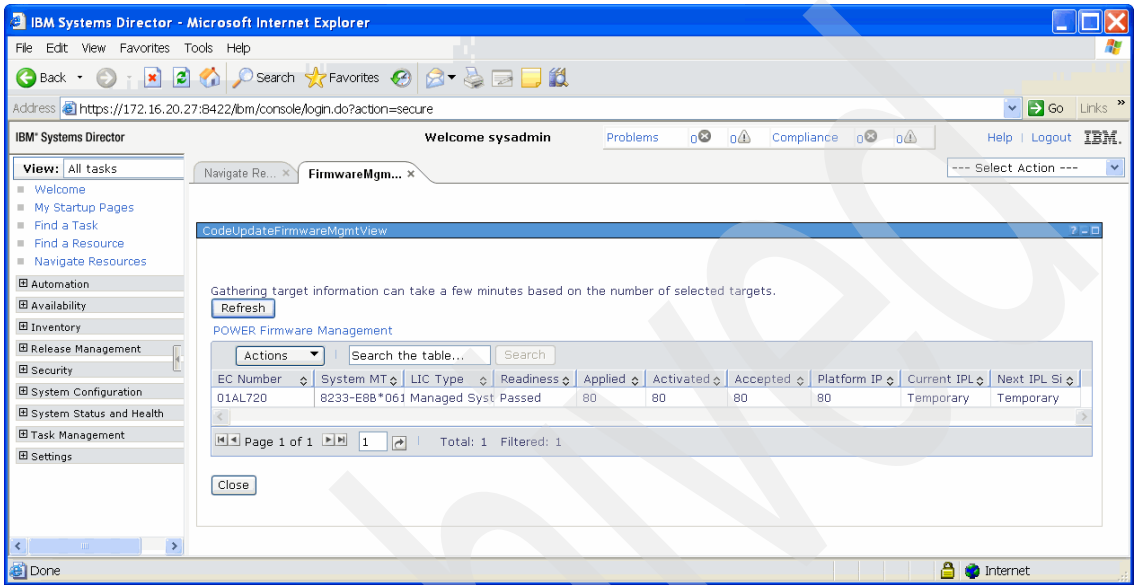


Figure 7-18 Power Firmware Management page

2. After the target information is gathered, the Accept/Reject, Disruptive Activate, Synchronize, Remove and Activate, and Set Next IPL Side options are available. The availability of the tasks is side dependent, meaning that, for example, if the P side of the FSP is active, **Accept** will not be available, and if the if T side is active, **Reject** will not be available. From the **Action** menu, click **Accept** (Figure 7-19).

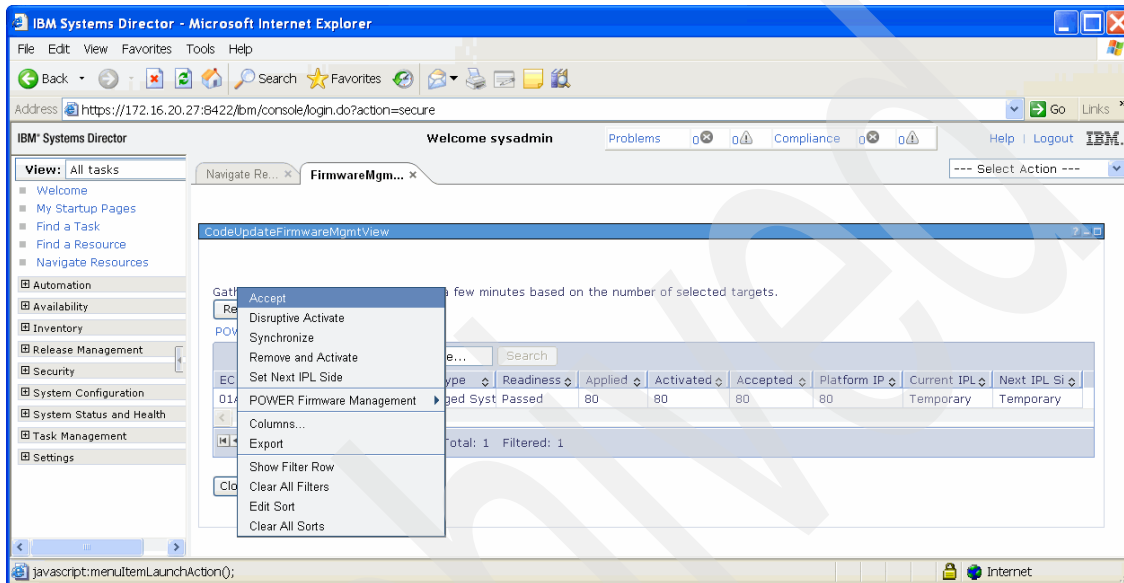


Figure 7-19 Accept

3. Click the **Start Accept Task** button (Figure 7-20).

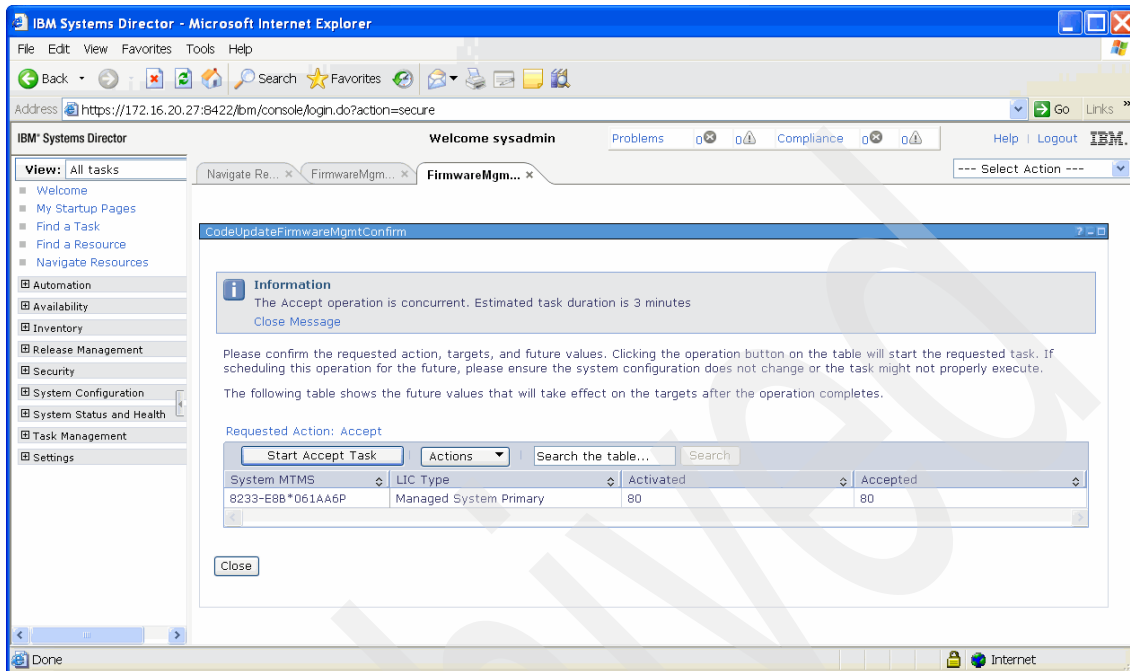


Figure 7-20 Start Accept Task

The Task Launch dialog box opens and prompts you to run the Start Accept Task now or to schedule it for later. Click **OK** to run the task now and the Active and Scheduled Jobs page shows the task's progress. The Complete status appears after the task is successfully run.

Virtual Server operation

The Virtual Server operation contains the operations for Virtual Servers. Some of these operation are done on a day-to-day basis, and some of them are done less often. The following topics are covered in this chapter:

- ▶ How to create a Virtual Server.
- ▶ How to activate a Virtual Server.
- ▶ How to shut down a Virtual Server.
- ▶ How to handle the configuration of Virtual Servers.
- ▶ How to do suspend and resume a Virtual Server.
- ▶ How to relocate a Virtual Server.
- ▶ How to do Virtual I/O management.

8.1 Virtual Server creation

On the Hardware Management Console, *Virtual Servers* (formerly known as LPARs) were created using the Systems Management tab and the context menus of the server on which the Virtual Servers were created. Those menus have not changed much, but are now located on the Welcome page of the IBM Systems Director Management Console (SDMC). The new menus have the option to create virtual adapters automatically, which is supported for virtual SCSI adapters and for Fibre Channel adapters. There are different ways the menus are accessed.

To create a Virtual Server, perform the following steps:

1. From the Welcome page, locate the host on which the Virtual Server will be created. Check the check box left to the host, then select **Actions** → **System Configuration** → **Create Virtual Server** (Figure 8-1).

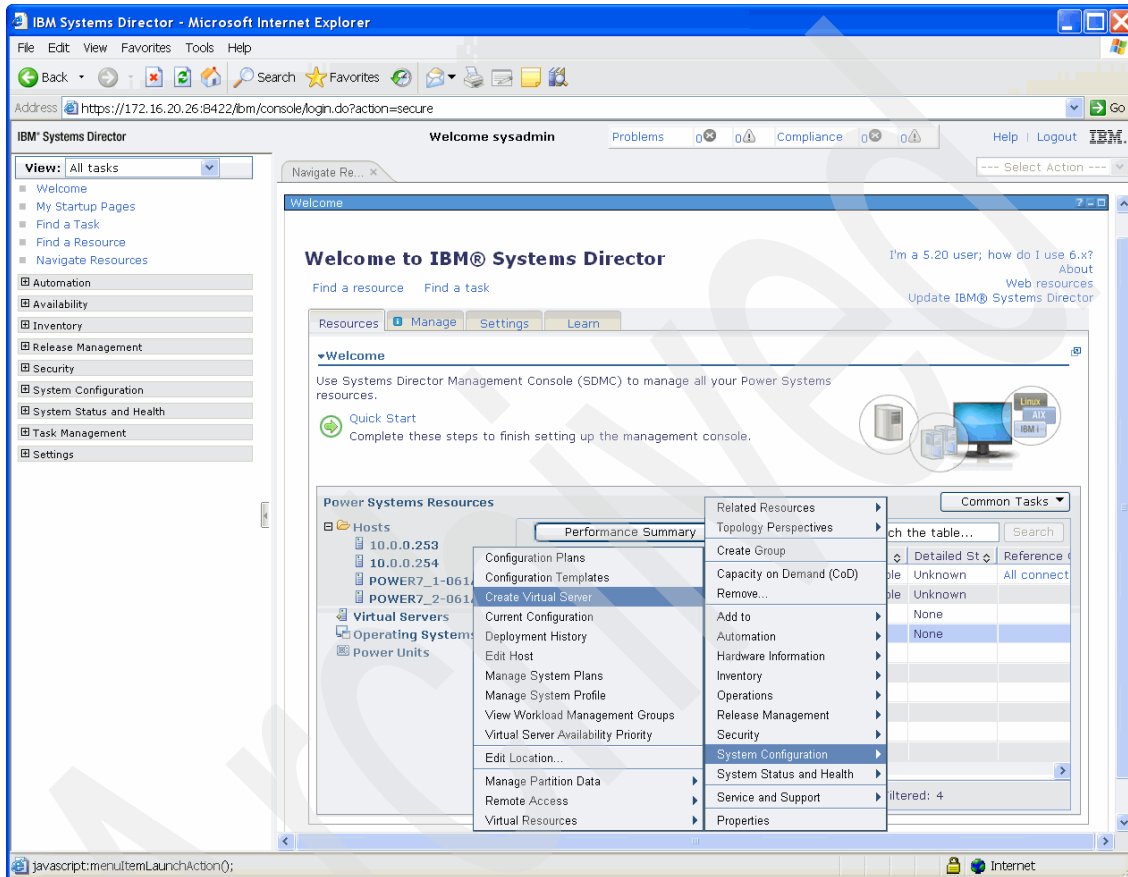


Figure 8-1 Welcome page with context menu: Create Virtual Server

Figure 8-2 shows the wizard that allows you to create a Virtual Server.

2. On the Name page, the name of the server must be entered. Other information, such as Virtual Server ID (the wizard has preset the next free ID already), type of environment (AIX/Linux, IBM i, or VIOS), and settings, such as Suspend capable or Assign all resources to this Virtual Server, can be changed. The Virtual Server created will default to AIX/Linux. The options for Virtual I/O Server differ, as well as the options for IBM i, and are discussed momentarily.

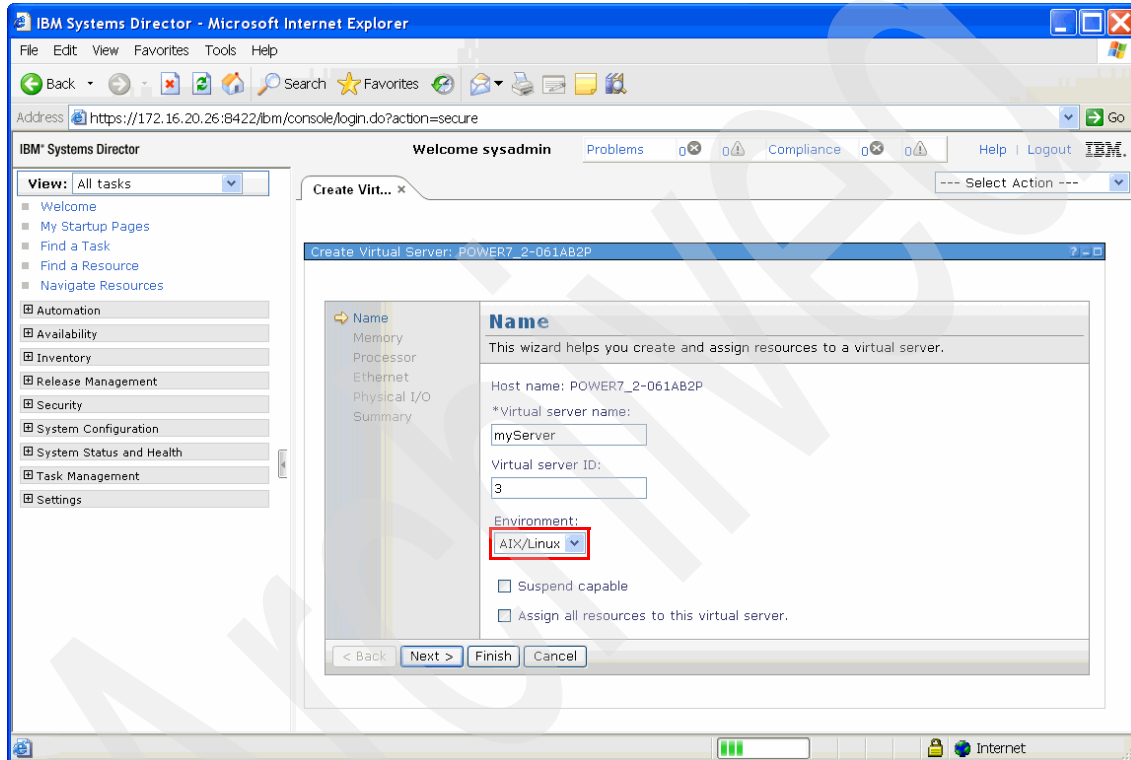


Figure 8-2 Create Virtual Server wizard

- When you are creating a Virtual Server for the Virtual I/O Server environment type, some selections will be not available (Figure 8-3). The **Suspend enable** and **Assign all resources to this virtual server** options are not available for a Virtual I/O Server environment.

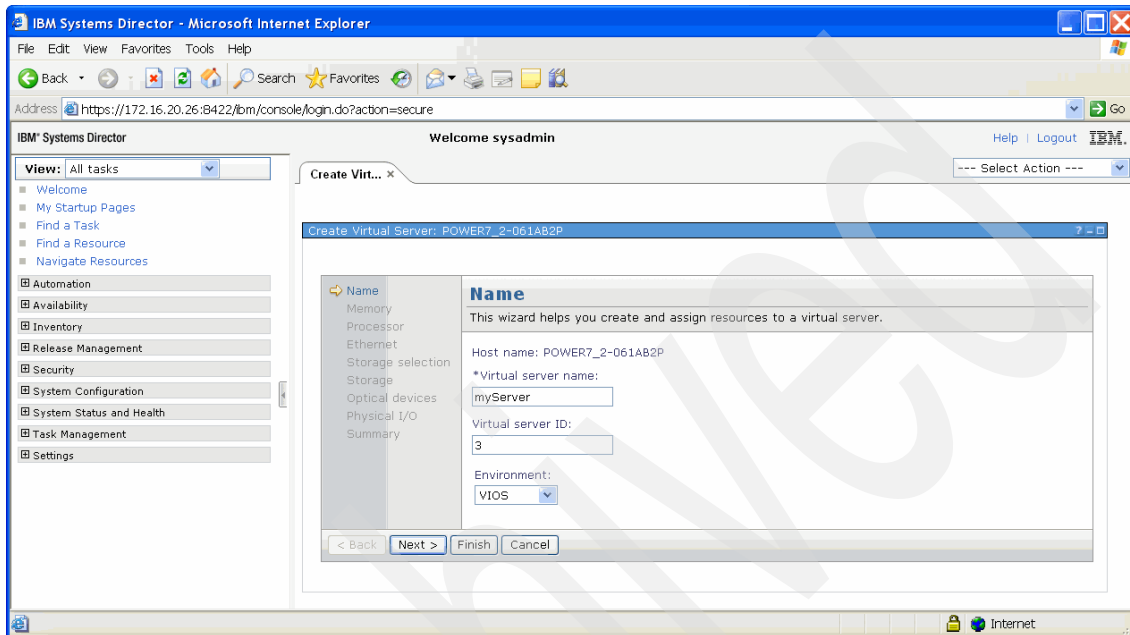


Figure 8-3 Create Virtual Server wizard: Virtual I/O Server Name

4. To create IBM i Virtual Servers, use the **Memory** menu (Figure 8-4). The difference here it that an additional entry exists, that is, the Load Source/Console pane.

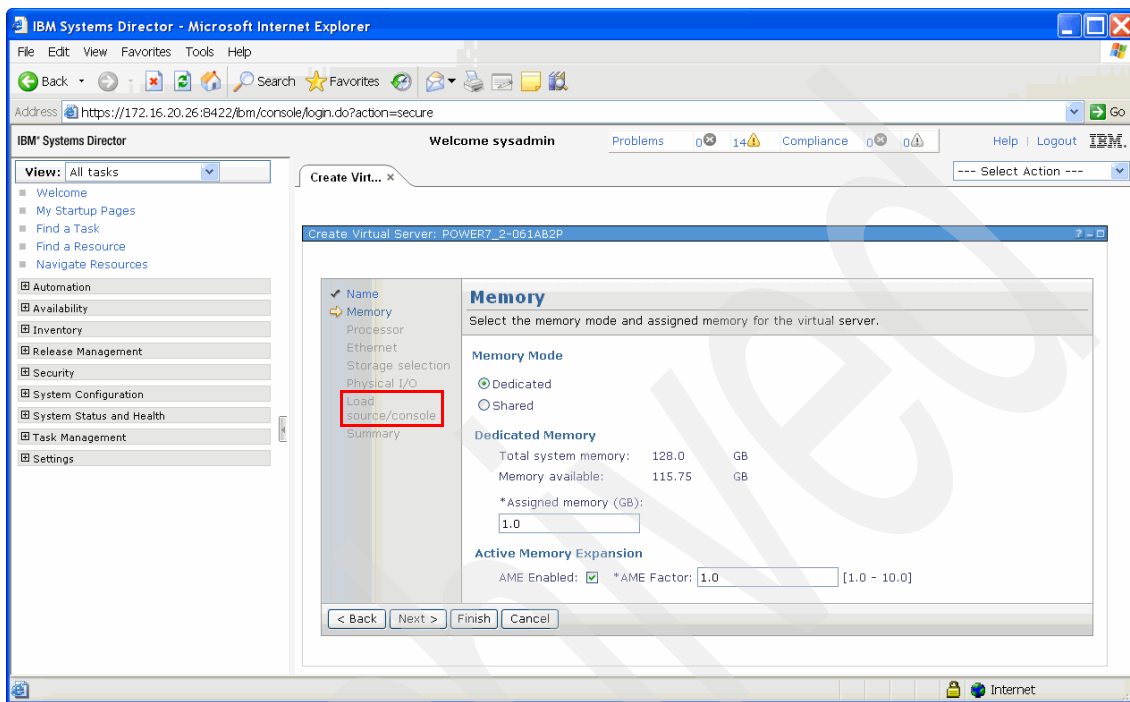


Figure 8-4 Create Virtual Server wizard: IBM i Name panel

5. The assigned memory can be dedicated or shared (Figure 8-5). The Shared option needs the Active Memory Sharing code to be activated. This activation is only available with PowerVM Enterprise Edition.

By default, 1 GB of RAM is assigned to the newly created Virtual Server. If you leave this default on, you can change the amount of memory assigned to the Virtual Server by using the **Manage Virtual Server** menu (Figure 8-31 on page 165).

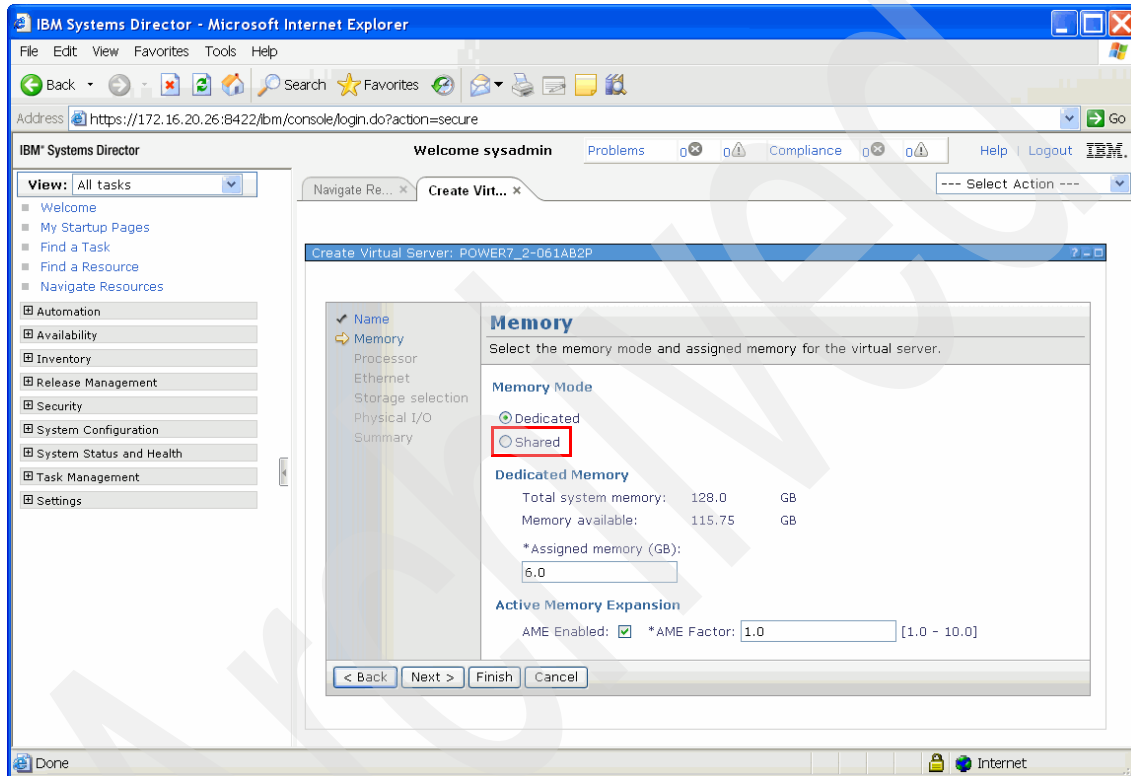


Figure 8-5 Create Virtual Server: Memory

6. As shown in Figure 8-6, the default processor mode for Virtual Servers is Shared, which means that processors in a shared pool are used. The shared pool to be used is the default pool and is not shown unless more than one shared processor pool has been created beforehand. In that case, a menu is shown that allows you to select the desired shared processor pool. Note that the assignment of Entitled Capacity values is not possible anymore when creating the Virtual Server. This assignment can be done by editing the Virtual Server Profile later.

By default, one virtual processor is assigned to a Virtual Server, but this setting can be easily changed using the Manage Virtual Server wizard (Figure 8-29 on page 163).

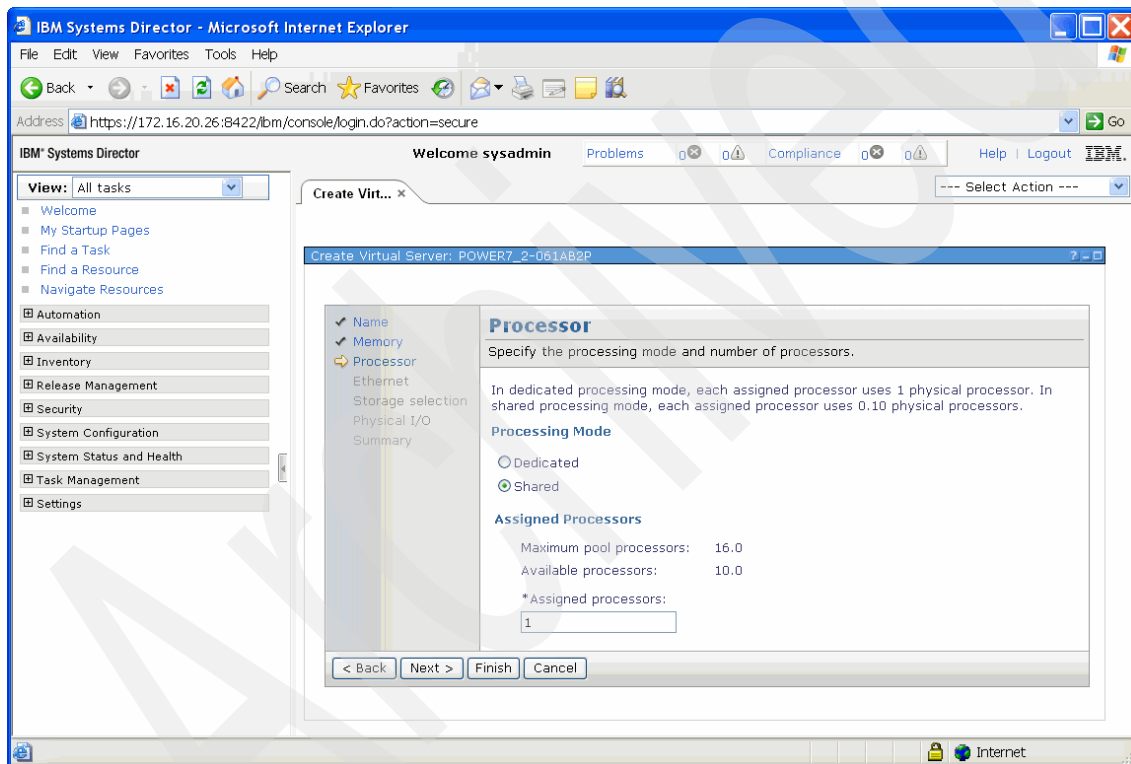


Figure 8-6 Create Virtual Server: Processor

- As shown in Figure 8-7, the wizard queries the available Ethernet connections of the Virtual I/O Servers. The first entry in the Virtual Ethernet tab shows a Shared Ethernet Adapter connection that is enabled for failover between Virtual I/O Servers. The second entry shows a Shared Ethernet Adapter that has been enabled for multiple VLANs. All the listed adapters are added to the Virtual Server. Additional adapters can be added by clicking the **Add** button. Also, if the check box to the left of an adapter is clicked, it can be edited and its properties changed.

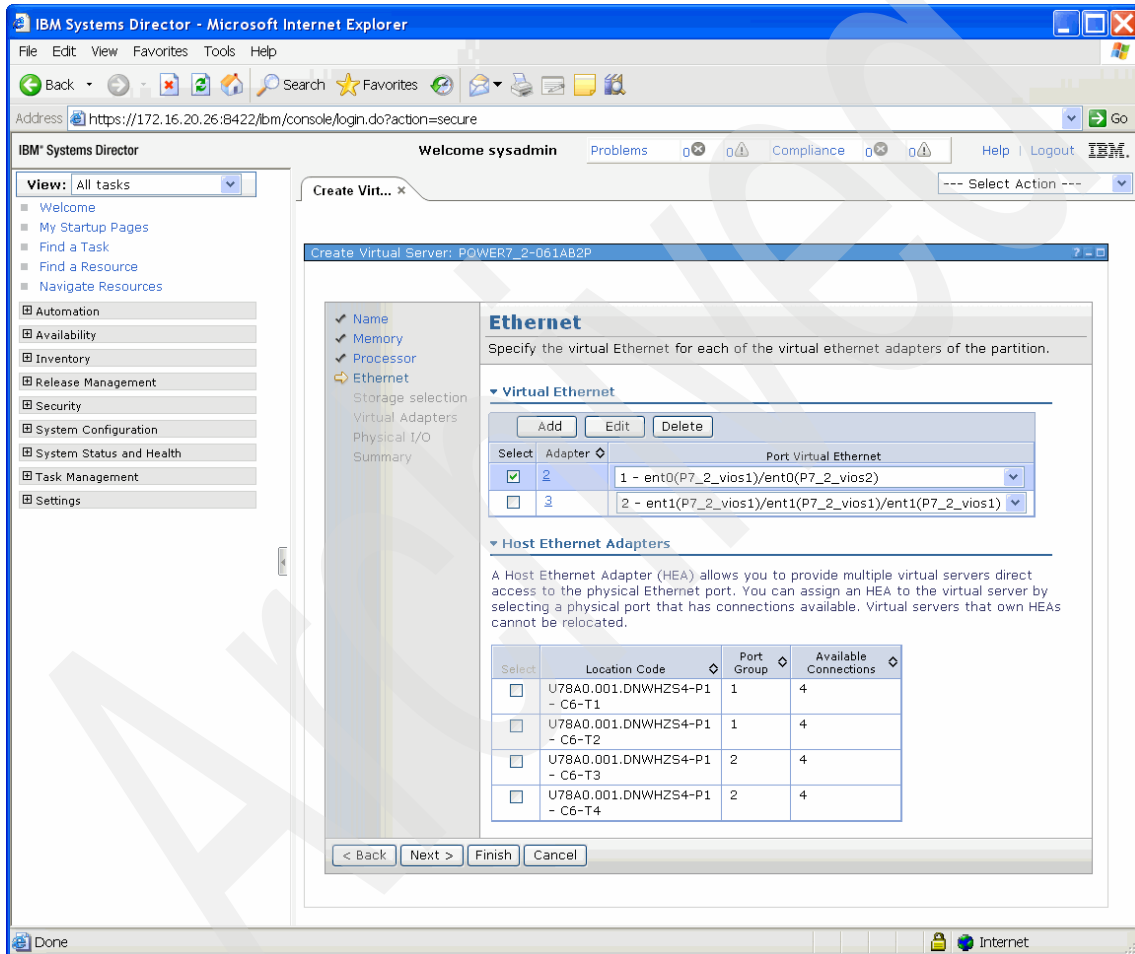


Figure 8-7 Create Virtual Server: Ethernet adapter

If you would like to add a Logical Host Ethernet Adapter port to the partition, check the box next to the desired adapter listed under Host Ethernet Adapter. The validation check of Live Partition Mobility will note this setting because it is considered a physical adapter for this purpose. This configuration is different from the HMC configuration, but much easier to do because there is no additional information to enter: Just click and you are set.

If you want to remove an adapter, check the check box next to the adapter and click **Remove**.

8. On the Storage tab, there are now two options offered (Figure 8-8). The first option offers configuration as it was on the Hardware Management Console, shown here as “No, I want to manage the virtual storage adapters for this server.” This option allows for manual creation of adapters and thus full control of adapter and slot definitions on the Virtual Server as well as their connecting adapters on the Virtual I/O Servers.

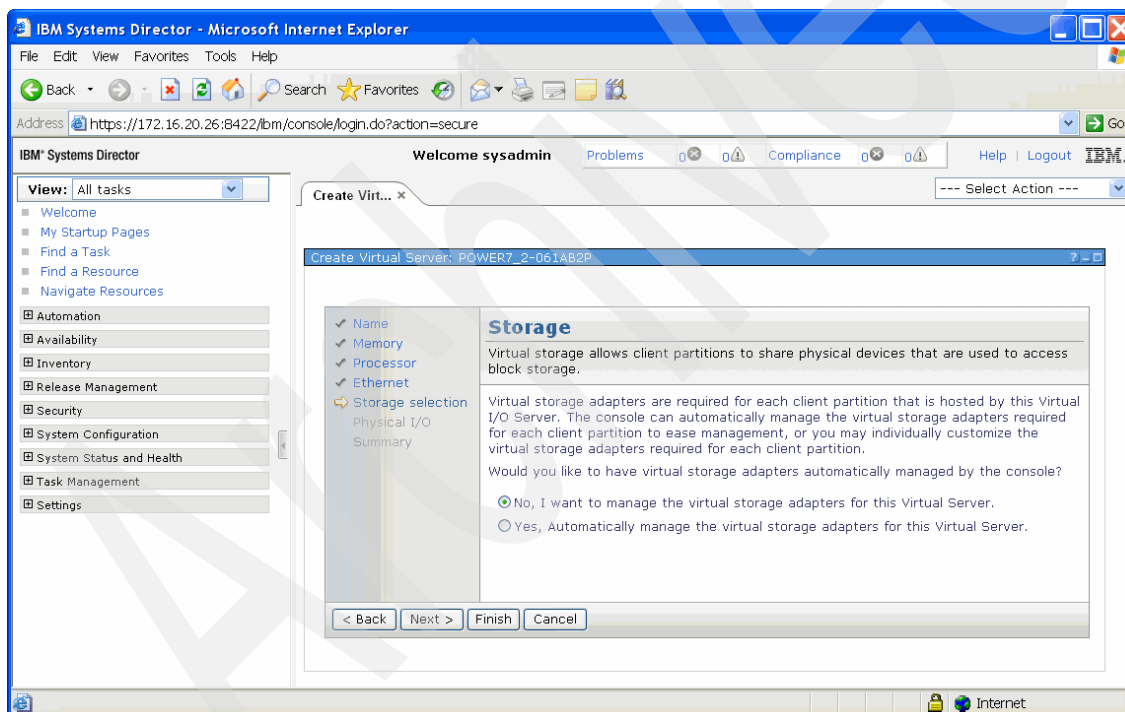


Figure 8-8 Create Virtual Server: Manual storage allocation

The ability to add storage adapters automatically when creating a Virtual Server was added to provide legacy support. When chosen, you should rarely need to work on virtual SCSI adapters when creating a Virtual Server. This ability simplifies configuration because manual checks ensure that the correct connection information for the connecting adapter on the Virtual I/O Server was entered and is not needed anymore.

If the second option “Yes, Automatically manage the storage adapters for this Virtual Server” is chosen, the wizard assigns the storage adapter to the next available virtual adapter slot. The connecting adapter on the Virtual I/O Server is created accordingly and the connection to the adapter in the Virtual Server is established automatically. The automatic management of storage adapters does not take into account considerations such as mirroring disks over two adapters or multipathing to the Virtual Server, but these options can be added after the Virtual Server has been created.

9. The Create Adapter entry (Figure 8-9) allows for manual definition of the properties of the storage adapter (Figure 8-10 on page 142). Note that it also allows for selection of the adapter type, for example, SCSI or Fibre Channel.

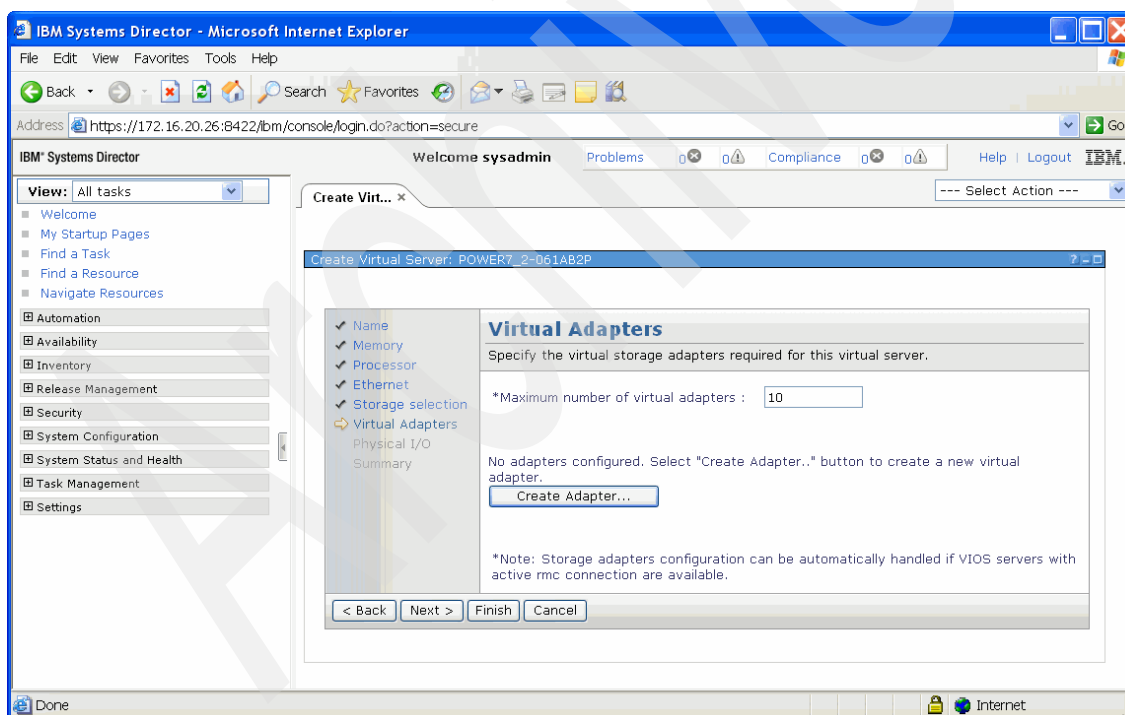


Figure 8-9 Create Virtual Server: Virtual Storage adapter creation

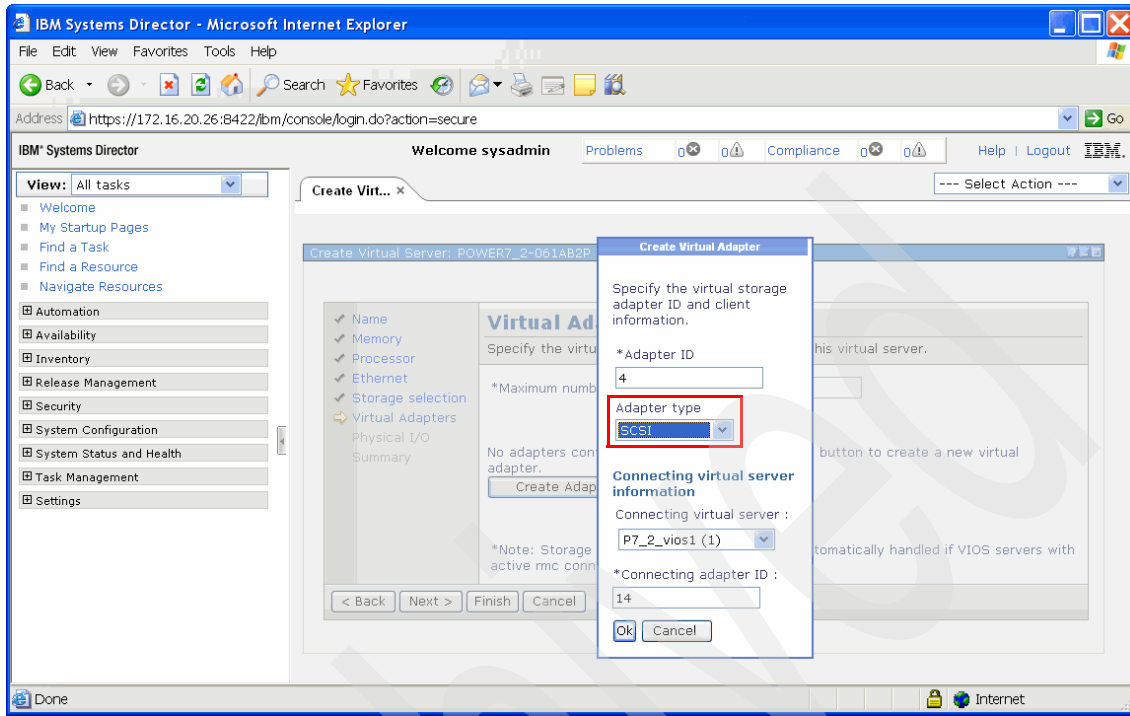


Figure 8-10 Create Virtual Server: Assign storage adapter IDs

10. The results are shown in Figure 8-11. If you decide to add another adapter to a second Virtual I/O Server, click the **Add** button.

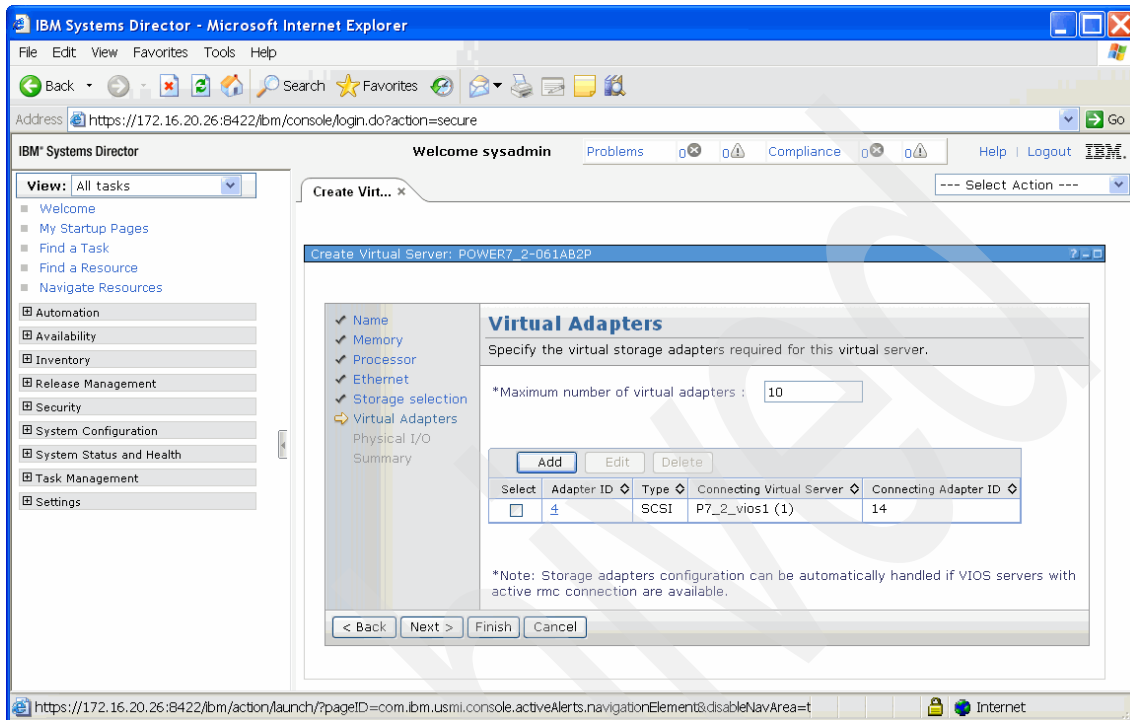


Figure 8-11 Create Virtual Server: Manual SCSI adapter creation

11. If automatic storage adapter creation is chosen (Figure 8-12), additional choices are offered for Virtual Disks, Physical Disks and Fibre Channel disks. You can check any of the check boxes for these choices in any combination.

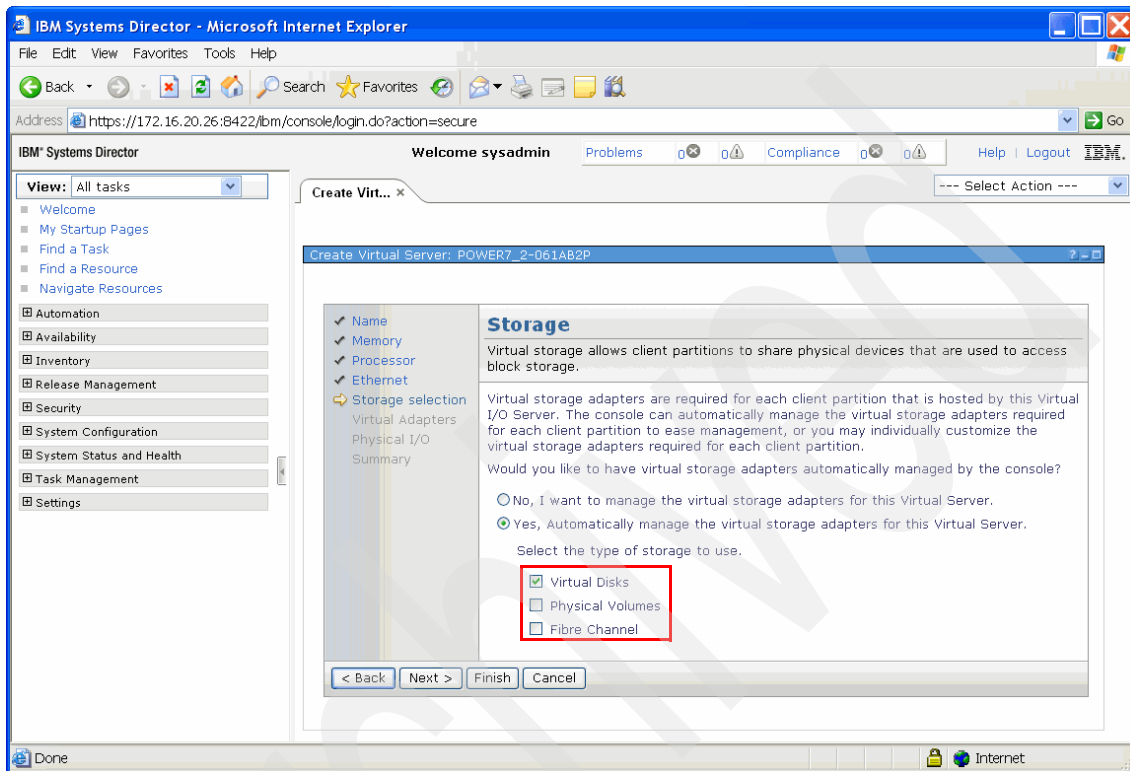


Figure 8-12 Create Virtual Server: Automatic adapter creation

12. Click **Next**. The page shown in Figure 8-13 opens. Clicking the **Create Virtual Disk** button opens a page where the properties of the virtual disk to be created are set.

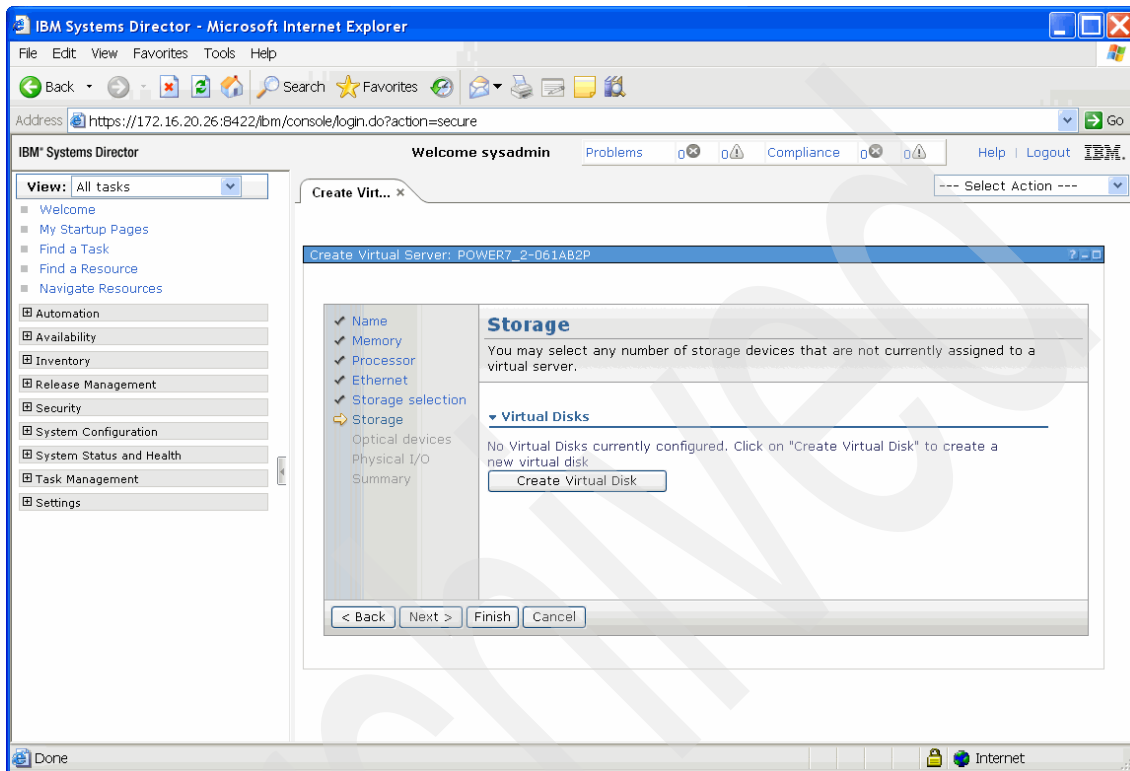


Figure 8-13 Create Virtual Server: Create virtual disk

As shown in Figure 8-14, the Virtual I/O Server, the name, the disk pool and the size must be specified for the disk to be created.

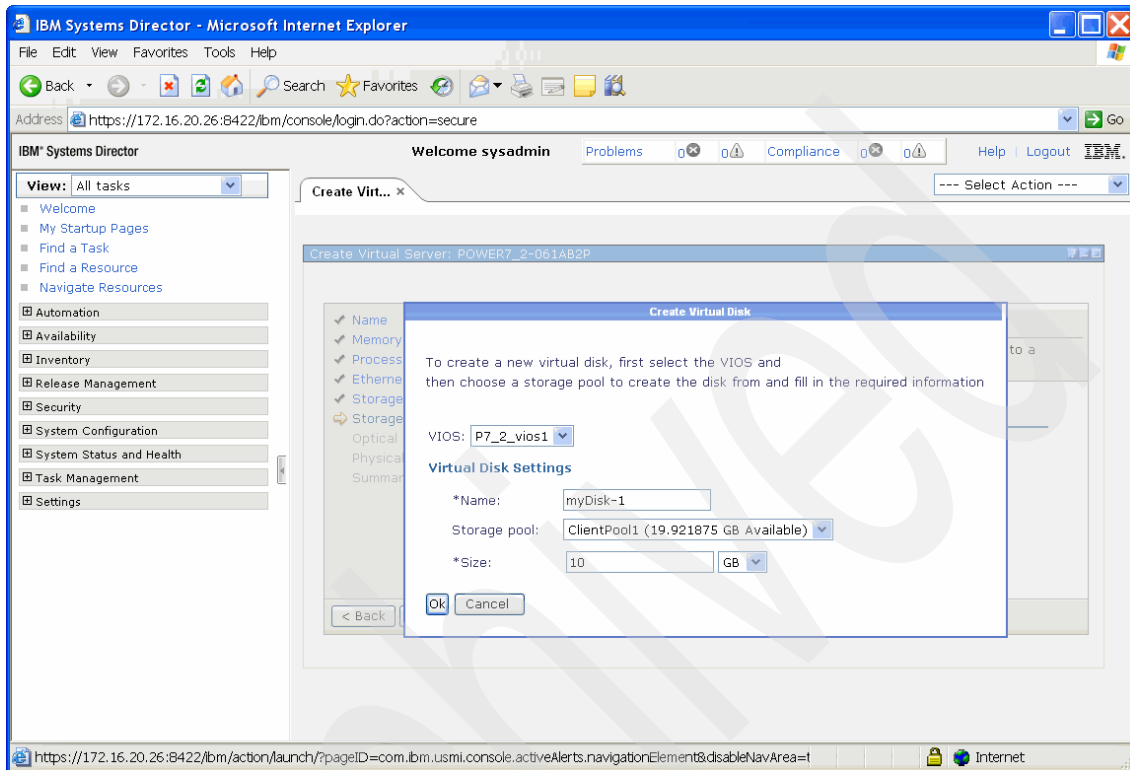


Figure 8-14 Create Virtual Server: Characteristics of a virtual disk

13. If automatic storage adapter creation for Physical Disks was checked, you can select available disks in all Virtual I/O Servers on the server using the page shown in Figure 8-15. Available disks are defined as disks that are not mapped to Virtual Servers and are not members of a volume group. More than one disk can be selected. If more than one disk is chosen from one Virtual I/O Server, just one virtual SCSI adapter is created. However, if disks from another Virtual I/O Server are chosen, a virtual adapter pointing from that Virtual I/O Server to the Virtual Server is also created. Note that the virtual disk created in step 12 on page 145 is assigned to this Virtual Server.

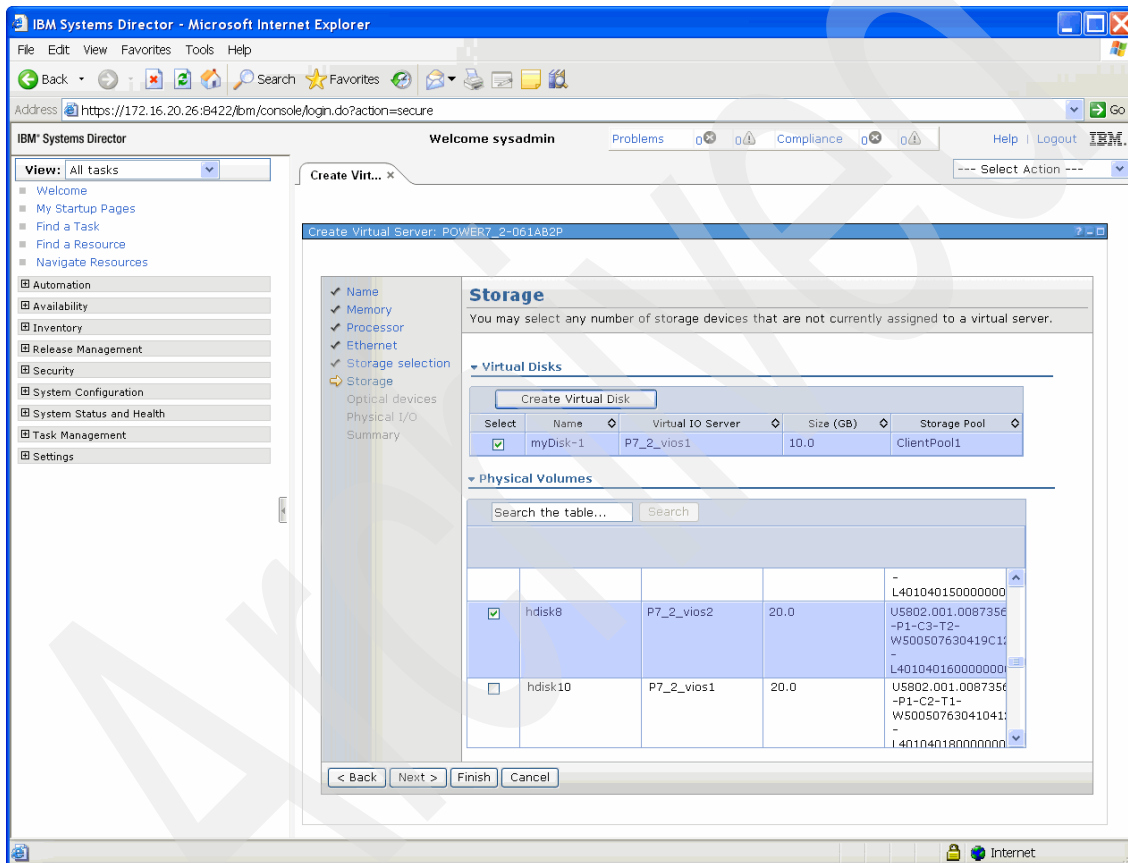


Figure 8-15 Create Virtual Server: Virtual and physical disk selection

14. If you select Fibre Channel in the page shown in Figure 8-16, then, on the Storage page, you can see the available Fibre Channel adapters on the Virtual I/O Servers, along with the number of available virtual connections for that adapter.

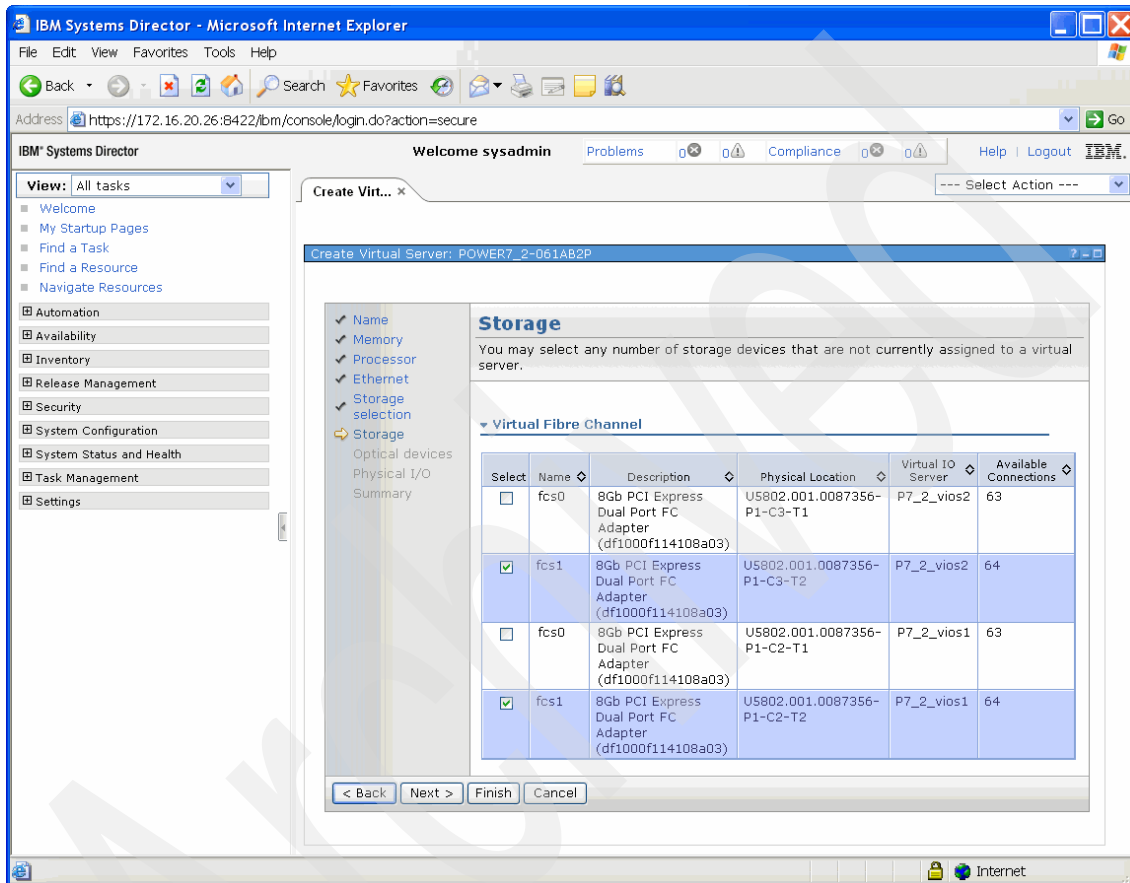


Figure 8-16 Create Virtual Server: Virtual Fibre Channel adapter selection

15. In Figure 8-17, you can select either physical or virtual optical media. A virtual optical device is chosen that contains installation media.

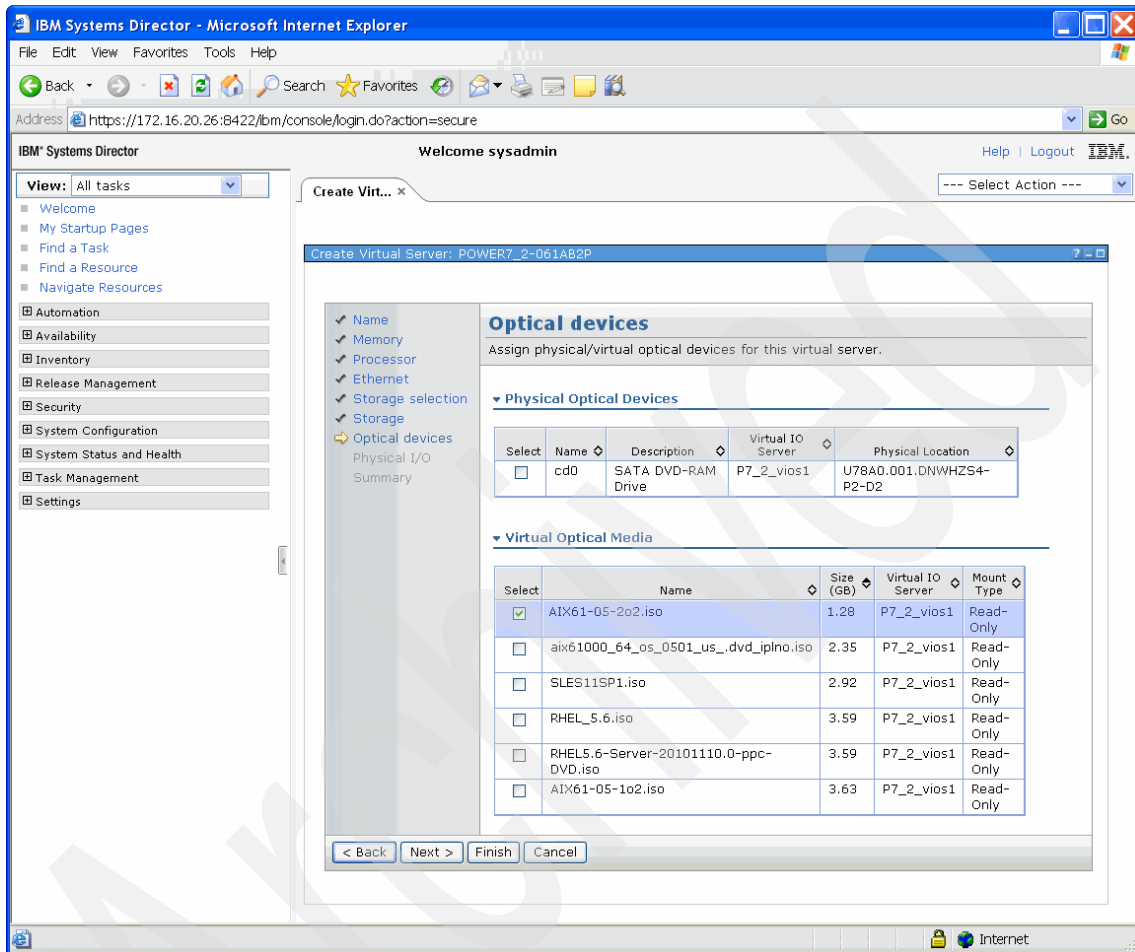


Figure 8-17 Create Virtual Server: Optical device and media selection

16.If you created an IBM i Virtual Server, an additional page is available before you get to the Summary page. This page allows you to specify the load source, the alternate load source, and to assign the console connection to the IBM i Virtual Server (Figure 8-18).

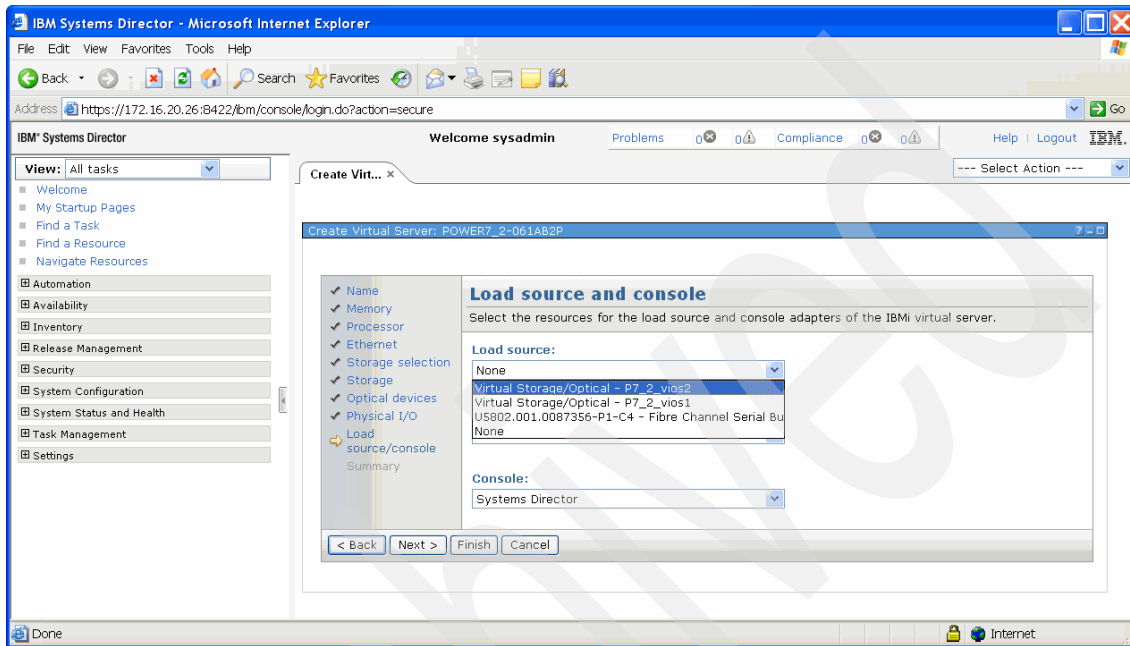


Figure 8-18 Create Virtual Server: Load Source and Console

17. The last page in the Create Virtual Server Wizard, the Physical I/O Adapters page, allows you to attach physical adapters to the Virtual Server. Here, for demonstration purposes, a Fibre Channel adapter and an Ethernet adapter are assigned to the Virtual Server (Figure 8-19).

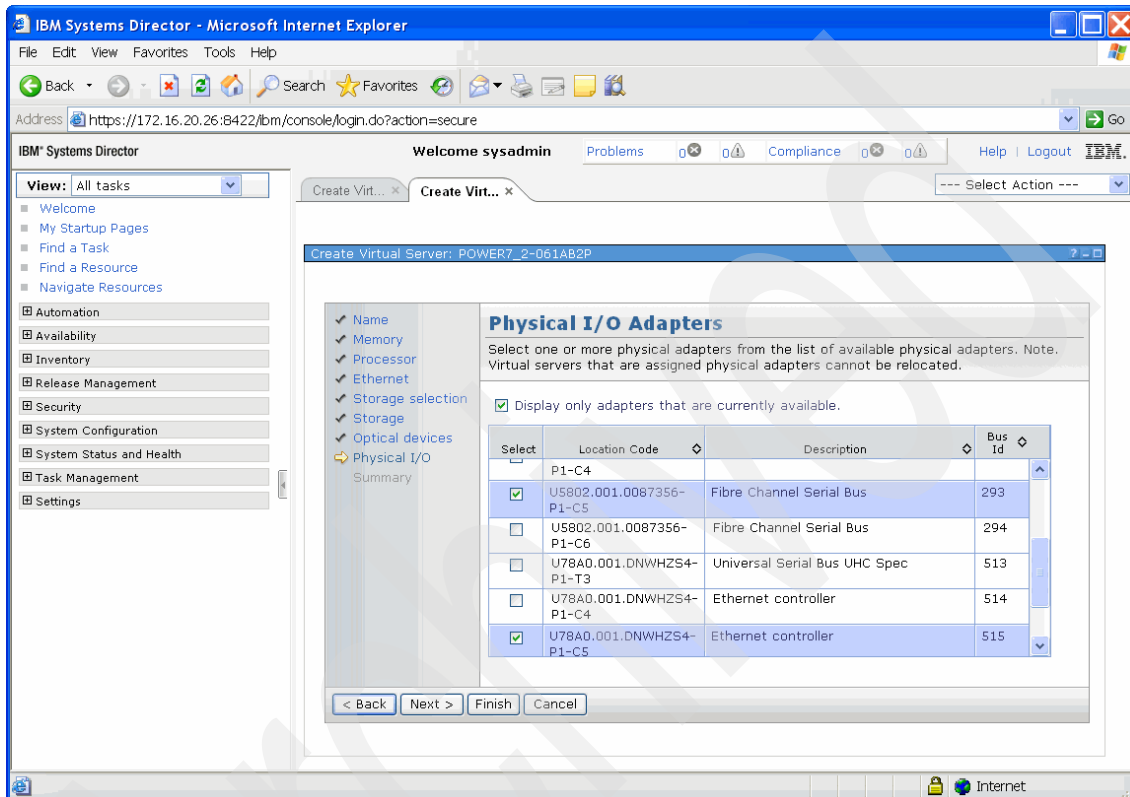


Figure 8-19 Create Virtual Server: Assign physical adapters

Command-line usage

You use the `mksyscfg` command to create Virtual Servers, just as you did on the Hardware Management Console. The syntax of the command has not changed, and it is called by appending the `smcli` command to the beginning of the command. Existing HMC scripts used to create Virtual Servers do not have to be modified the SDMC. Refer to 10.1.3, “Power Systems management commands” on page 280 for more information.

Example 8-1 is a sample command that is used to create an Virtual Server.

Example 8-1 Create Virtual Server using smcli mksyscfg

```
sysadmin@sdmca:~> smcli mksyscfg -r lpar -m POWER7_2-061AB2P -i  
name=myServer,profile_name=DefaultProfile,lpar_id=3,lpar_env=aixlinux,m  
in_mem=256,desired_mem=6144,max_mem=6144,mem_mode=ded,proc_mode=shared,  
min_proc_units=0.1,desired_proc_units=4.0,max_proc_units=4.0,min_procs=  
1,desired_procs=4,max_procs=4,"virtual_serial_adapters=0/server/1/any//  
any/1,1/server/1/any//any/1",virtual_scsi_adapters=4/client/1/P7_2_vios  
1/14/0,"virtual_eth_adapters=2/0/1//0/0/ETHERNET0//all/none,3/0/2//0/0/  
ETHERNET0//all/none"
```

8.2 Virtual Server activation

Before a newly created Virtual Server can be managed, it has to be activated. After the first activation, the properties of the Virtual Server can be changed.

To activate a Virtual Server, perform the following steps:

1. Right-click the server name and select **Operations** → **Activate** → **Profile** to activate the Virtual Server with a specific profile (Figure 8-20).

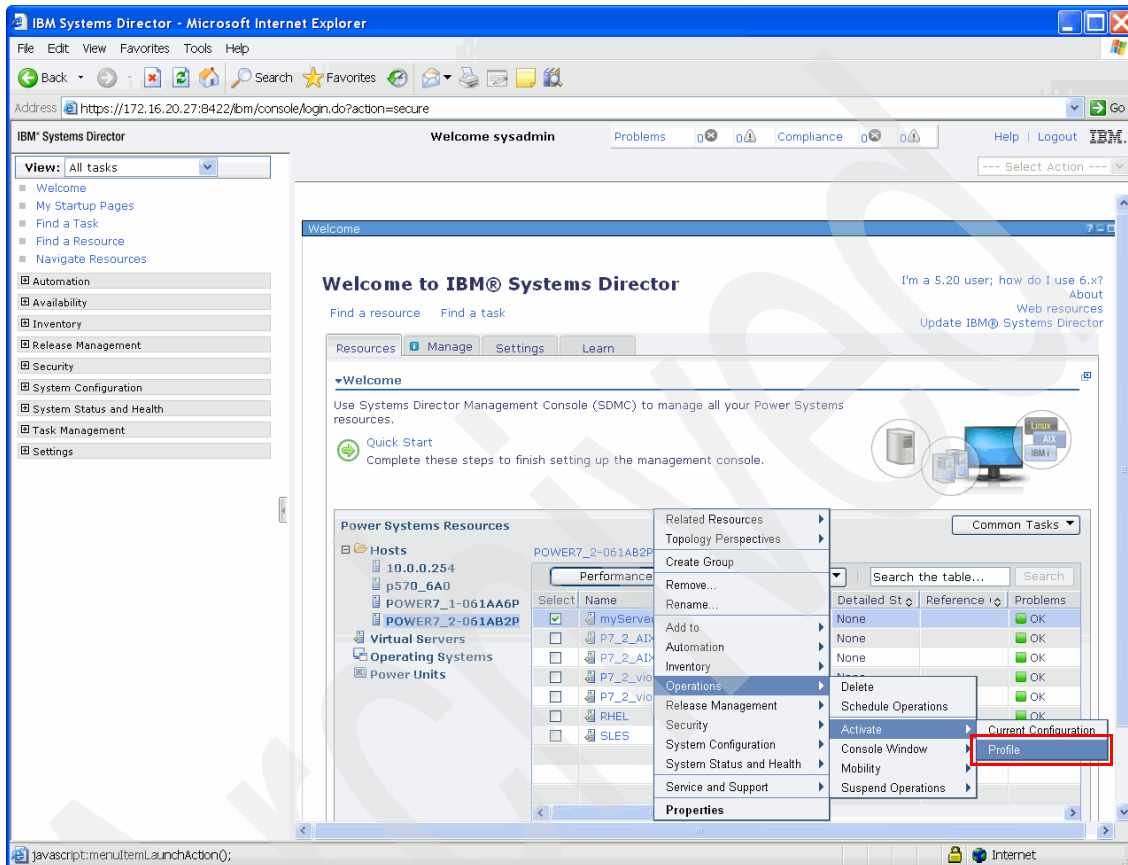


Figure 8-20 Activate Virtual Server: Profile option

2. Select a profile. In our example, we only have the default profile, which is called DefaultProfile (Figure 8-21).

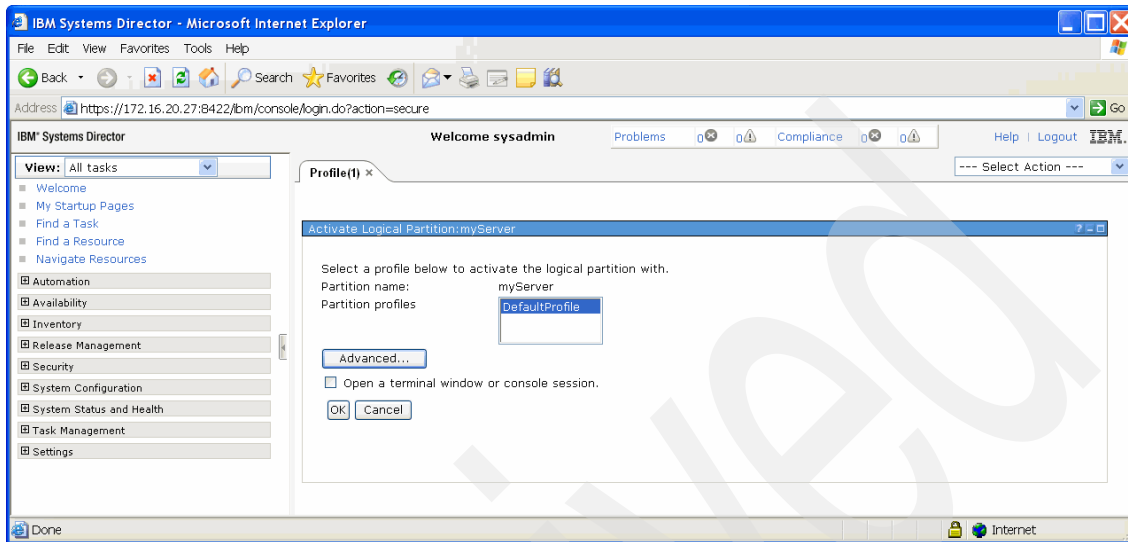


Figure 8-21 Activating Virtual Server: DefaultProfile selected

3. Click the **Advanced** tab and select the options for the keylock position and boot mode (Figure 8-22).

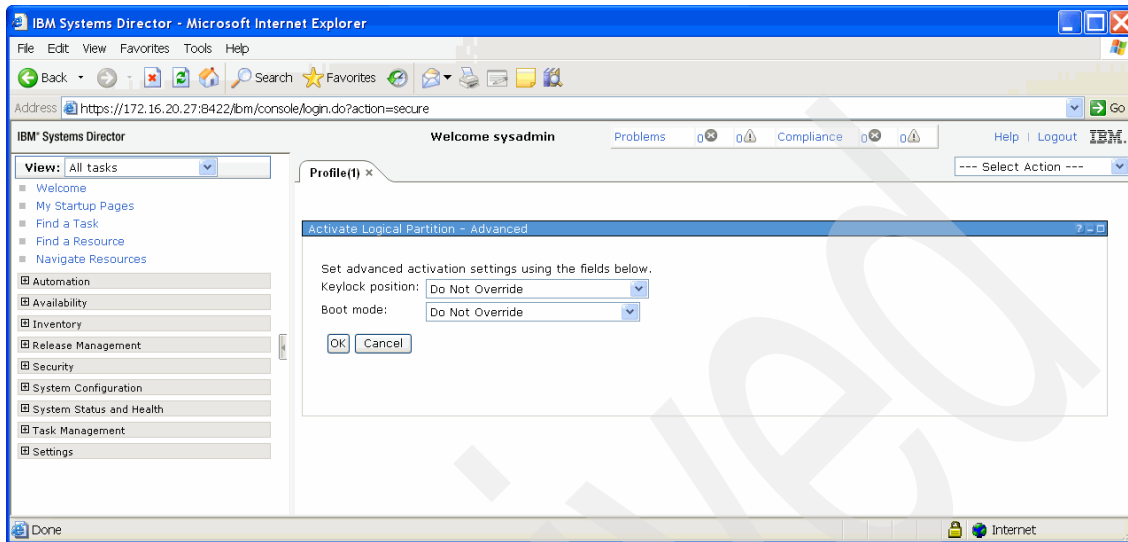


Figure 8-22 Activating Virtual Serve: Keylock position and boot mode

- The Welcome page opens and shows the state and detailed state of the Virtual Server (Figure 8-23).

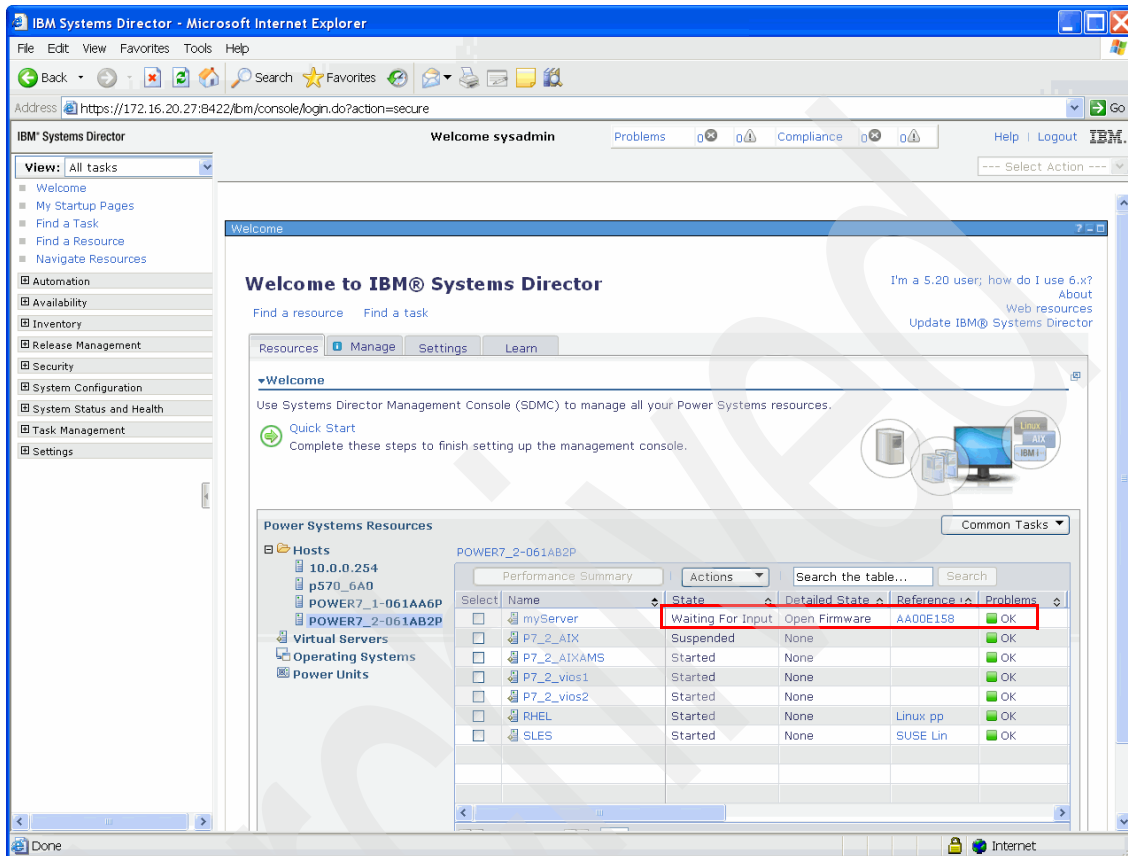


Figure 8-23 Welcome page: State and detailed state shown after activation

The `smcli chsysstate` command can be used to activate a Virtual Server (Example 8-2).

Example 8-2 Activate a Virtual Server using smcli chsysstate

```
sysadmin@sdmca:~> smcli chsysstate -r lpar -m POWER7_2-061AB2P -o on -f
DefaultProfile -n myServer
```

8.3 Virtual Server shutdown

To shut down a Virtual Server, navigate to the Welcome page, right-click the name of the Virtual Server, and select **Operations** → **Shutdown** (Figure 8-24).

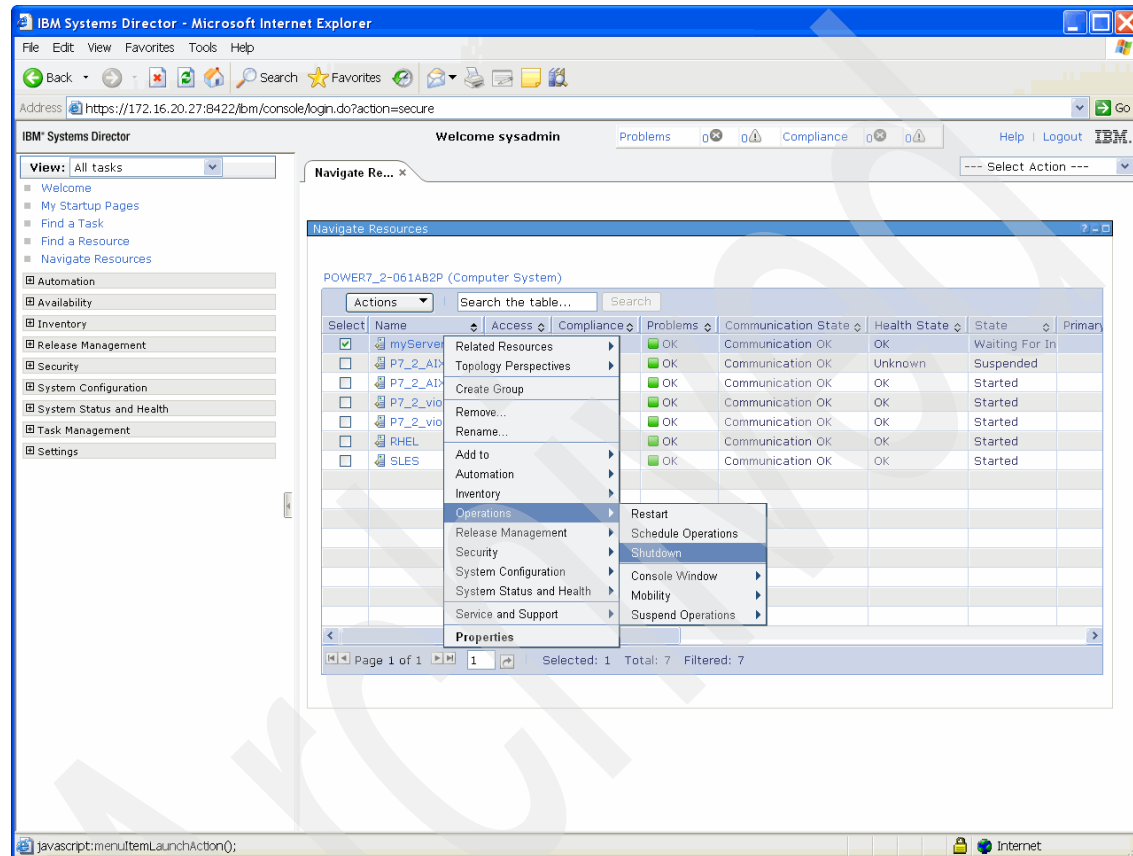


Figure 8-24 Shut down a Virtual Server

The next page (Figure 8-25) shows the available options for shutting down the operations as either Delayed or Immediate. If you click **Immediate**, you will be asked if a battery is exchanged. If not, click **No**.

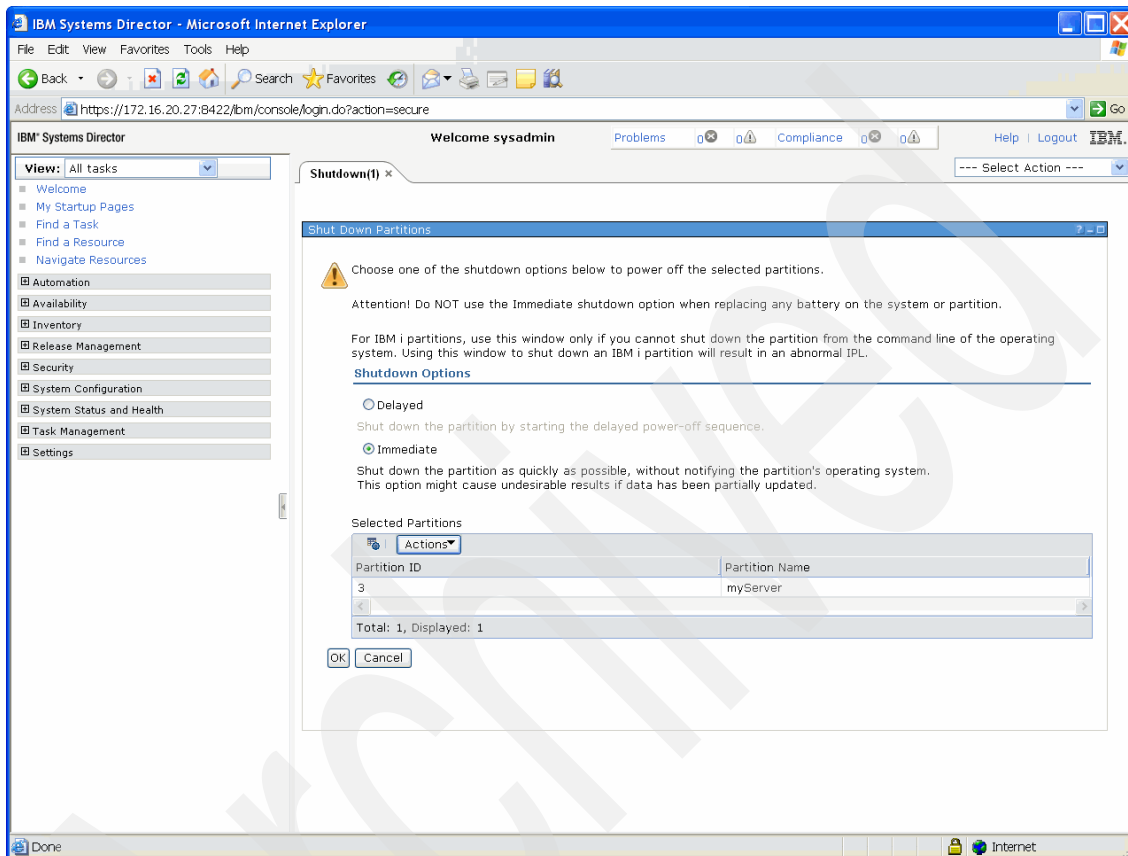


Figure 8-25 Shutdown options

If you choose to use the command line to shut down the Virtual Server, use the command shown in Example 8-3.

Example 8-3 Shutting down a Virtual Server using smcli chsysstate

```
sysadmin@sdmca:~> smcli chsysstate -r lpar -m POWER7_2-061AB2P -o
shutdown --immed -n myServer
```


8.4 Virtual Server management

The Manage Virtual Server menu option in the Welcome page allows you to customize existing Virtual Servers. In this page, most of the settings previously available in different menus on the Hardware Management Console have been consolidated here. Usage improvements allow for easier navigation and handling of tasks related to Virtual Server management. Because the Systems Director Management Console interface is context sensitive, the available options depend on the state of the Virtual Server.

After creating the Virtual Server, it must be activated to manage it. The Virtual Server is then ready to be managed by the Manage Virtual Server option.

To manage the Virtual Server, navigate to the Welcome page, right-click the name of the Virtual Server, and select **System Configuration** → **Manage Virtual Server** (Figure 8-26).

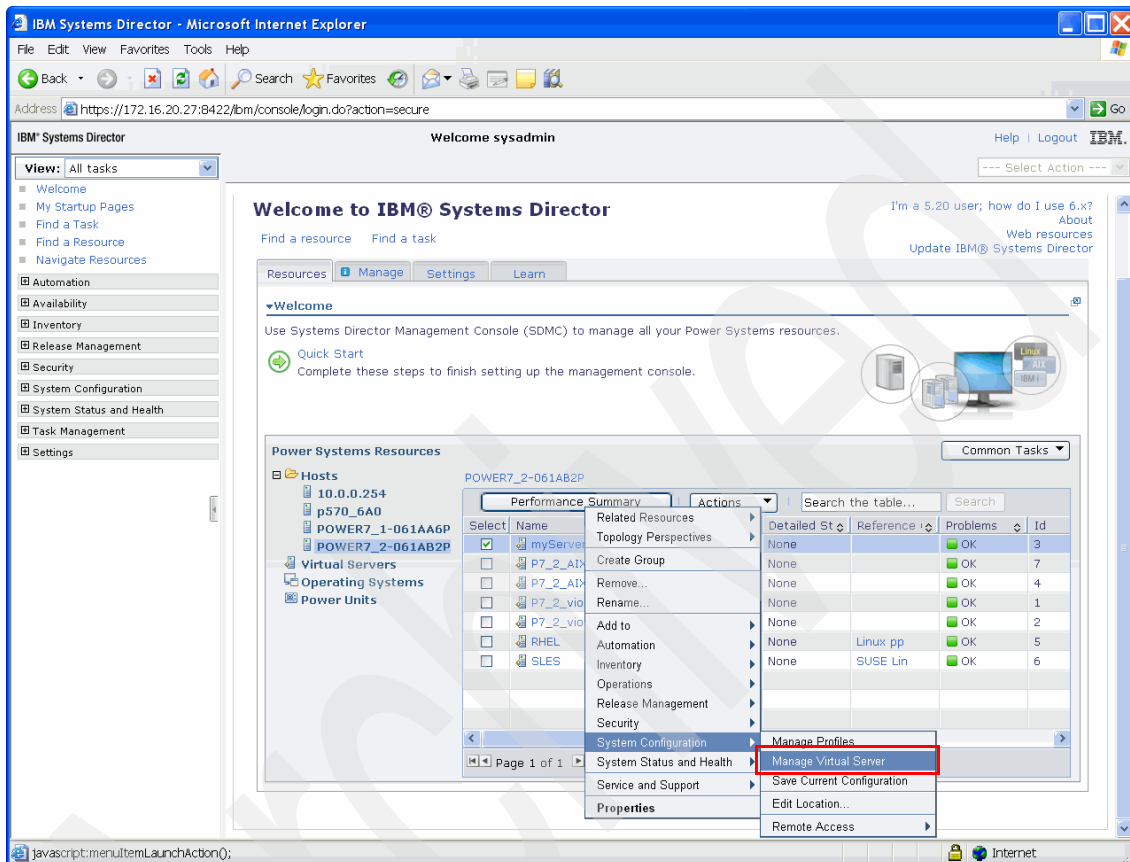


Figure 8-26 Manage Virtual Server menu entry

The page with the General Settings tab opens (Figure 8-27). The settings that can be changed here are shown in boxes, either for text fields or as clickable fields; non-changeable settings appear as text.

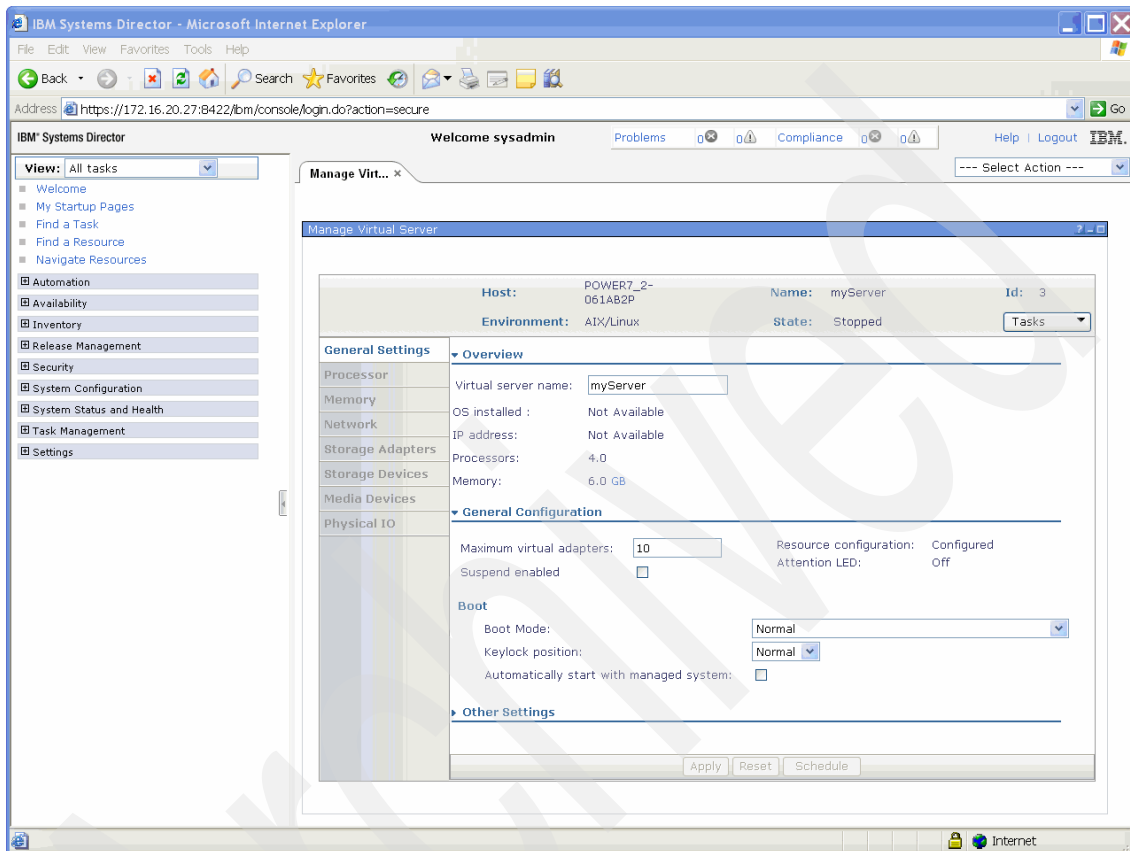


Figure 8-27 Manage Virtual Server: General Settings

Note: The Apply, Reset, and Schedule buttons at the bottom of the page are disabled. These buttons are only activated after you make a change to the displayed settings. If a drop-down menu is changed, the new value of that box is shown in blue. Changes to check boxes and text fields are marked by an asterisk next to the value description.

The Tasks button (Figure 8-28) allows you to execute the following tasks directly from the Manage Virtual Server page:

- ▶ Activate Current Configuration
- ▶ Activate Profile
- ▶ Console page (open and close Console page)
- ▶ List scheduled jobs
- ▶ Mobility (Migrate, Validate, and Recover)
- ▶ Reference Code History
- ▶ Save Current Configuration

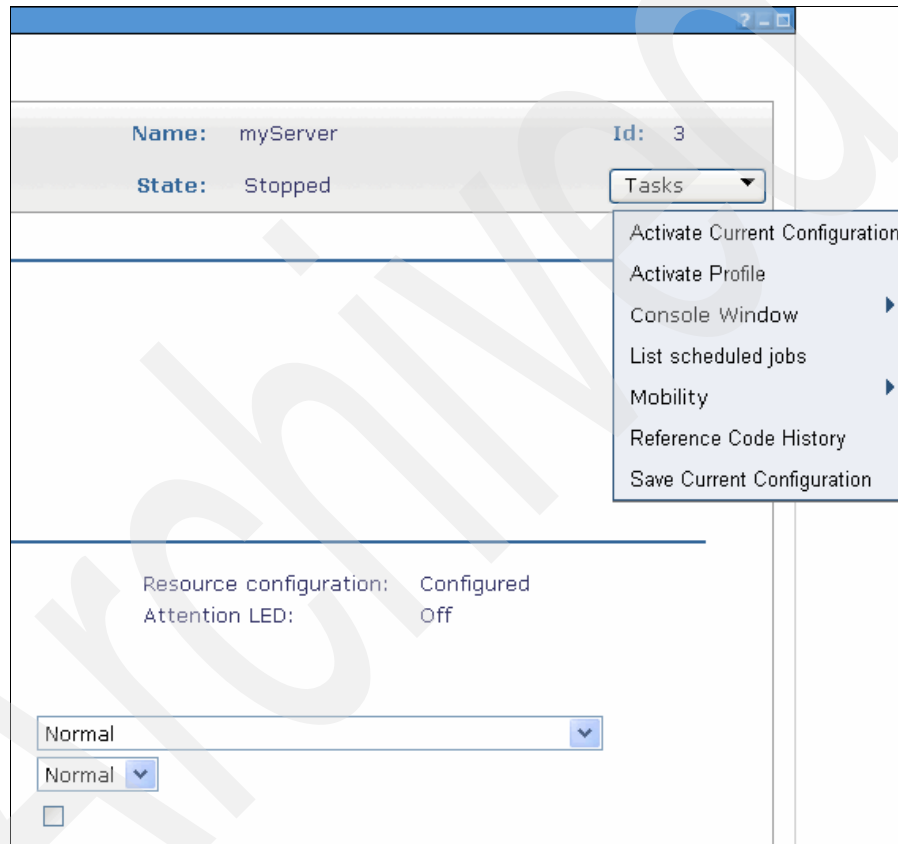


Figure 8-28 Tasks button in General Settings tab

The **Processor** page allows you to change the processor related settings of the Virtual Server, including the processor compatibility mode (Figure 8-29).

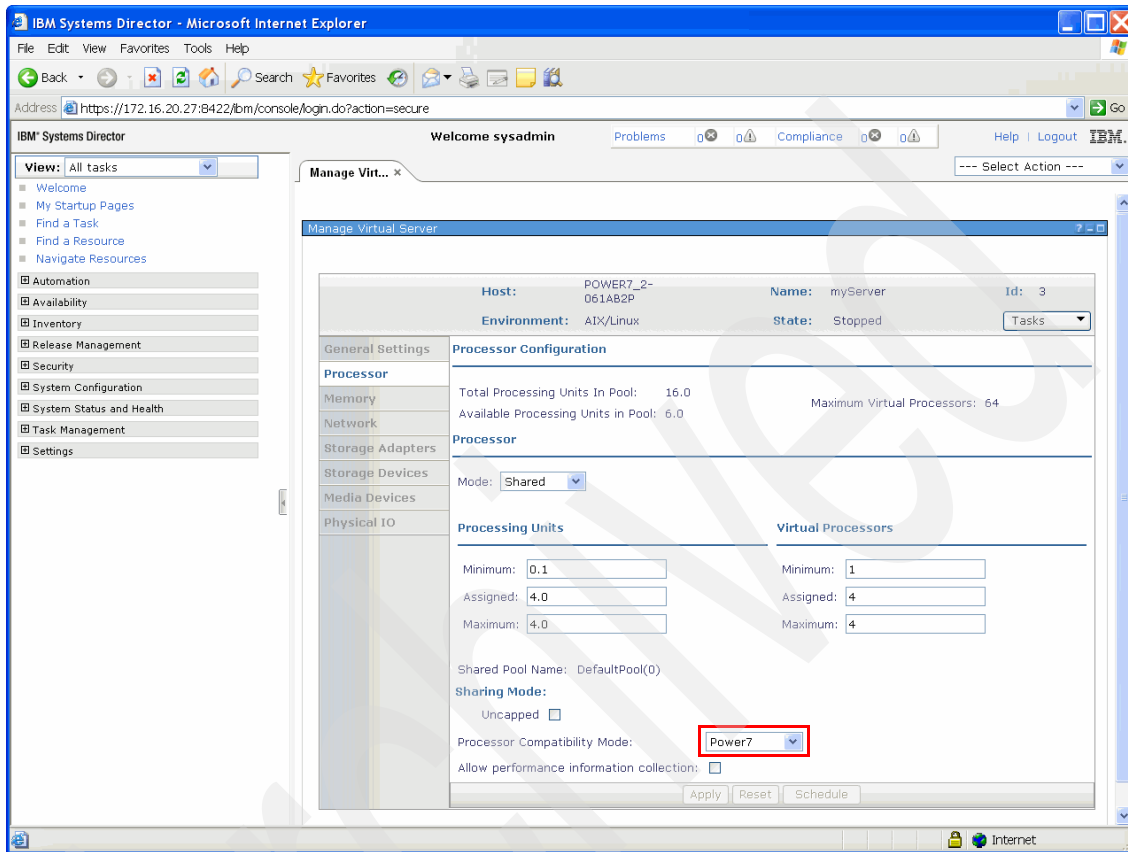


Figure 8-29 Manage Virtual Server: Processor tab

Note the blue values in the drop-down menu and the changed appearance of the buttons at the bottom of the page (Figure 8-30). In this case, the processor mode is set to Dedicated and the appropriate values for the Shared Processor mode are not shown anymore.

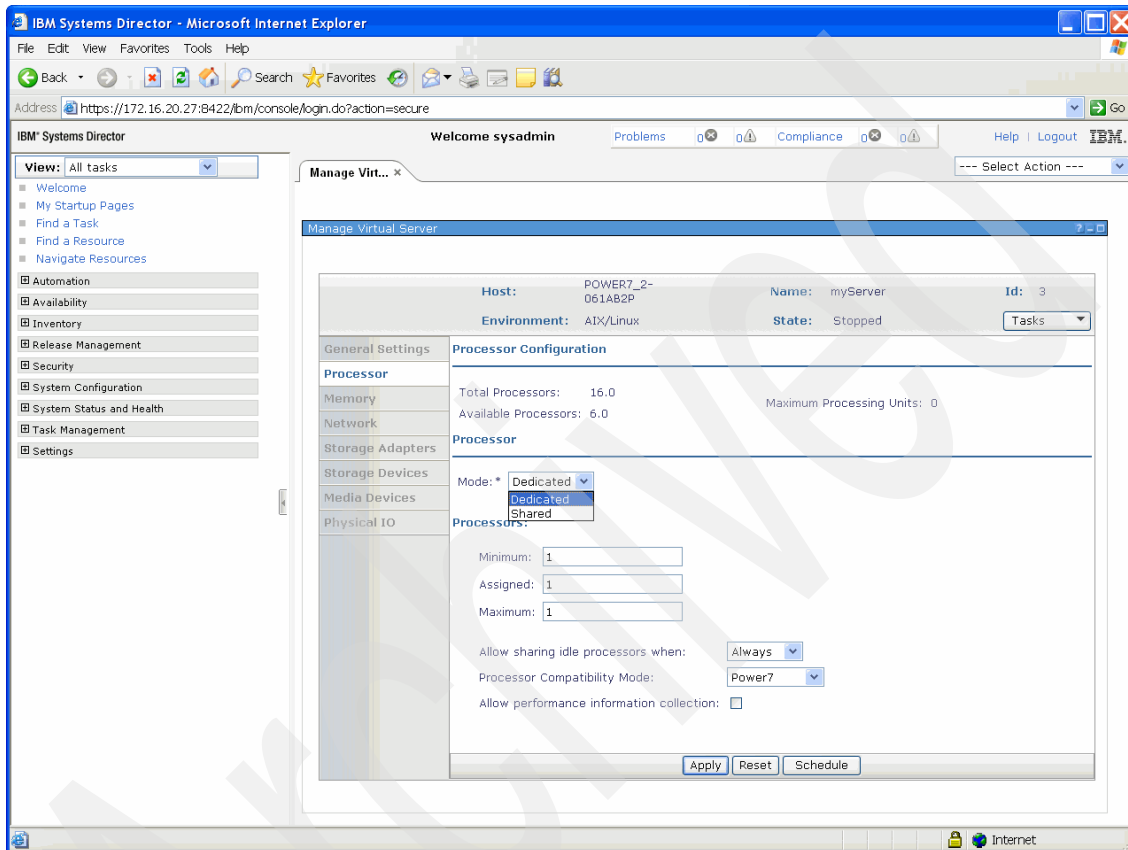


Figure 8-30 Manage Virtual Server: Dedicated processor mode

The default memory mode for Virtual Servers is Dedicated and Active Memory Expansion (AME) is enabled by default with an expansion factor of 1.0 (Figure 8-31). This mode enables the setting to be put into effect without requiring a reboot, should you need to use AME later.

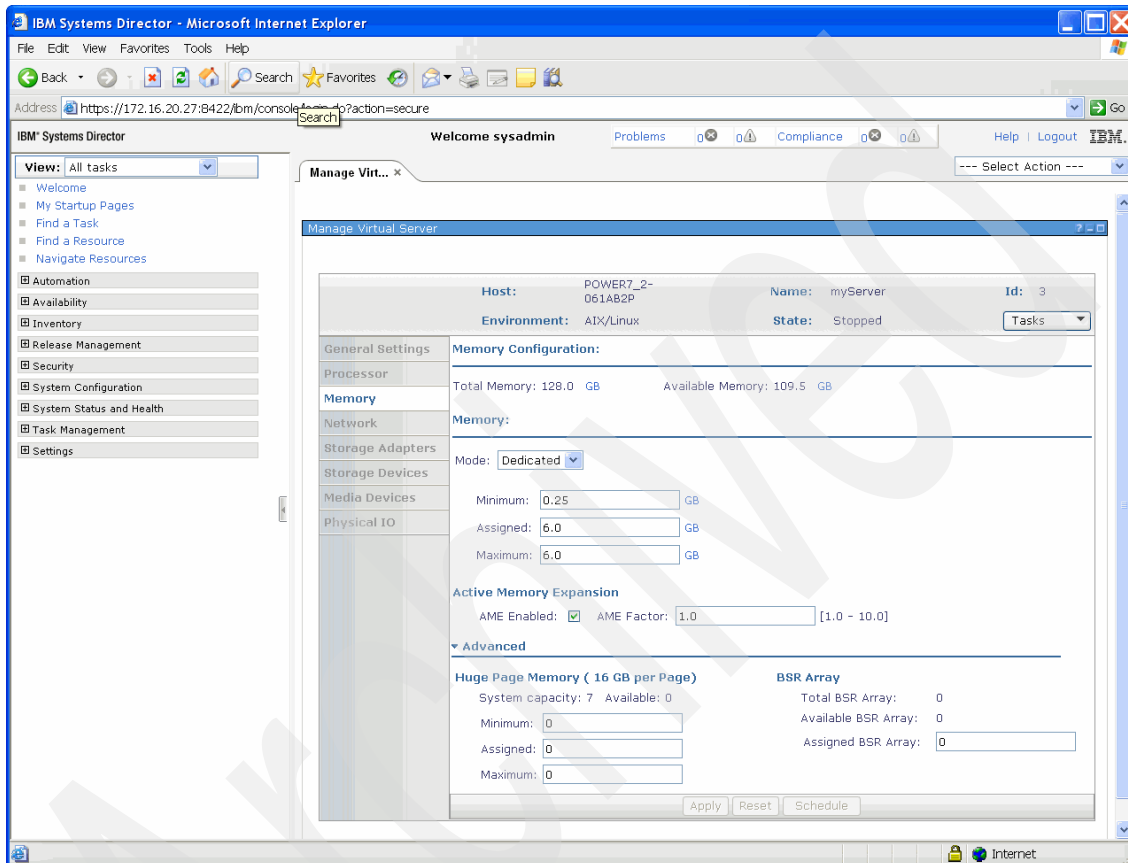


Figure 8-31 Manage Virtual Server: Dedicated memory settings

If the memory mode is set to Shared, as shown in Figure 8-32, Advanced Memory Sharing (AMS) has to be active, as it is a PowerVM Enterprise feature and the Virtual I/O Server(s) must be configured for AMS beforehand.

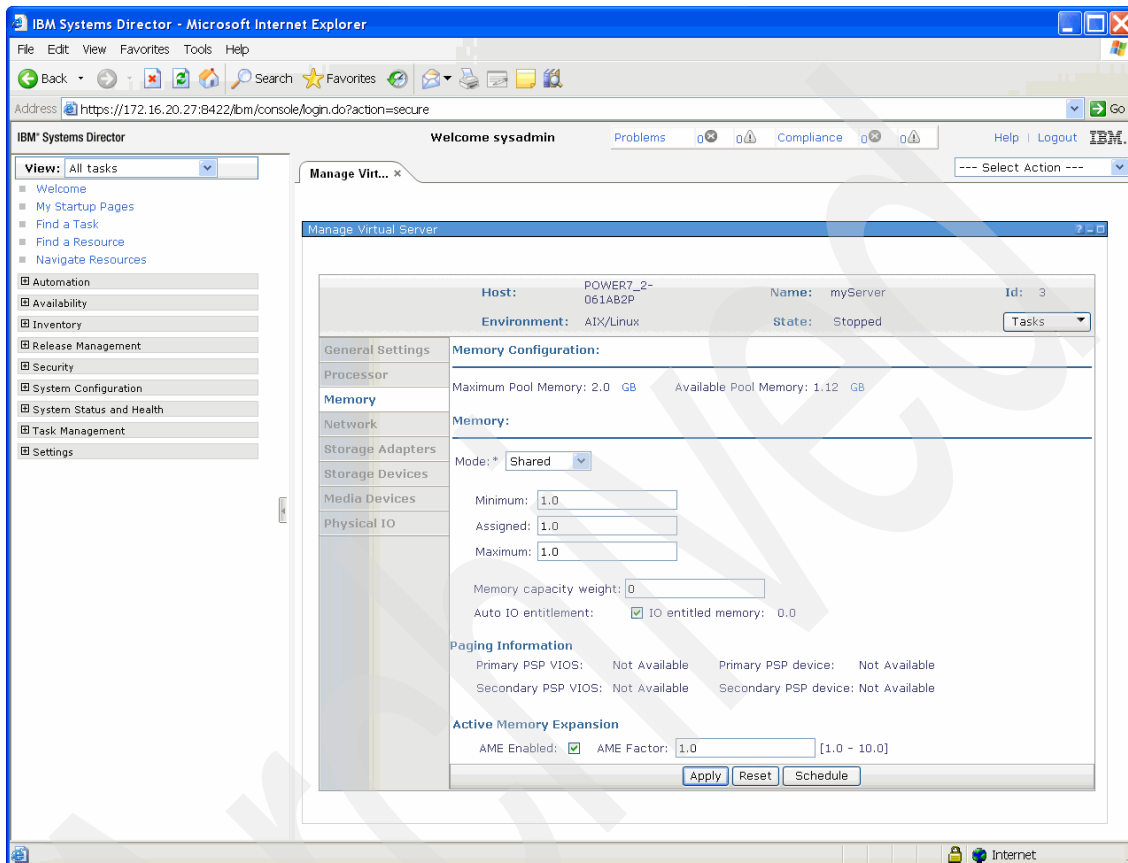


Figure 8-32 Manage Virtual Server: Shared memory settings

On the following Network tab (Figure 8-33), you can configure virtual network adapters for the Virtual Server. You can also add ports to the Logical Host Ethernet Adapter by clicking the **Add** button.

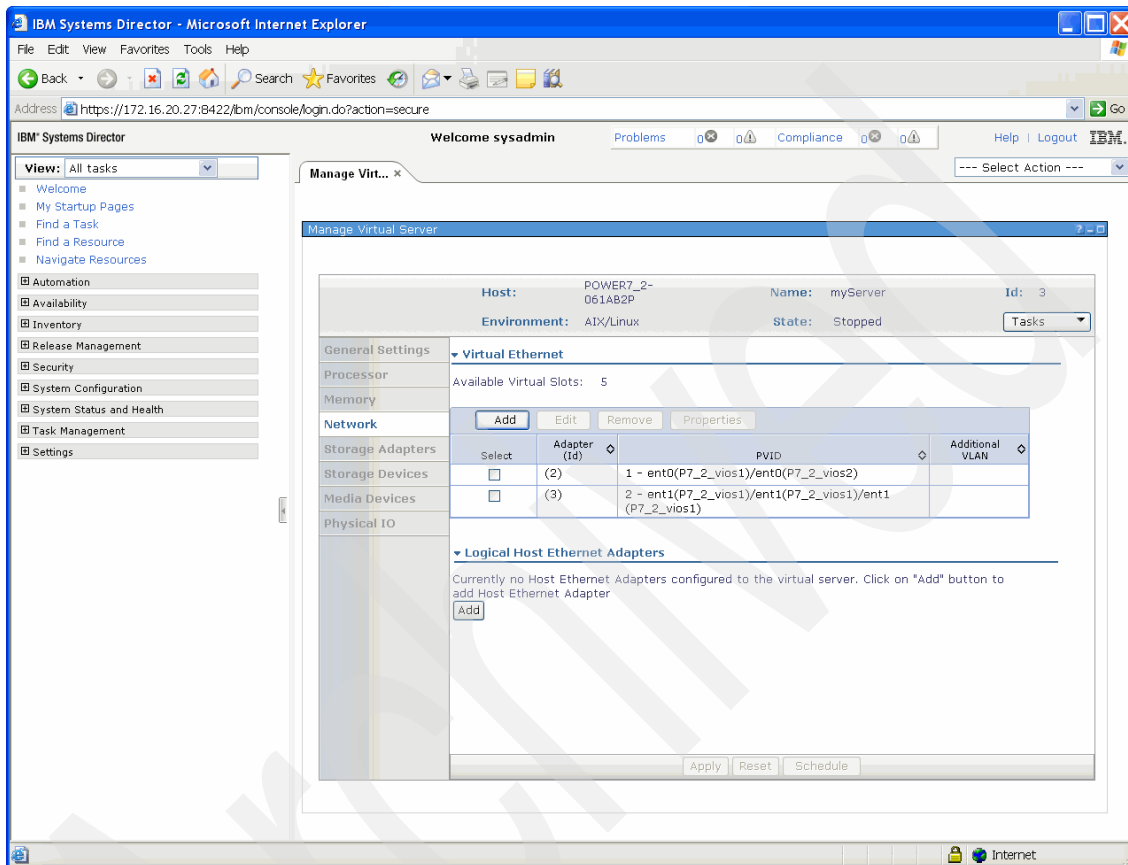


Figure 8-33 Manage Virtual Server: Network page

If the check box right to the virtual network adapter is checked, the Edit button becomes active. Click **Edit** to change the properties of that network adapter (Figure 8-34). Although not shown here, in the Advanced Virtual Ethernet Configuration section, the following settings can be changed:

- ▶ MAC address
- ▶ Quality of service
- ▶ MAC address restrictions

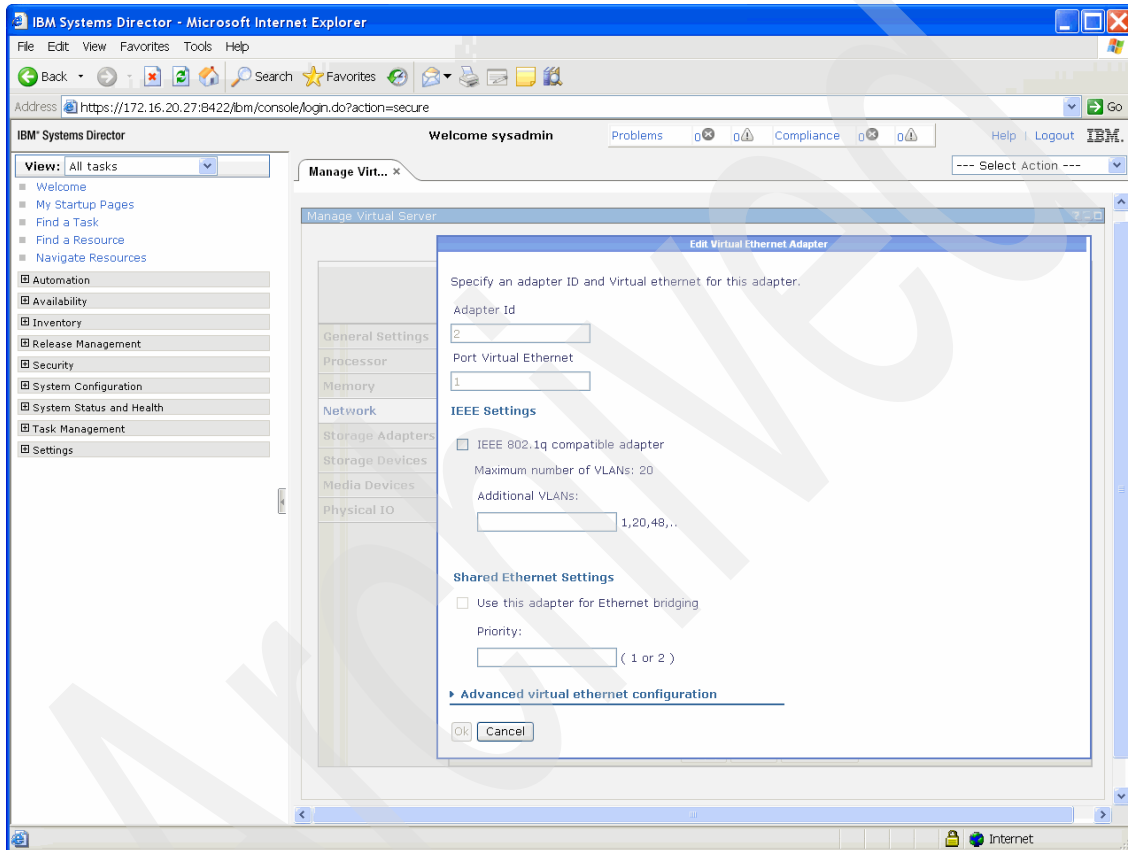


Figure 8-34 Manage Virtual Server: Edit Virtual Ethernet Adapter

On the Storage Adapters page (Figure 8-35), you can removed existing storage adapters if you check the check box and click **Remove**.

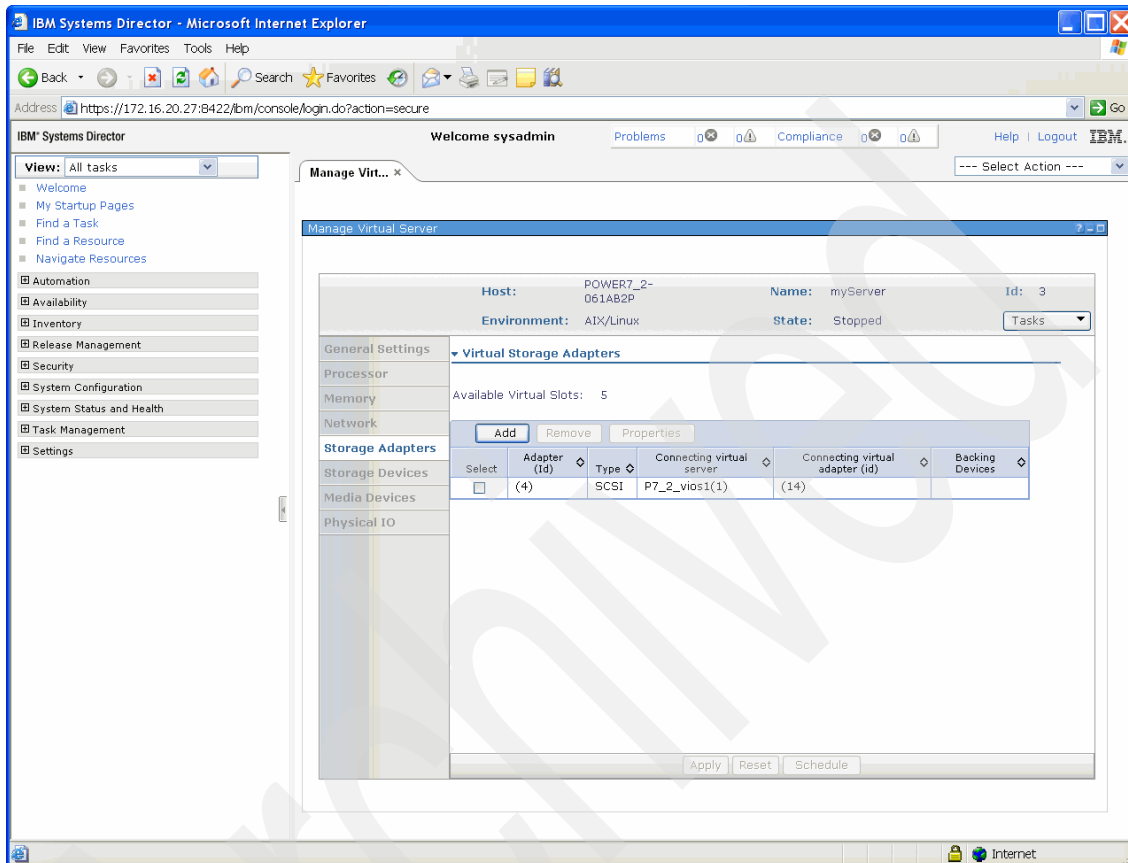


Figure 8-35 Manage Virtual Server: Add Virtual Storage Adapter

To add an storage adapter, click the **Add** button (Figure 8-35 on page 169) and enter the desired values for this adapter. A virtual SCSI adapter is added in Figure 8-36.

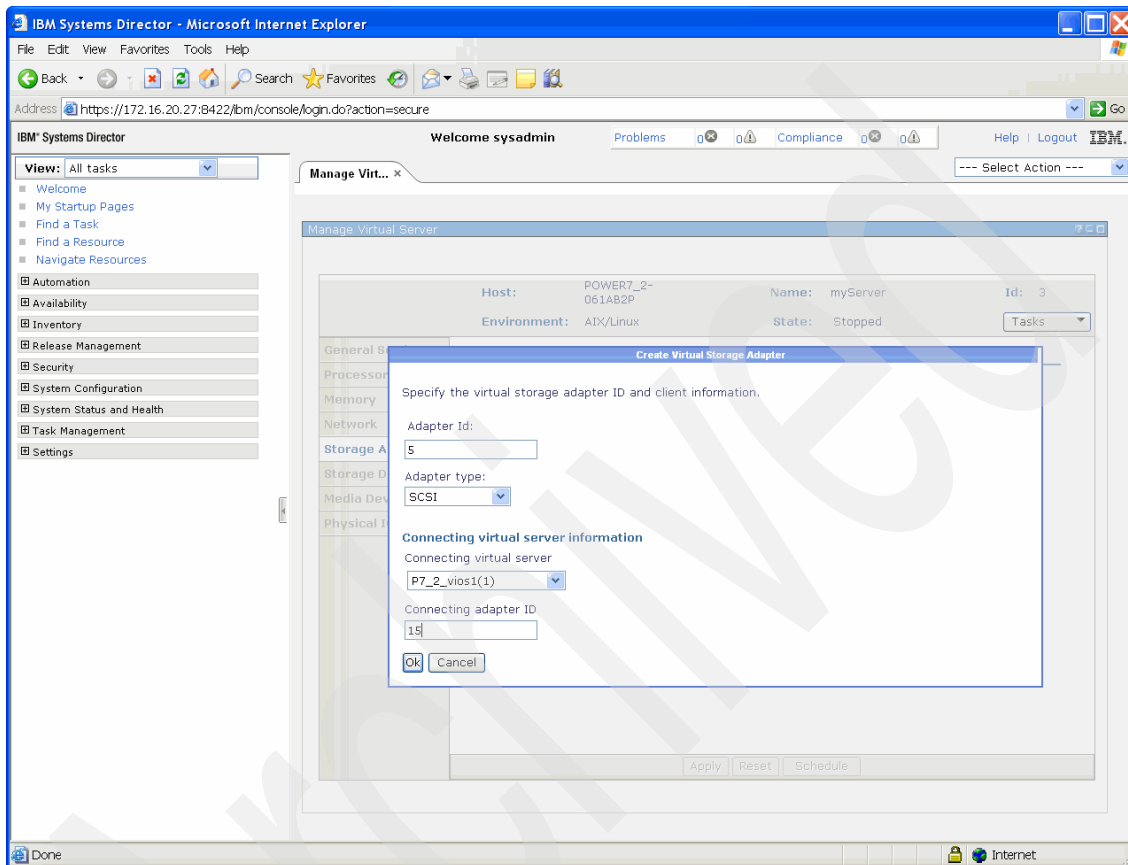


Figure 8-36 Manage Virtual Server: Create Virtual SCSI Storage Adapter

If you chose to add a Virtual Fibre Channel adapter, the page shown in Figure 8-37 opens. Note that the World Wide Port Names for that adapter are generated automatically, but can be changed later by running the **smcli chsyscfg** command. Remember that the **Apply** button has to be clicked to actually execute the operation.

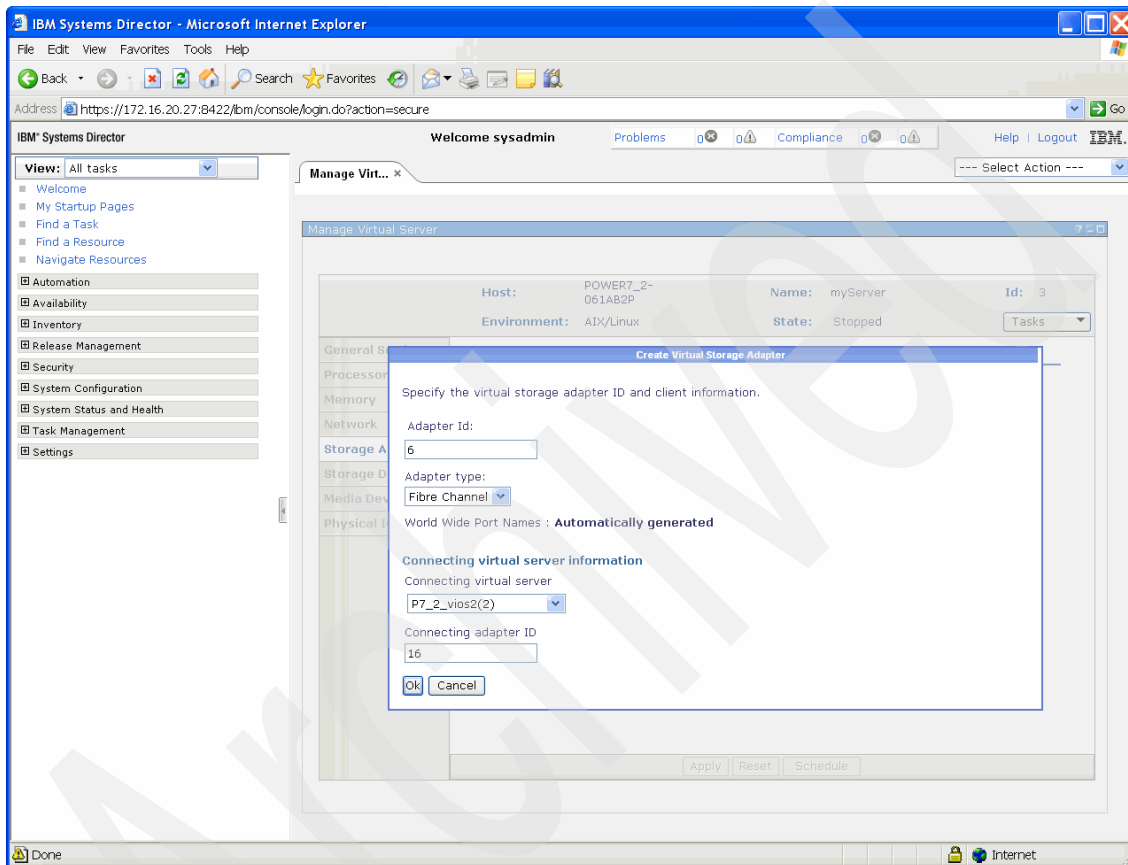


Figure 8-37 Manage Virtual Server: Create Virtual FC Storage Adapter

On the Storage Devices page (Figure 8-38), three types of storage devices can be added:

Virtual Disks These disks have to be created on the Virtual I/O Server beforehand to be available in the dialogue.

Physical Volumes Physical Volumes have to be assigned to the Virtual I/O server beforehand and are available for selection, as shown in Figure 8-39 on page 173.

Fibre Channel To add new virtual Fibre Channel adapters to the Virtual Server, click the **Add** button. An Add Fibre Channel Adapter menu appears and lists the physical Fibre Channel adapters on the Virtual I/O server(s) that re available for mapping with the newly created Virtual Fibre Channel adapter (Figure 8-40 on page 174).

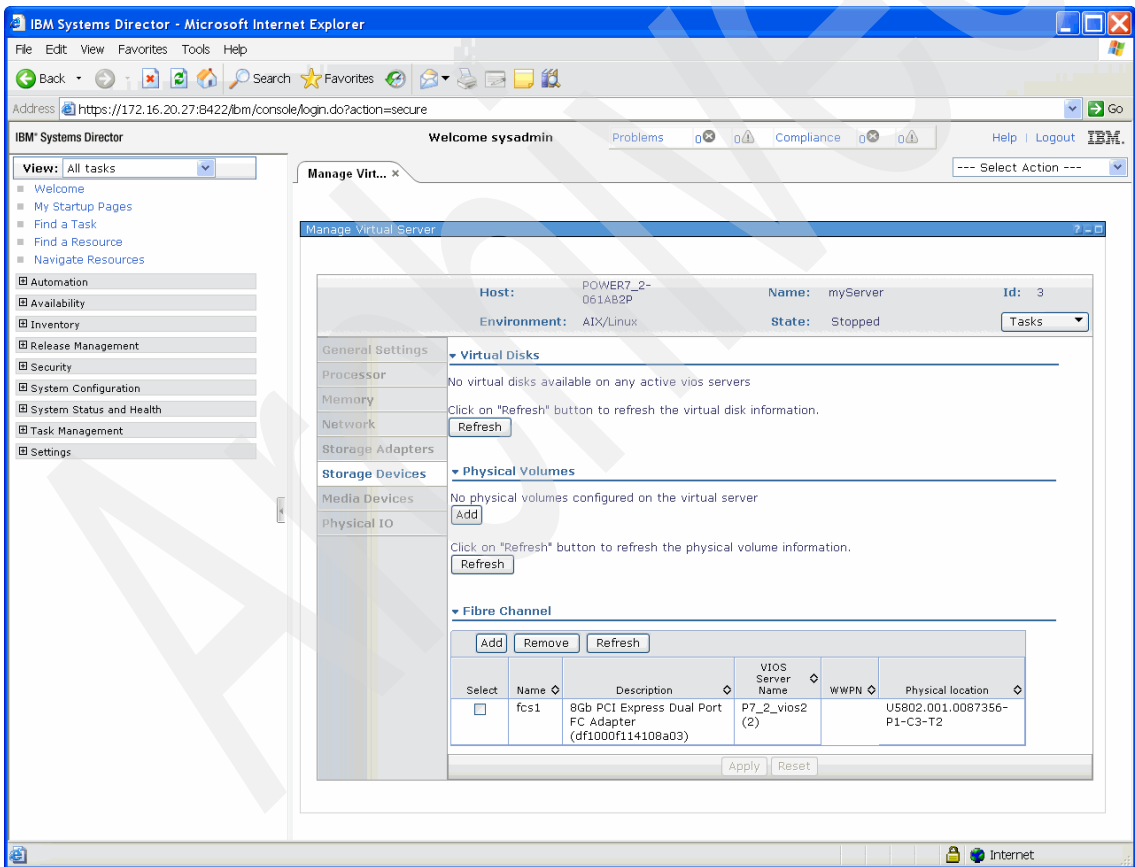


Figure 8-38 Manage Virtual Server: Storage Devices

Figure 8-39 shows the available physical volumes on the Virtual I/O servers. We select hdisk8 on the second Virtual I/O server, P7_2_vios2(2).

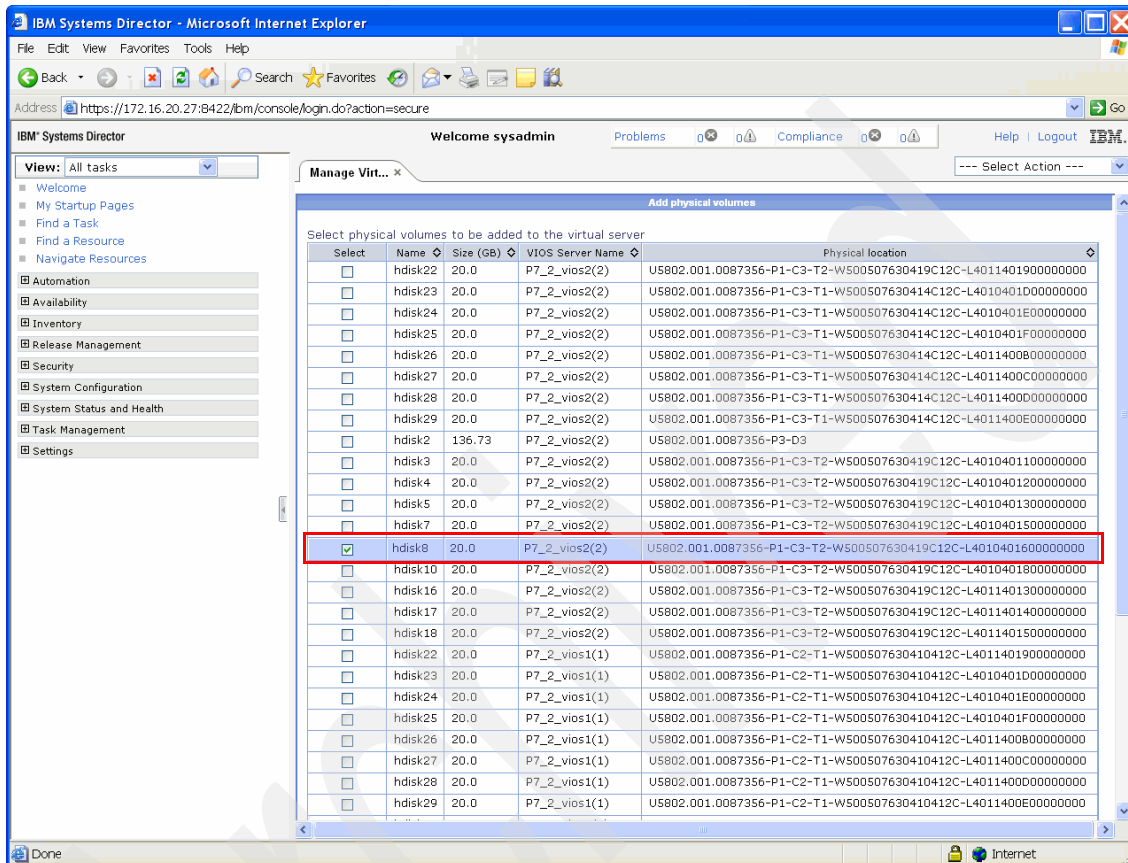


Figure 8-39 Manage Virtual Server: Add Physical Volume

The Add Fibre Channel menu allows you to add additional Virtual Fibre Channel adapters. Because no more than one Virtual Fibre Channel adapter per physical Fibre Channel adapter per Virtual Server is supported and one Virtual Fibre Channel adapter already had been created for this Virtual Server, only three physical Fibre Channel adapters are available for mapping (Figure 8-40).

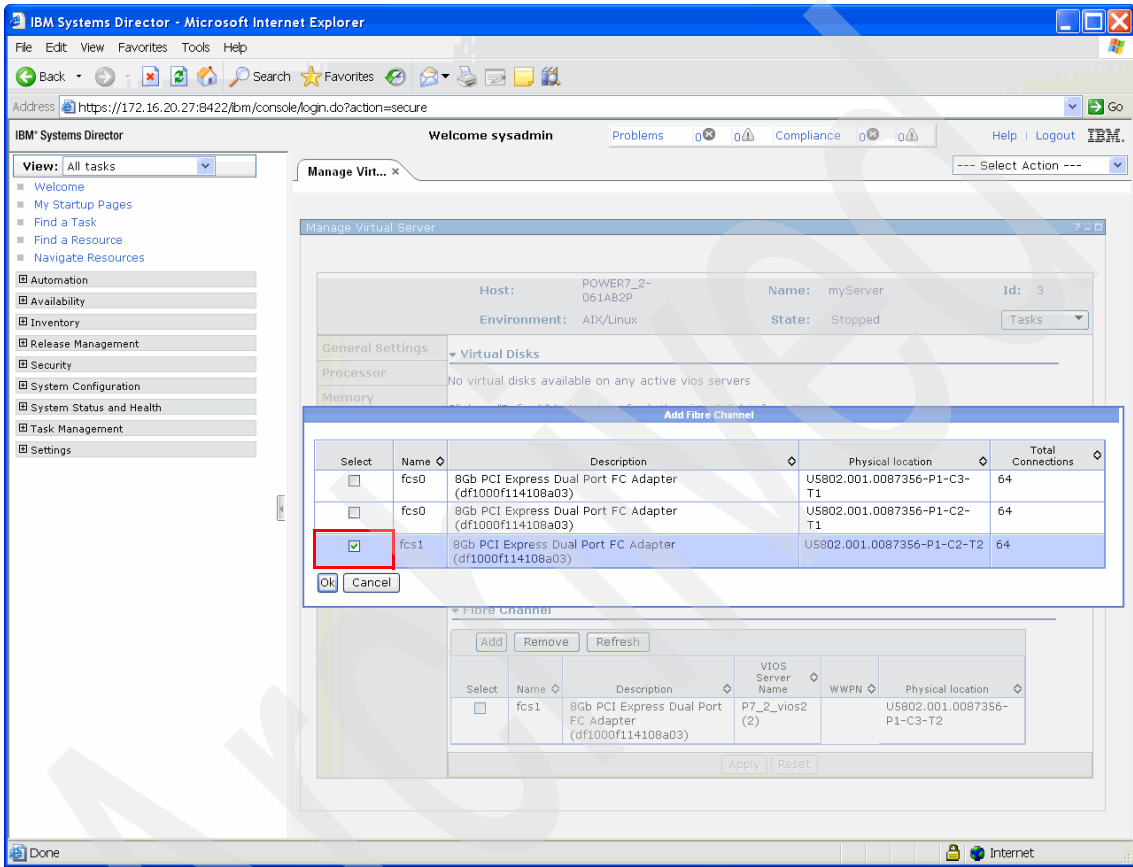


Figure 8-40 Manage Virtual Server: Add Fibre Channel

The Media Devices page lets you add media devices to the Virtual Server, that is optical devices, such as CD or DVD drives that are connected to the Virtual I/O Servers. Virtual Media refers to the Virtual Media Library on the Virtual I/O Server that is created and filled with images of CDs or DVDs that then can be made available to Virtual Servers. Figure 8-41 shows the initial Media Devices page.

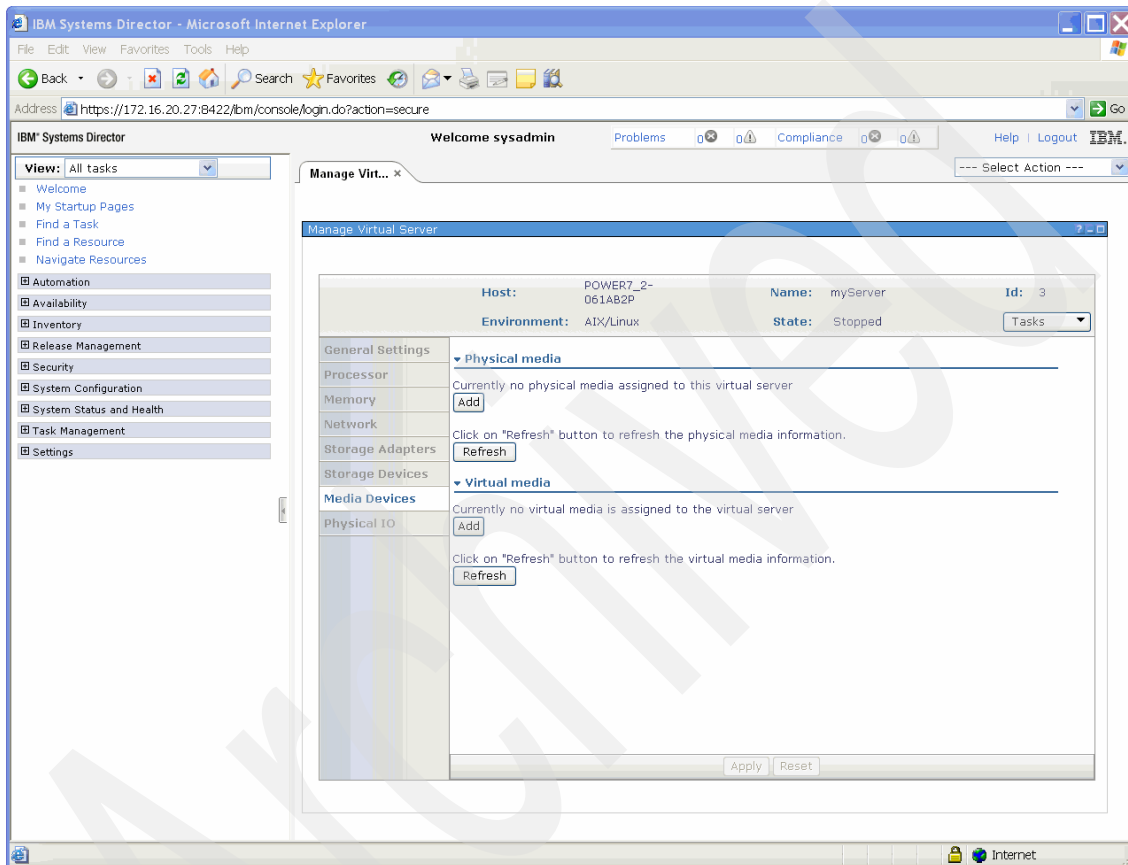


Figure 8-41 Manage Virtual Server: Media Devices page

Figure 8-42 shows the available Physical Media devices. Click the **OK** button to add the device to the Virtual Server.

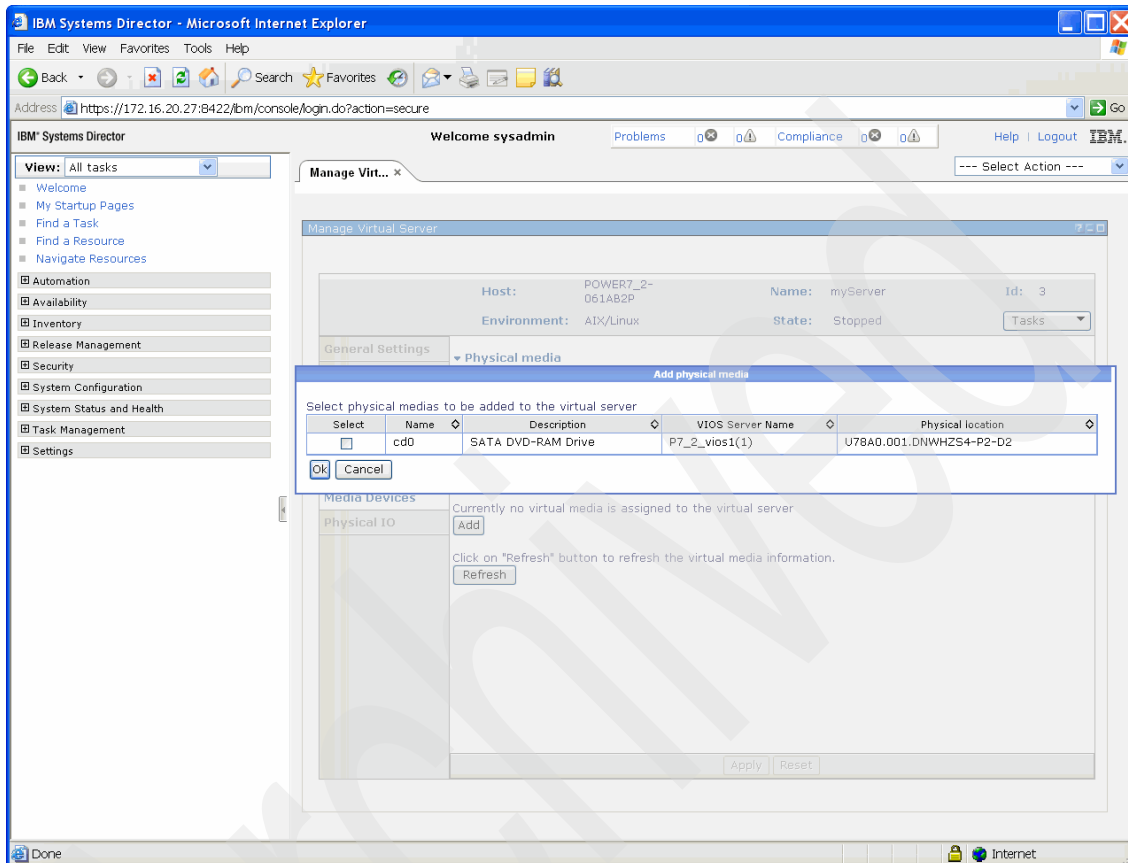


Figure 8-42 Manage Virtual Server: Add Physical Media

Clicking **Add** in the Virtual Media section of the Media Devices page opens a list of the available virtual media in the Virtual Media Library of the Virtual I/O Server (Figure 8-43).

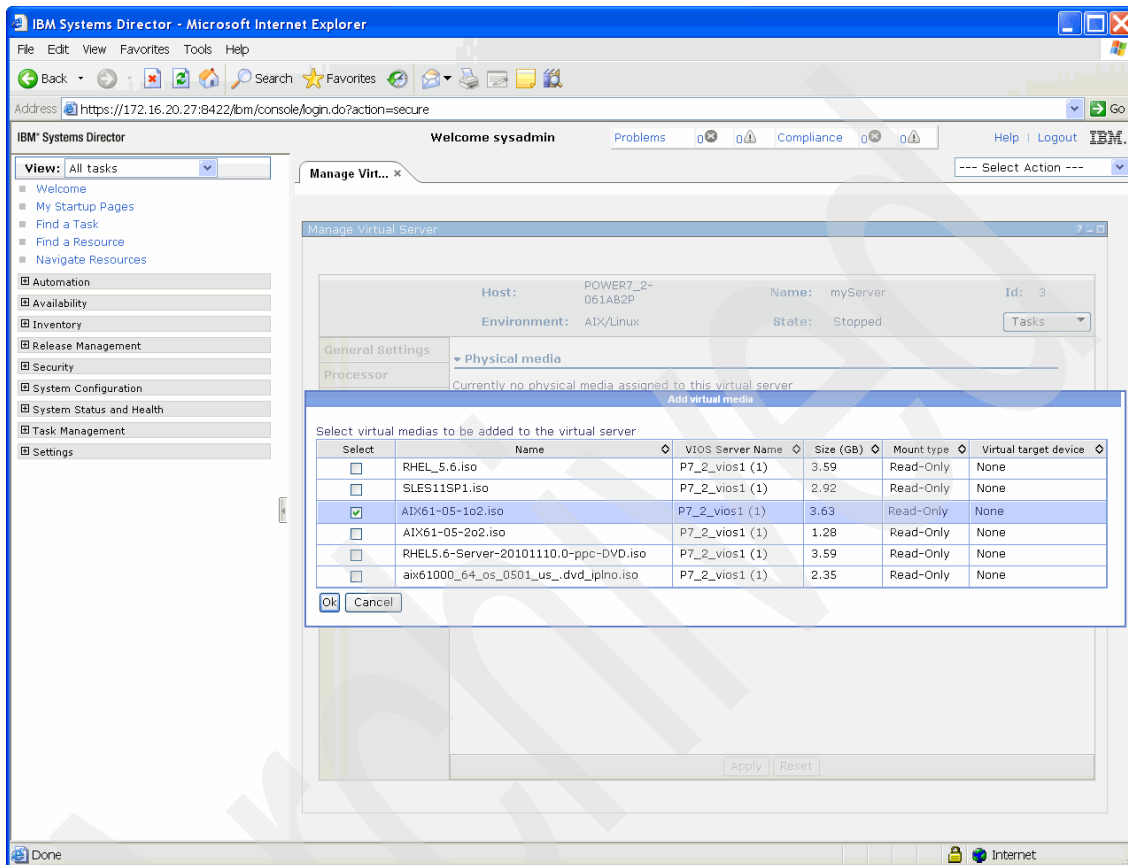


Figure 8-43 Manage Virtual Server: Adding virtual media

The task in Figure 8-43 on page 177 creates a Virtual Optical device adapter that is called a *Virtual Media Device*. After creating the Virtual Media Device, clicking **Modify** opens a page where the media inserted into the Virtual Media device can be changed (Figure 8-44).

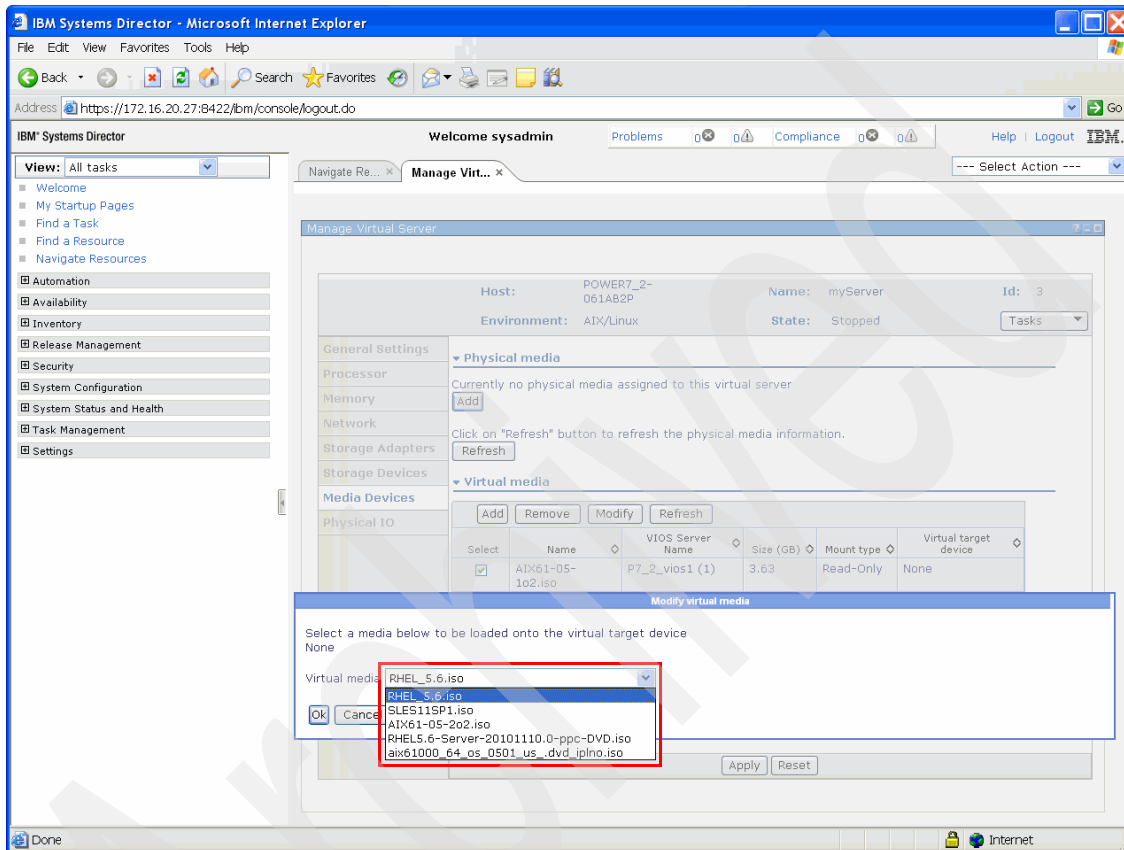


Figure 8-44 Manage Virtual Server: Modify virtual media

The last page in Manage Virtual Servers (Figure 8-45) allows you to add physical adapters to the Virtual Server.

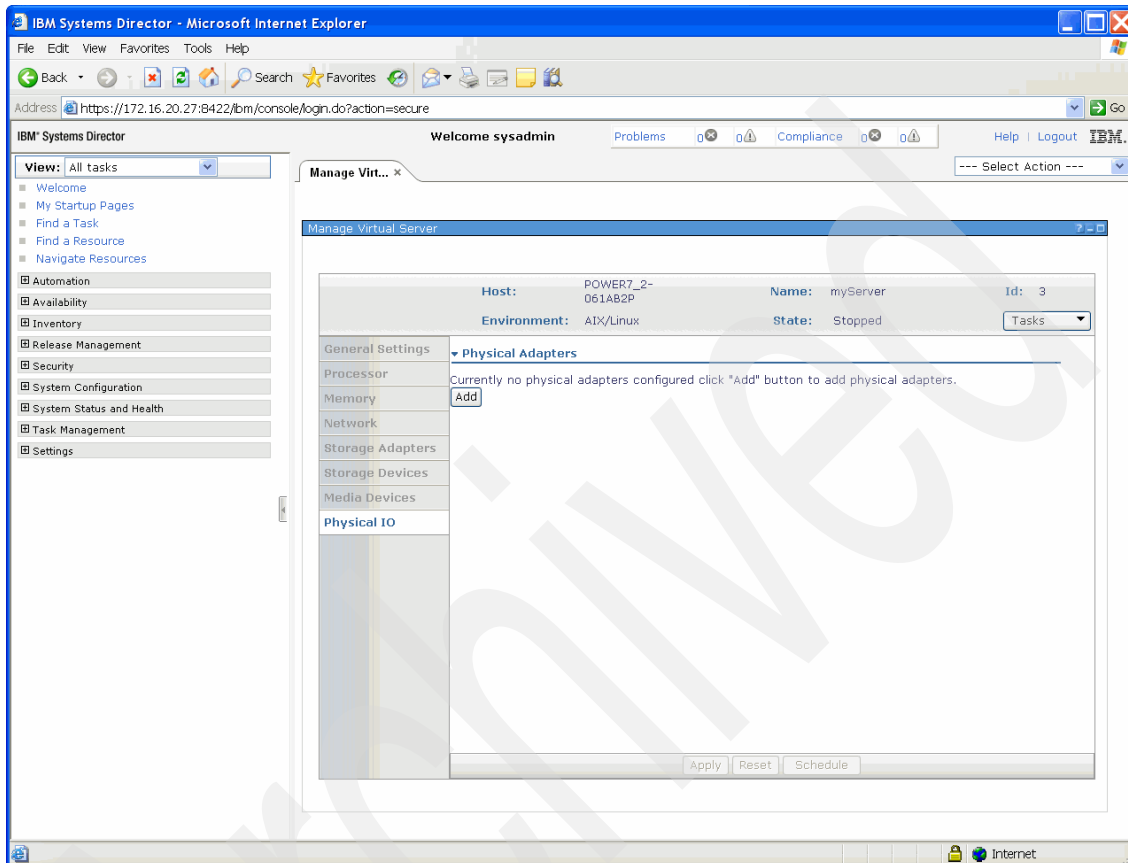


Figure 8-45 Manage Virtual Server: Physical Adapters

If you click the **Add** button, the list of physical adapters on the server appears (Figure 8-46). The **Display only available physical adapters** check box is checked, excluding adapters that are already assigned to a Virtual Server, which reduces the risk of accidentally assigning a physical adapter that is already being used by another Virtual Server to this Virtual Server.

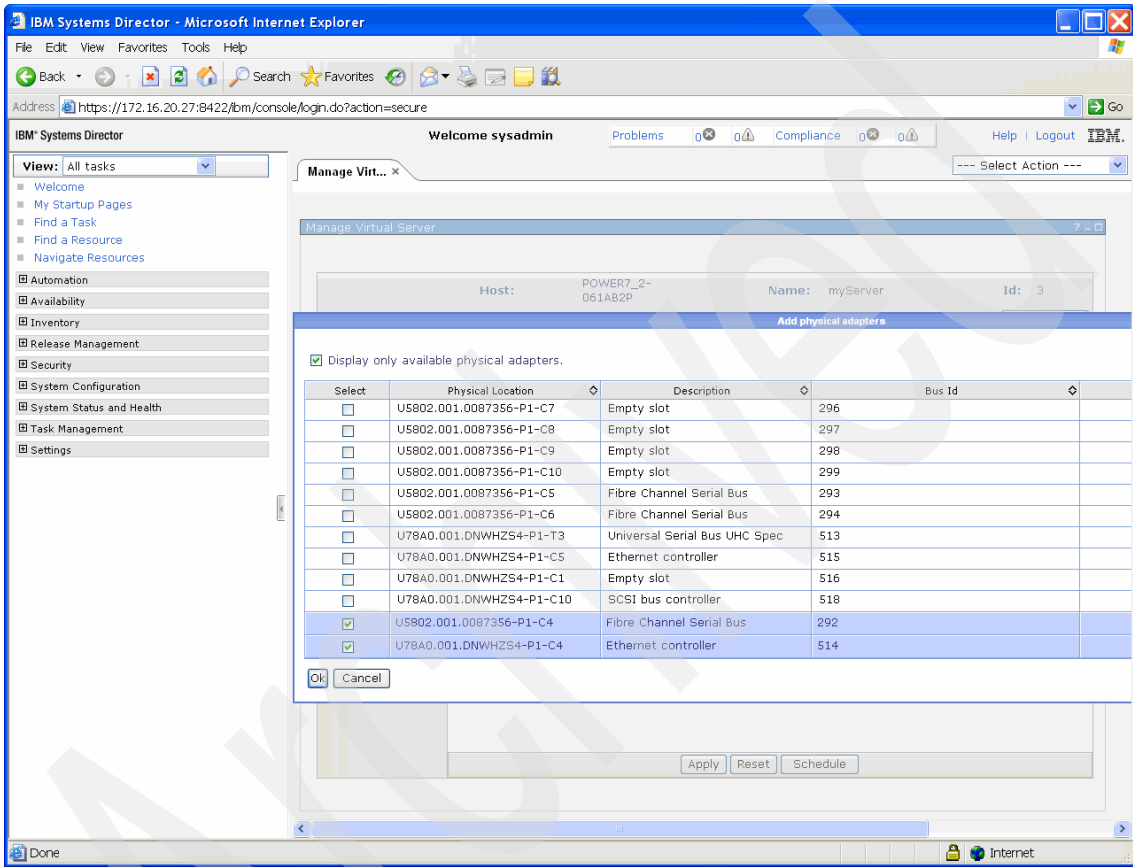


Figure 8-46 Manage Virtual Server: Add physical adapters

Note: Remember to click the **Apply** button after you make your selection and then click **OK**. Otherwise, the adapter will not be added and your selection is lost.

When adding the physical adapters and virtual adapters, there is a short period of time where the addition of the adapter to the Virtual Server is shown as pending (Figure 8-47).

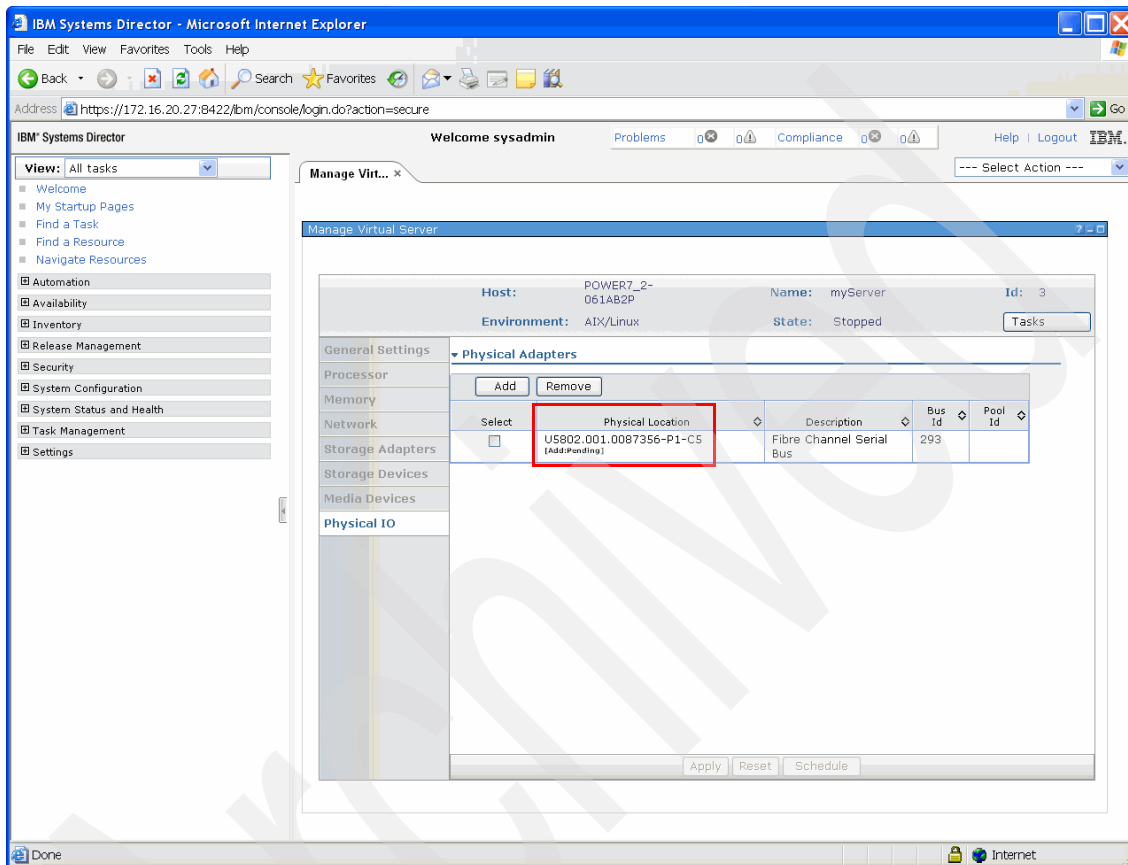


Figure 8-47 Manage Virtual Server: Physical adapter addition pending

8.4.1 Command-line usage

Changes to the Virtual Server configuration also can be made using the command line. Run **smcli chsyscfg** to accomplish this task (Example 8-4). In this example, two physical adapters are added. It is also possible to add virtual adapters. Run the **man chsyscfg** command for more details about this process.

Example 8-4 Adding physical adapters using smcli chsyscfg

```
sysadmin@sdmca:~> smcli chsyscfg -r prof -m POWER7_2-061AB2P -i  
name=DefaultProfile,lpar_name=myServer,\"io_slots=21010202/none/0,21010  
124/none/0\"
```

8.4.2 Current Configuration

To understand the differences between the HMC and the SDMC, it is important to know that the SDMC uses the concept of Current Configuration to store the state of a Virtual Server. This concept can be compared to the running state of an LPAR in the HMC. The HMC requires that you always keep track of changes made to the LPAR by DLPAR operations and save those changes to the profile of the LPAR to make the changes persistent across reboots. Alternatively, the Current Configuration on the SDMC is stored in its database. This configuration is visible when you activate a Virtual Server, and there are two options:

- ▶ Activate the Virtual Server with the Current Configuration: This is the state the hardware configuration of the Virtual Server was in when it was stopped. The Current Configuration can be saved to an existing profile, overwriting that profile. It can also be saved to a new profile. The Current Configuration is always reflected in the Manage Virtual Server page.
- ▶ Activate the Virtual Server with a profile: There can be more than one profile. The default profile is created when the Virtual Server is created and is called DefaultProfile. Different profiles can be applied to the Virtual Server when it is started.

On the Welcome page, navigate to the Virtual Server and right-click the Virtual Server to access the menu options for Current Configuration and Manage Profile (Figure 8-48).

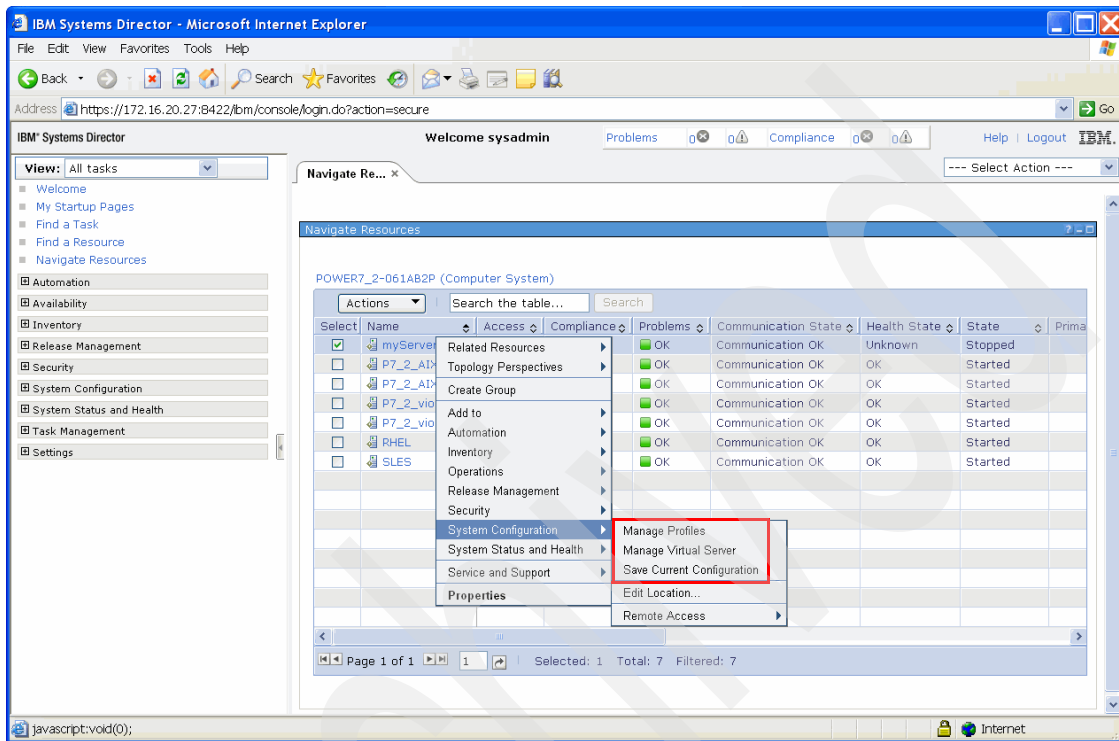


Figure 8-48 Current Configuration and Profile management

Clicking **Save Current Configuration** takes you to the Save page (Figure 8-49). Here it is possible to write the Current Configuration to the default profile, thereby overwriting it. Click **New Profile** to enter a name for the new profile.

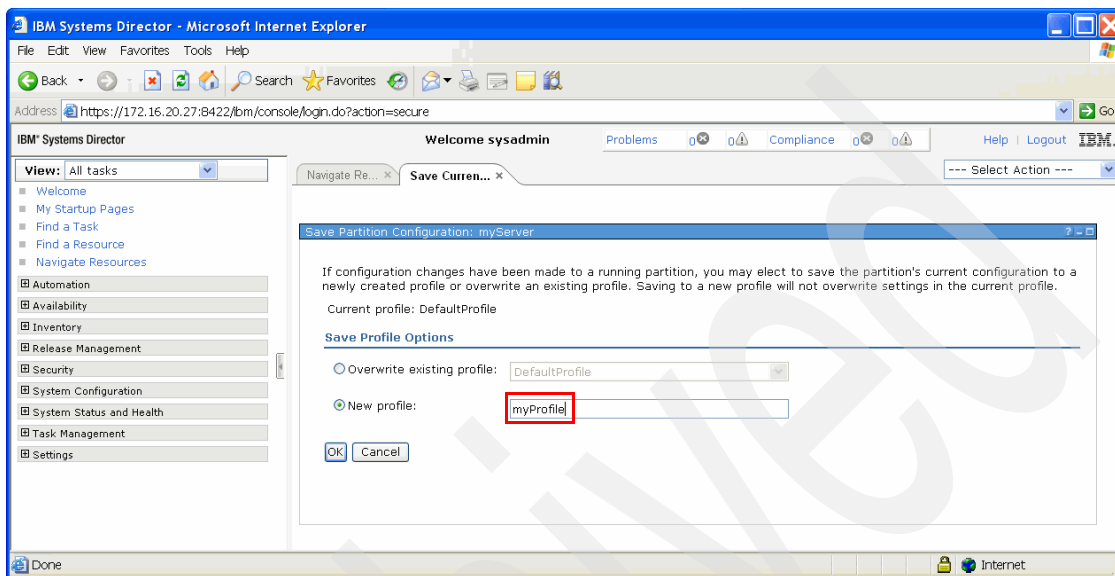


Figure 8-49 Save Current Configuration to a profile

8.4.3 Virtual Server Profiles

The Virtual Server Profile contains the configuration of the Virtual Server. When the Virtual Server is created, the first profile is also created and is called DefaultProfile. This profile contains all of the hardware resources that were configured on the Create Virtual Server page. Any changes made on the Manage Virtual Server page are not reflected in the profile unless the changes are saved. You can save these changes in the Manage Virtual Server panel by clicking the **Tasks** button (Figure 8-50).

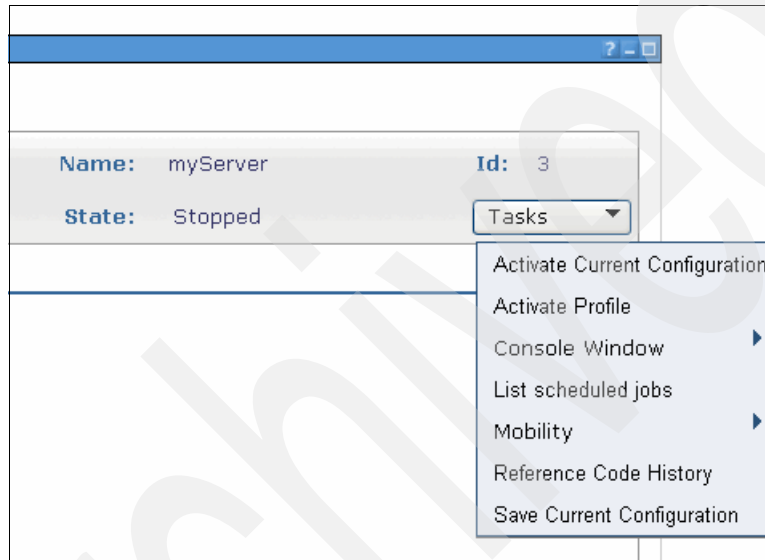


Figure 8-50 Tasks button in Manage Virtual Server page: Server not activated

Remember that the display of menus is context sensitive and shows only tasks and operations that are available in the current state of the Virtual Server. In Figure 8-50 on page 185, the state of the Virtual Server is Stopped. If the Virtual Server was started and remains in the Systems Management Services (SMS) menu, no Remote Monitoring and Control (RMC) connection is available (Figure 8-51). The available options in the Tasks menu change accordingly.

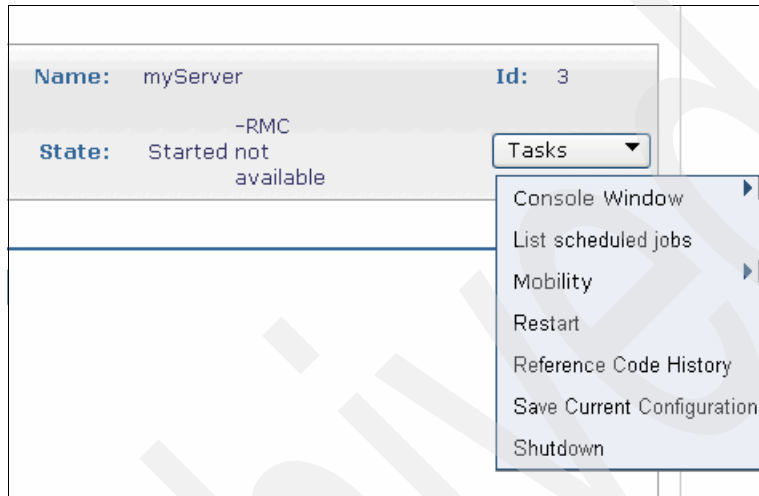


Figure 8-51 Tasks button in Manage Virtual Servers page: Server in SMS

To access the profiles of a Virtual Server, refer to Figure 8-48 on page 183. Select **System Configuration** → **Manage Profiles** to open the page shown in Figure 8-52.

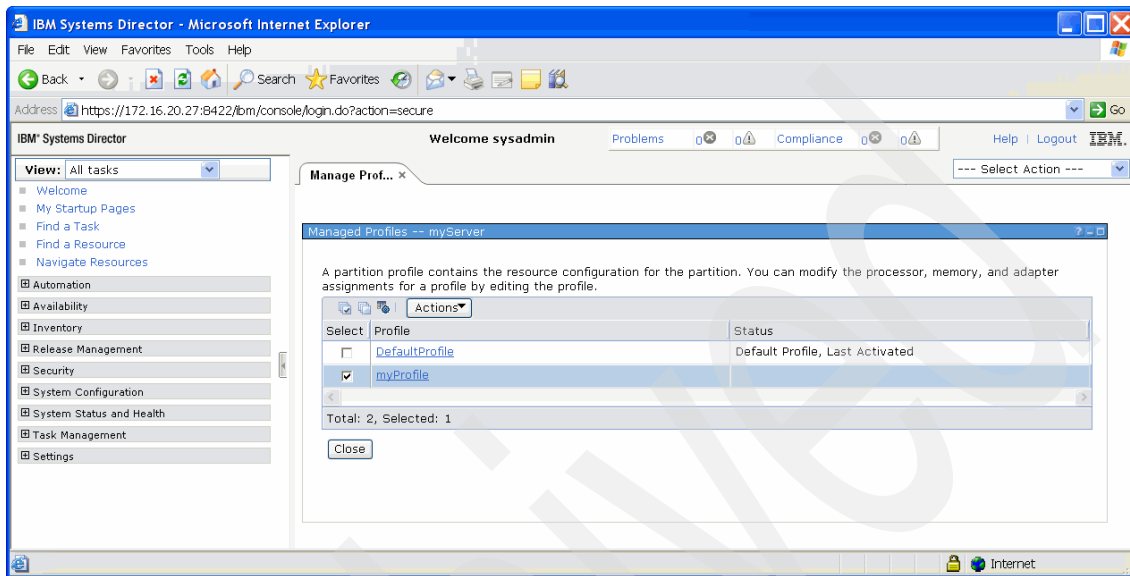


Figure 8-52 Manage Profiles page

Click the **Actions** button to open a menu where the Save Current Profile entry is added (Figure 8-53).

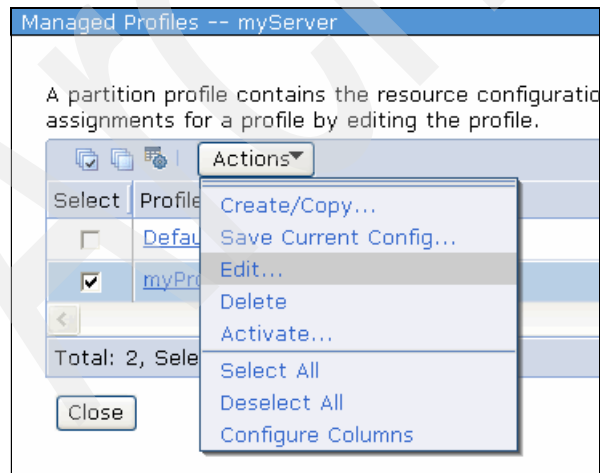


Figure 8-53 Actions menu in Manage Profiles page

Click **Edit** to open the Logical Partition Profile Properties menu. This menu allows you to view and edit the properties of the Virtual Server (Figure 8-54).

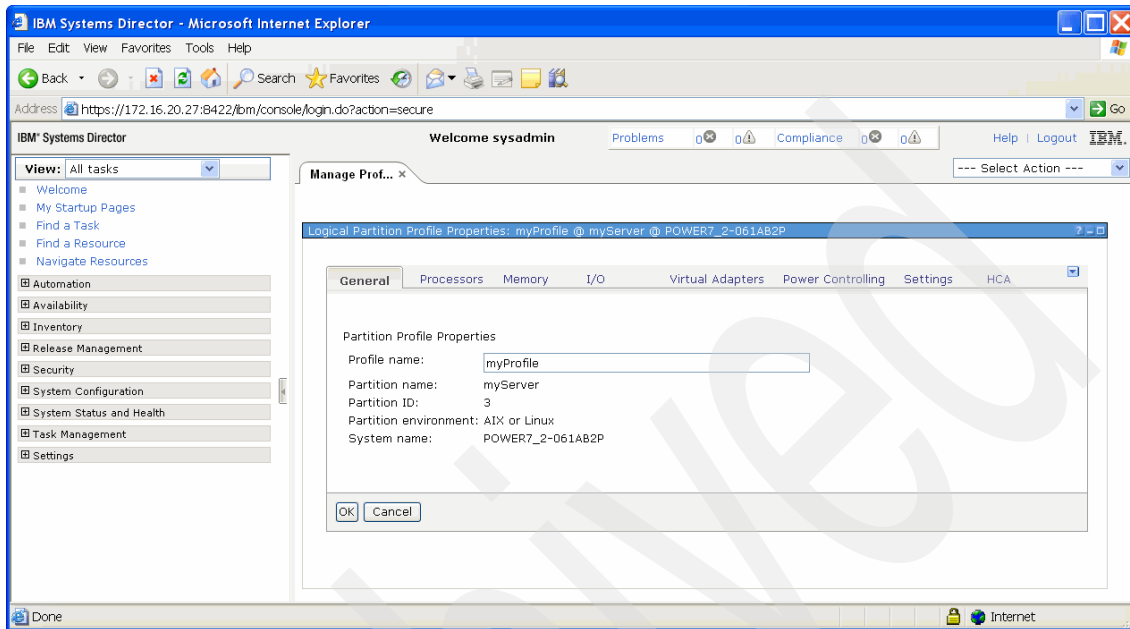


Figure 8-54 Manage Profiles: Edit Virtual Server properties

8.4.4 Server Profiles

Server Profiles represent a collection of Virtual Server Profiles that are available on the physical server. With a Server Profile, a physical server can be activated and the Virtual Servers contained in the Server Profile will start automatically when the server is activated.

Note: If there are any Virtual Servers defined that depend on virtual resources provided by an Virtual I/O Server, and the profiles of those Virtuals Servers are contained in a System Profile, and this System Profile is activated to start the Virtual Servers automatically, there could be a conflict situation in the activation order. Be sure to examine your configuration carefully to avoid this conflict.

There are initially no System Profiles defined for a server. To create a System Profile, enter a name into the System Profile name field. (This step is mandatory.) Right-click the server name and click **Add** (Figure 8-55).

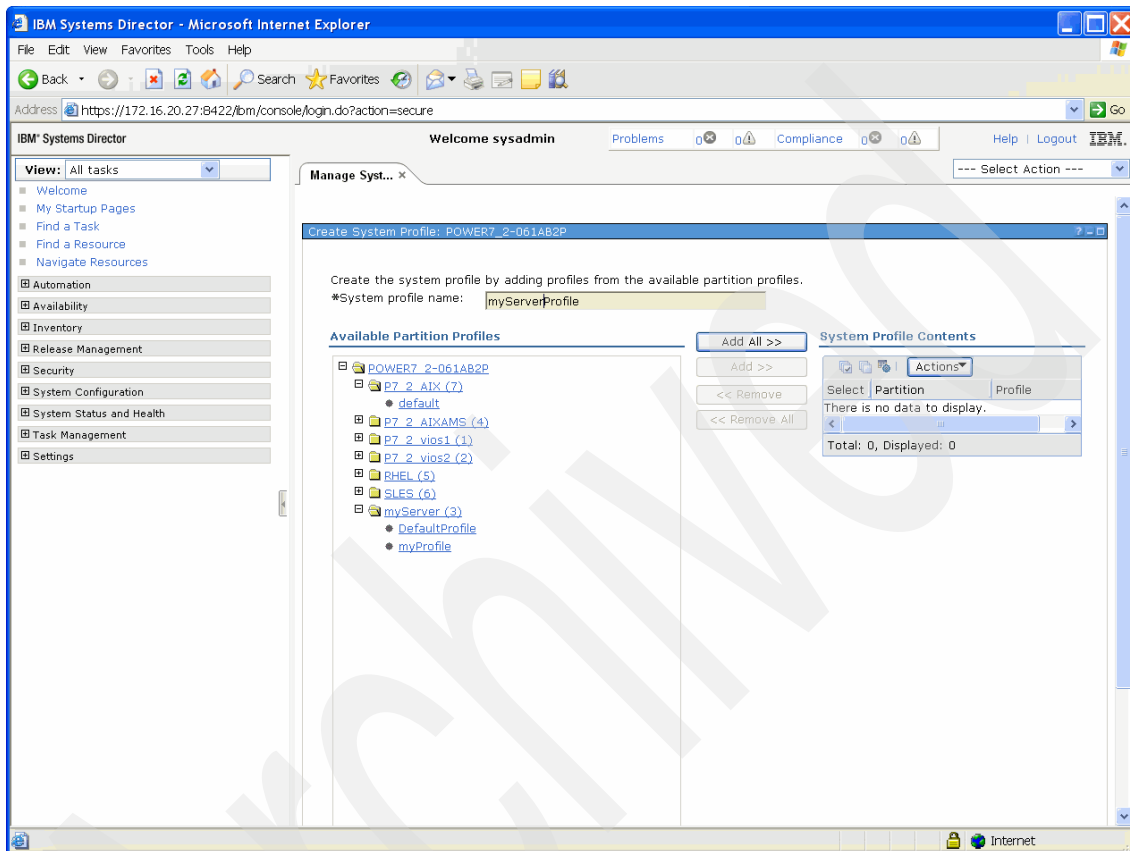


Figure 8-55 Server Profile initial menu

The Create Server Profile page has two panes that show the server and all the Virtual Servers defined on that server.

Expand the toggle of the Virtual Server to see all the profiles of that Virtual Server. For a Virtual Server, one profile can be selected and added by clicking the **Add** button. Alternatively, clicking **Add All** adds all of the last activated profiles to the Server Profile (Figure 8-56). Make sure that the Virtual Server Profiles you add suit your needs to avoid unwanted effects when the Server Profile is activated.

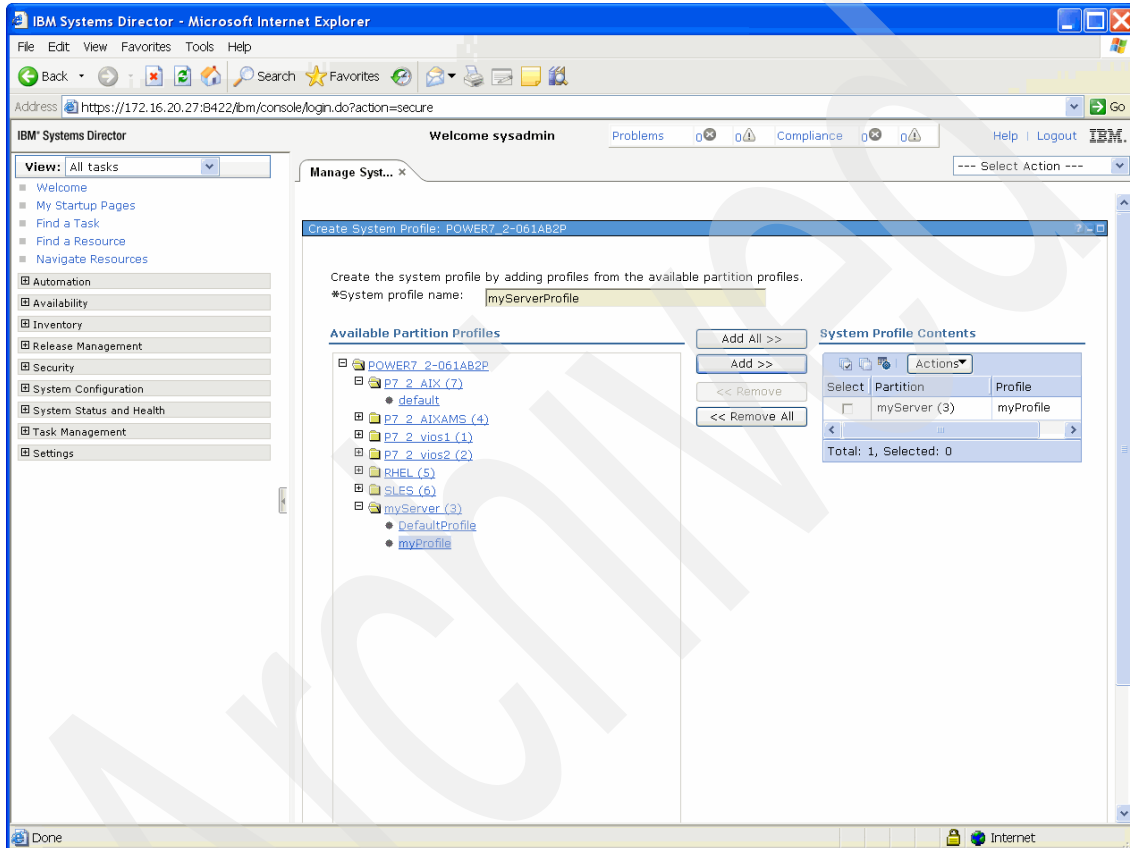


Figure 8-56 Server Profile with on Virtual Server Profile added

Note that Virtual Servers using shared memory cannot be added to a system profile. If you attempt to add these servers, you will receive a warning (Figure 8-57).

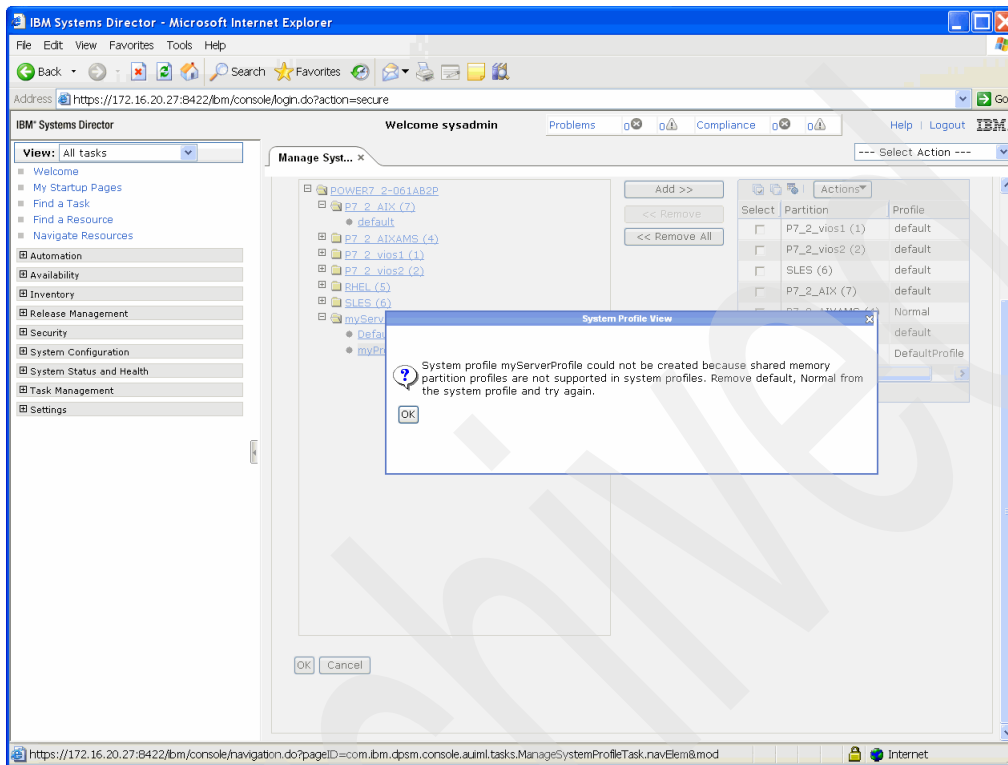


Figure 8-57 Server Profile: Warning while trying to add profiles using AMS

To remove a Virtual Server Profile from this System Profile, check the check box of that Virtual Server Profile and click **Remove**. You can also remove all of the contents of the Server Profile by clicking **Remove All**. Multiple Server Profiles can be defined for a single server if different names for Server Profiles are chosen, as it is with Virtual Server Profiles.

Command-line usage

A System Profile can also be defined by running **smcli mksyscfg** on the command line (Example 8-5). To change the Server Profile, use the **chsyscfg** command.

Example 8-5 Creating System Profile with smcli mksyscfg

```
sysadmin@sdmcb:~> smcli mksyscfg -r sysprof -m POWER7_2-061AB2P -i  
name=myServerProfile,lpar_names=myServer,profile_names=DefaultProfile
```

8.5 Suspend and resume

Both suspend and resume operations can be done by using the SDMC.

Note: Be careful when using the suspend and resume operation within a PowerHA-clustered Virtual Server, as this action can lead to a multiple active node situation if a suspended node is resumed after the standby node has taken over. This situation can lead to data loss.

8.5.1 Suspend a Virtual Server

To perform a suspend operation on an Virtual Server, perform the following steps:

1. Select **Actions** → **Operations** → **Suspend Operations** → **Suspend** (Figure 8-58).

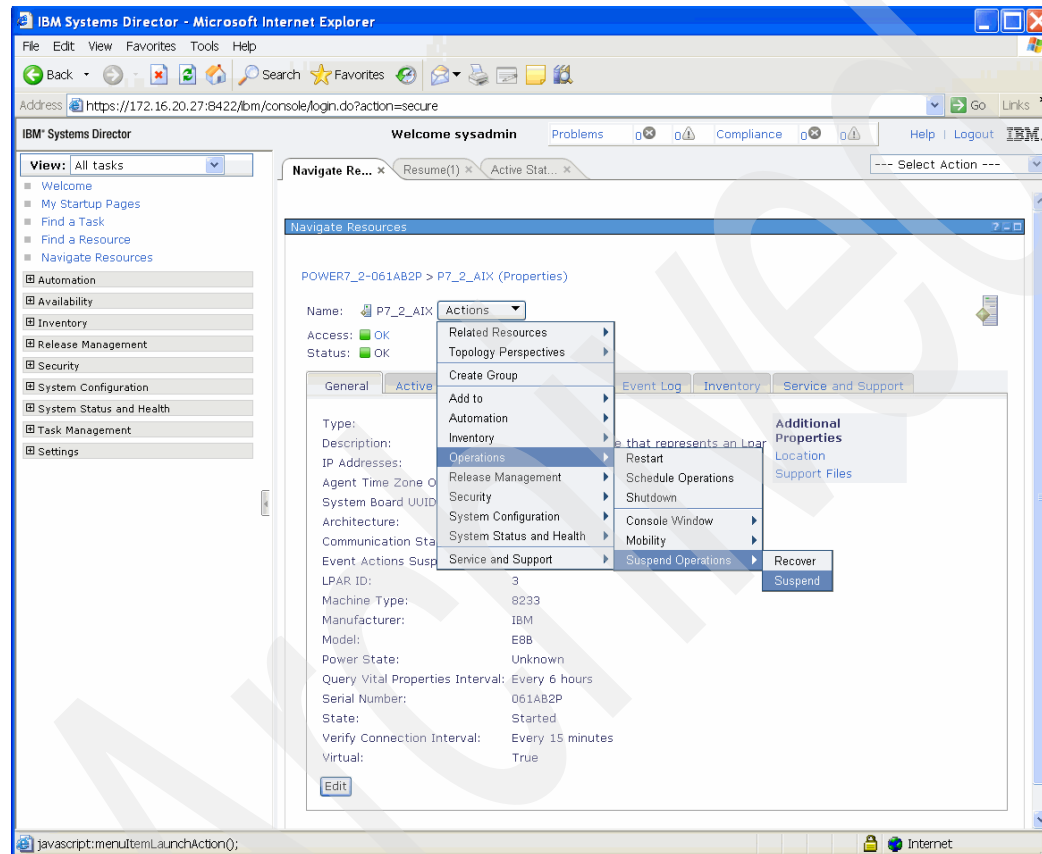


Figure 8-58 Select Suspend operation from Virtual Server menu

- From the **Partition Suspend/Resume** page (Figure 8-59), you can select **Suspend** to initiate the suspend operation. You can also select **Validate** before clicking **Suspend** to ensure that the Virtual Server is ready for the operation.

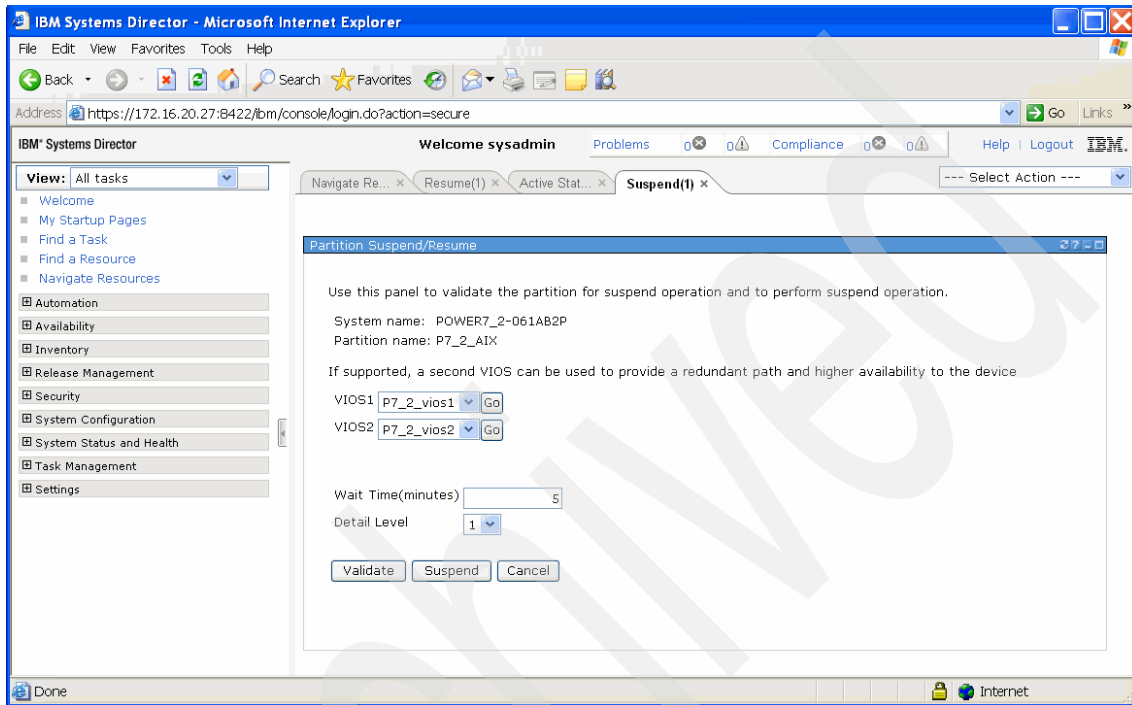


Figure 8-59 Validate and suspend

The Suspend status page shows the progress of the suspend operation and shows a successful completion.

8.5.2 Resume a Virtual Server

From the resource page of a suspended Virtual Server, you can perform a resume operation in a manner similar to the suspend operation by performing the following steps:

- Select **Actions** → **Operations** → **Suspend Operations** → **Resume**.
- From the Partition Suspend/Resume page, you can select **Resume** to initiate the resume operation. You can also select **Validate** before selecting **Resume** to ensure that the Virtual Server is ready for the operation.

The Resume status page shows the progress of the resume operation and shows a success completion.

8.6 Mobility

To perform partition mobility operations to move a partition from one physical server to another using the SDMC GUI, perform the following steps:

1. Select **Actions** → **Operations** → **Mobility** → **Validate** (Figure 8-60).

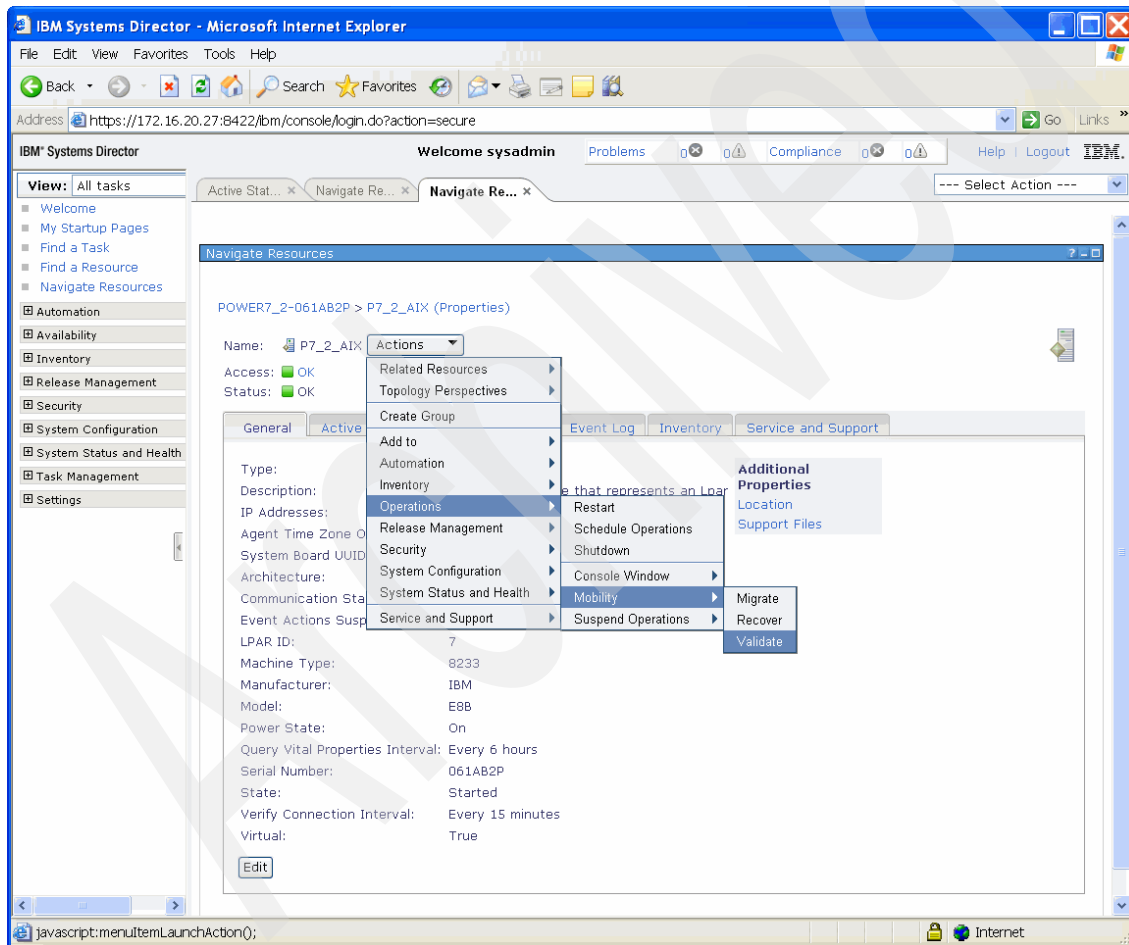


Figure 8-60 Select Validate from the partition page

2. In the Validate page, the **Migrate** and **View VLAN** buttons should be currently disabled (Figure 8-61). Complete the applicable fields for the migration and click the **Validate** button to validate that the partition is ready for a partition mobility operation.

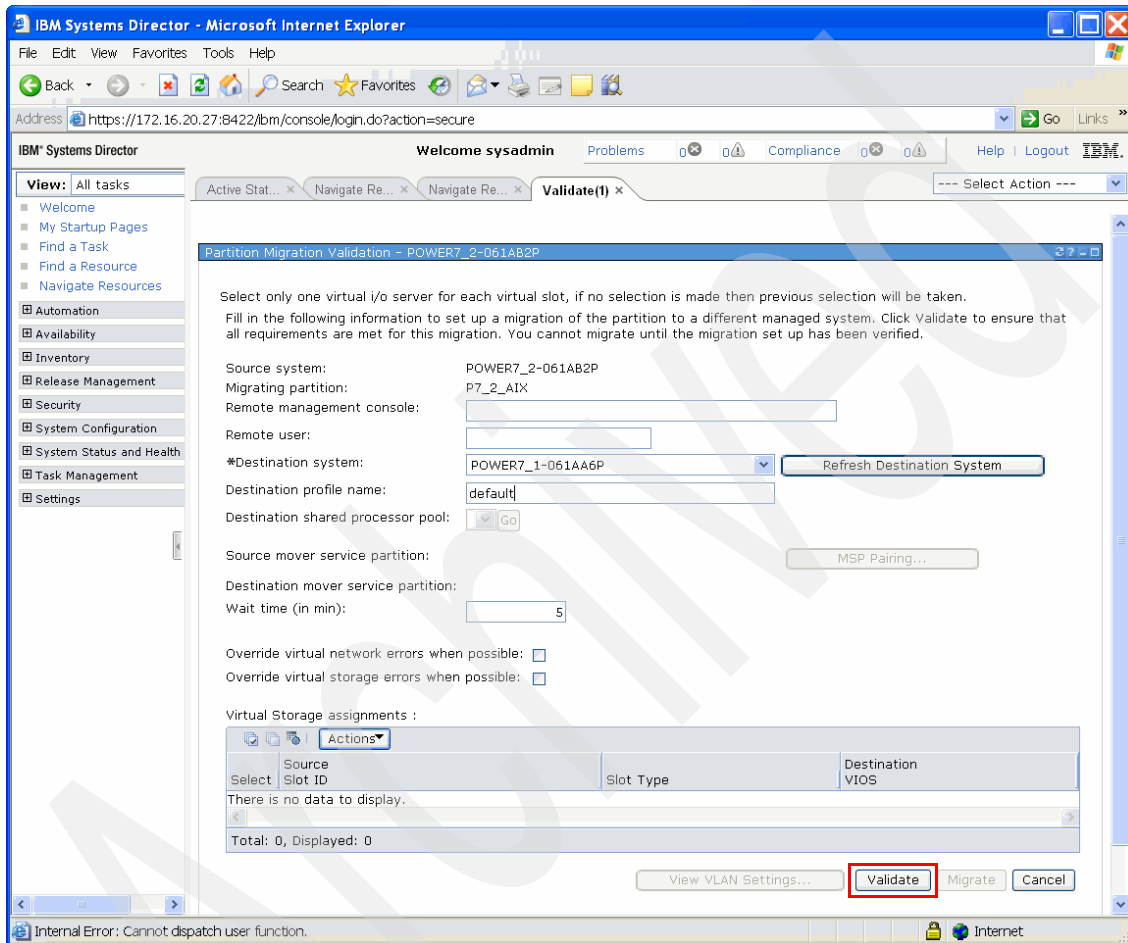


Figure 8-61 Click Validate

3. After the partition has been successfully validated, return to the Validate page. The Migrate button should now be available. Click **Migrate**.

The Partition migration status page opens and show the status of the migration operation. After the migration has successfully completed, the partition has been moved to the destination system.

IBM Systems Director Management Console management

This chapter covers the various tasks involved in managing and administrating the IBM Systems Director Management Console (SDMC) hardware and software appliances. We also give a short comparison of SDMC concepts to the concepts used on the Hardware Management Console (HMC). In this chapter, we discuss:

- ▶ HMC user concepts versus IBM Systems Director user concepts
- ▶ Users, roles, and groups
- ▶ Network configuration
- ▶ Backup and restore of the SDMC appliance
- ▶ Problem determination
- ▶ SDMC appliance updates

9.1 User management and security

Virtualization means that more than one system is running on the same hardware. Often, different systems are owned by different entities, for example, finance or human resources departments. Depending on the company's structure, security measurements may require that one user administering the Virtual Server for the finance department must not administer the Virtual Server for the human resources department, even if it is running on the same hardware or in the same pool. Also, it might be required that users work with different permissions, for example, operations personnel can start and stop the Virtual Server but not configure it. A user and security concept has to be put in place. This configuration was already possible on the HMC, but the naming and flow of operations has changed considerably in the SDMC. This section maps the known concepts in HMC to those used in the SDMC and how to use them.

9.1.1 Hardware Management Console concepts

On the HMC, there were predefined users and tasks and roles. Users were created and managed on the HMC itself and confined to the machine on which they were created. The SDMC instead uses the concept of a *user registry*, just like IBM Systems Director, because the IBM Systems Director component of the SDMC is used for it. A user registry can be the user management base of the underlying operating system, LDAP, or a domain controller. For more information about how IBM Systems Director handles users and security, refer to *Implementing IBM Systems Director 6.1*, SG24-7694.

Hardware Management Console users, roles, and tasks

To manage different aspects of the HMC and attached systems, the HMC used user roles and HMC tasks to manage access and permissions to the HMC itself as well as the attached systems.

For the SDMC, the IBM Systems Director concept was extended to create and manage users with either registry. For a quick mapping of default users, refer to Table 9-1.

Table 9-1 Default users on HMC and SDMC

| HMC | SDMC |
|---------|----------|
| root | root |
| hscroot | sysadmin |
| hscpe | pe |

Because the terminology and the structure of user and security management changes from the HMC to the SDMC, the different concepts are shown here to ease transition.

User roles

The user roles defined on the HMC are shown in Table 9-2.

Table 9-2 User roles on the HMC and SDMC

| HMC user role | SDMC user role | Function |
|---------------|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| hmcservicerep | | Service Representative. A service representative is an employee who is at your location to install, configure, or repair the system. |
| hmcviewer | SMMonitor, SMUser | Viewer. A viewer can view HMC information, but cannot change any configuration information. |
| hmcoperator | SMManager | Operator. An operator is responsible for daily systems operation. |
| hmcpe | | 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. |
| hmcsuperadmin | SMAAdministrator | 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. |

HMC tasks

Based on user roles, specific commands grouped by tasks could be executed by the user that hold the role. For a complete listing of commands allowed by role, refer to *Hardware Management Console V7 Handbook*, SG24-7491.

Tasks on the HMC were grouped by topic:

- ▶ HMC Management
- ▶ Systems Management
- ▶ Frame Management
- ▶ Control Panel Functions

9.1.2 IBM Systems Director concepts

Users in IBM Systems Director are users that are defined in the configured user registry. By default in IBM Systems Director, user creation and assignment to user groups are handled on the user registry level. A user registry is an entity handling users. This entity can be the local operating system of the SDMC, an LDAP server, or a Kerberos server. Each user registry has its own set of users that is independent of those on any other user registry in the network. The process of identifying a user and making sure that the user is who he claims to be is called *authentication*. Usually authentication is done by entering a user name and a password.

Authorization then occurs when an authenticated user is assigned permissions to perform tasks. The IBM Systems Director in the SDMC uses a role-based access control (RBAC) model for authorization. A role is a collection of permissions on operations within IBM Systems Director that are then assigned to a user. There are predefined roles in SDMC, and roles can also be defined by a user that has SMA administrator authority. Furthermore, roles can be combined to form even larger sets of permissions. To learn more about roles and their definitions, refer to section 3.7, “Managing Credentials”, in *Implementing IBM Systems Director 6.1*, SG24-7694.

It is possible to add users to the SDMC that have been defined in different user registries, for example, using the user registry of the SDMC base operating system. LDAP and Kerberos can be used for authentication and authorization as well. This situation offers more flexibility and allows for a wide range of configuration options.

As an extension to this concept, the SDMC allows for the creation of users and user groups in the underlying base operating system of the SDMC. Some system users and user groups are already preinstalled on that base operating system.

Note: If another user registry is employed besides the one of the underlying basic operating system of the SDMC, all of those users not defined on the SDMC base operating system must be created in that remote user registry. The SDMC can only read entries in remote user registries but cannot create them.

Users

Initially, only the following interactive user registry users are defined to the SDMC:

- root

This is the root user of the underlying operating system.

► sysadmin

This is the user designed to be the primary administrator of the SDMC.

► pe

This is the user designed to perform the tasks of the product engineer as defined above for the HMC.

Users on the SDMC can be listed by using the `smcli lsuser` command. In Example 9-1, this command is used to produce a full listing of user properties for the sysadmin user.

Example 9-1 Listing the sysadmin user using the smcli lsuser command

```
sysadmin@sdmca:~> smcli lsuser -l sysadmin
sysadmin:
  ObjectType: User
  DisplayName: sysadmin
  Description:
  FullName: sysadmin
  Email: null
  TelephoneNumber: null
  Mobile: null
  HomePhone:
  Pager: null
  LastLoginDate: 2010-12-13T17:35:08-05:00
  LastLoginAddress: 172.16.254.34/172.16.254.34
  IsLocked: False
  UniqueID: 500
  IsActive: True
  ActiveSessions:
    ID: dqG-dKGGG9hfQoolkkgGGG
    Description:
    Login Date: Mon Dec 13 17:35:08 EST 2010
    Login Address: 172.16.254.34/172.16.254.34

    ID: DIRCLI-10038
    Description: lsuser
    Login Date: Mon Dec 13 18:30:02 EST 2010
    Login Address: sdmcb/172.16.20.27
  AssignedRoles: {'GroupRead' applied to <ALL GROUPS>}
  ImpliedRoles: {'SMAadministrator' applied to <ALL GROUPS>}
  GroupMembership: {'sadmin'}
```

User groups

The following user registry groups are employed for granting granular access permissions:

- ▶ **smadmin (Administrator group)**
Members of the smadmin group are authorized for all operations. They have administrative access to IBM Systems Director and can perform all administrative tasks. These members can define the privileges available to the smmgr, smuser, and smmon groups. The privileges available to members of the smadmin group cannot be restricted.
- ▶ **smmgr (Manager group)**
Members of the smmgr group can perform management operations, which are a subset of the functions that a member of the smadmin group can perform.
- ▶ **smuser (User group)**
The smuser group includes all authenticated users. Members can perform only basic operations.
- ▶ **smmon (Monitor group)**
Members of the smmon group can access those administrative functions that provide read-only access, such as monitoring.
- ▶ **smservicerep (Service Representative Group)**
Members of the service representative group can perform management operations related to the installation, configuration, or repair of the system.

Refer to Figure 9-1 for a display of users and their initially assigned groups after installing the SDMC. Also note that roles are assigned to groups and to users.

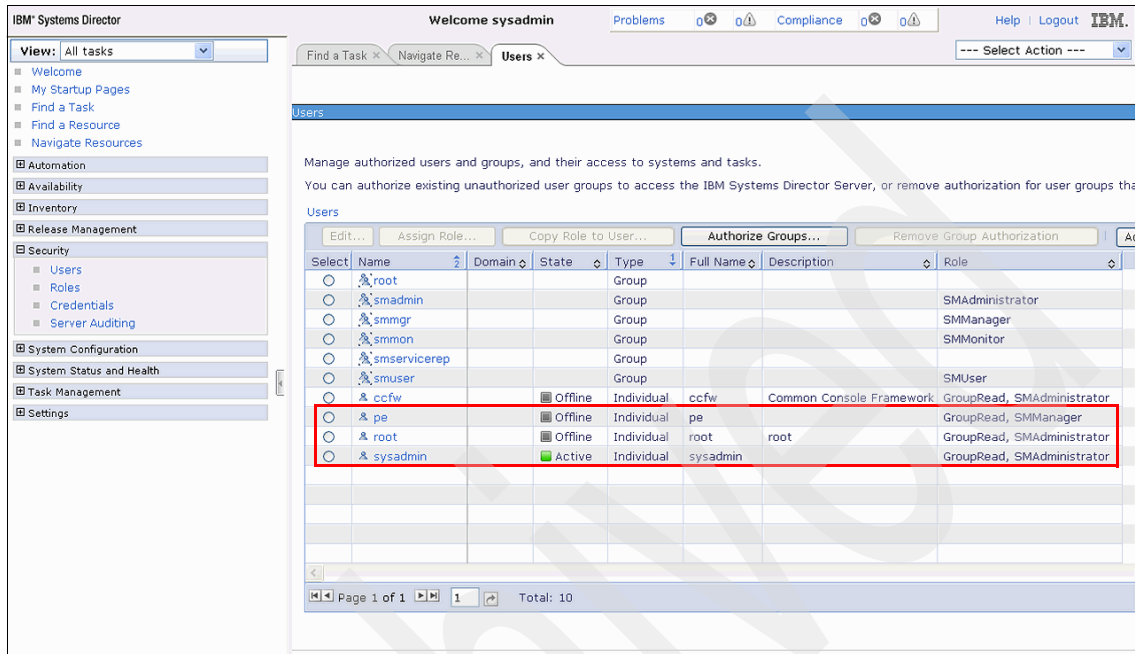


Figure 9-1 Systems Director Management Console: Initial users page

As shown in Example 9-2, user groups can be listed on the command line by using the `smcli lsusergp` command.

Example 9-2 Listing user groups using `smcli lsusergp`

```
sysadmin@sdmca:~> smcli lsusergp -l
root:
```

```
ObjectType: User Group
DisplayName: root
Description: null
ManagedAsGroup: false
AssignedRoles:
ImpliedRoles:
Members: root
GroupMembership:
```

```
smadmin:
```

```
ObjectType: User Group
DisplayName: smadmin
Description: null
ManagedAsGroup: false
```

```
AssignedRoles: {'SMAAdministrator' applied to <ALL GROUPS>}
ImpliedRoles:
Members: ccfw,sysadmin,root
GroupMembership:

smmgr:
  ObjectType: User Group
  DisplayName: smmgr
  Description: null
  ManagedAsGroup: false
  AssignedRoles: {'SMMManager' applied to <ALL GROUPS>}
  ImpliedRoles:
  Members: pe
  GroupMembership:

smmon:
  ObjectType: User Group
  DisplayName: smmon
  Description: null
  ManagedAsGroup: false
  AssignedRoles: {'SMMonitor' applied to <ALL GROUPS>}
  ImpliedRoles:
  Members:
  GroupMembership:

smservicerep:
  ObjectType: User Group
  DisplayName: smservicerep
  Description: null
  ManagedAsGroup: false
  AssignedRoles:
  ImpliedRoles:
  Members:
  GroupMembership:

smuser:
  ObjectType: User Group
  DisplayName: smuser
  Description: null
  ManagedAsGroup: false
  AssignedRoles: {'SMUser' applied to <ALL GROUPS>}
  ImpliedRoles:
  Members: newUser
  GroupMembership:
```

Roles

There are four roles that are initially defined on the SDMC:

- ▶ **SMAAdministrator**

The Administrator role has full authority to all tasks and commands, including security administration, product installation, and configuration.

- ▶ **SMManager**

The Manager role can perform a subset of the tasks that an Administrator can perform. Typically, system administration, system health management, and configuration tasks are available.

- ▶ **SMUser**

The User role includes any authenticated user and allows only basic operations, such as viewing resources and properties.

- ▶ **SMMonitor**

The Monitor role can access those administrative functions that provide read-only access. Primarily, monitoring, notifications, and status tasks are available.

Additionally, another role is predefined in the Systems Manager Director Console:

- ▶ **GroupRead**

This permission grants a user the ability to view or open a group defined in SDMC.

Roles can be listed on the command line by using the **smcli lsrole** command (Example 9-3).

Example 9-3 Listing the SMAAdministrator role using smcli lsrole

```
sysadmin@sdmca:~> smcli lsrole -l SMAAdministrator
SMAAdministrator:
  ObjectType: InstanceAccessRole
  DisplayName: SMAAdministrator
  Description: The Administrator role has full authority to all tasks
and commands, including security administration, product installation,
and configuration.
  IsDefaultRole: false
  IsSystemDefinedRole: true
  Permissions: All Permissions
```

Creating a role

To create a role, perform the following steps:

1. Expand **Security** and click **Roles**. The **Roles** page opens (Figure 9-2).

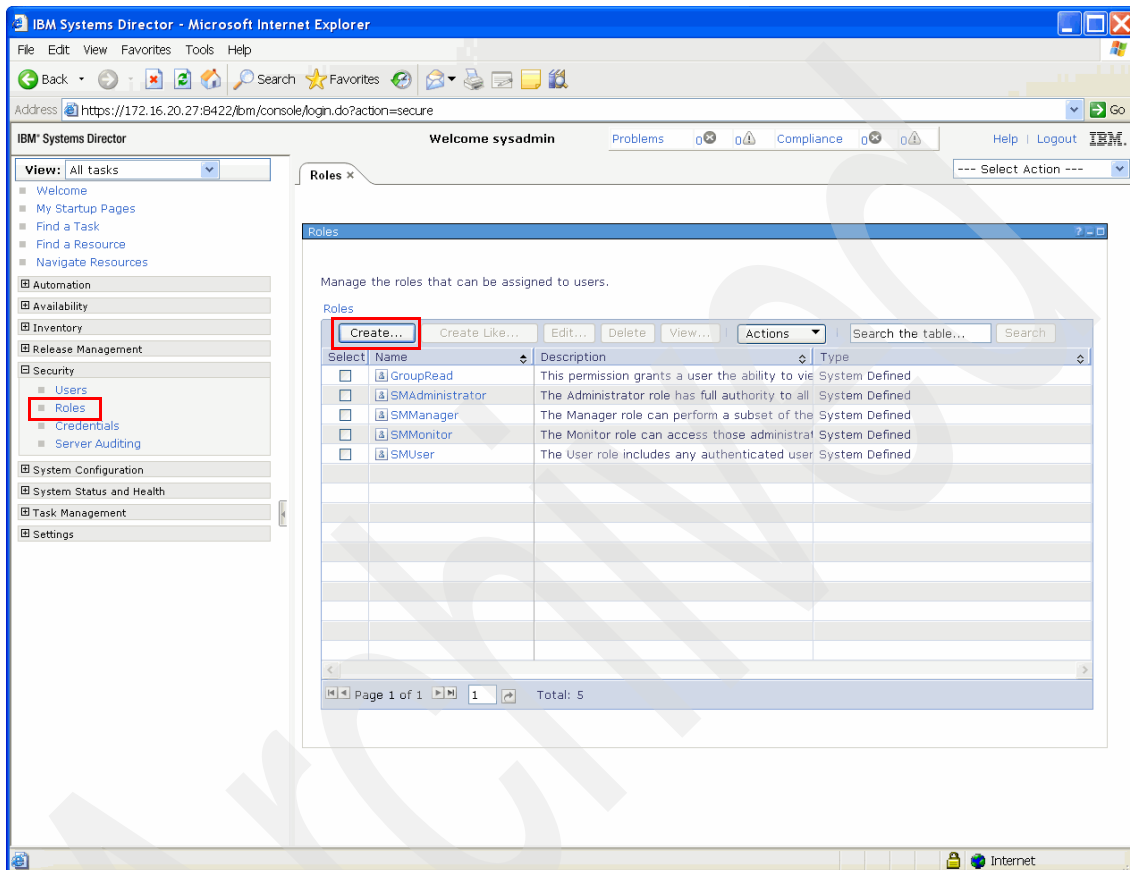


Figure 9-2 Initial Roles page

2. Click **Create** to open the Roles wizard Welcome page. Clicking **Next** opens the Name page, where a name for this role has to be entered. Optionally, you also can give a description of this role in the Description field (Figure 9-3).

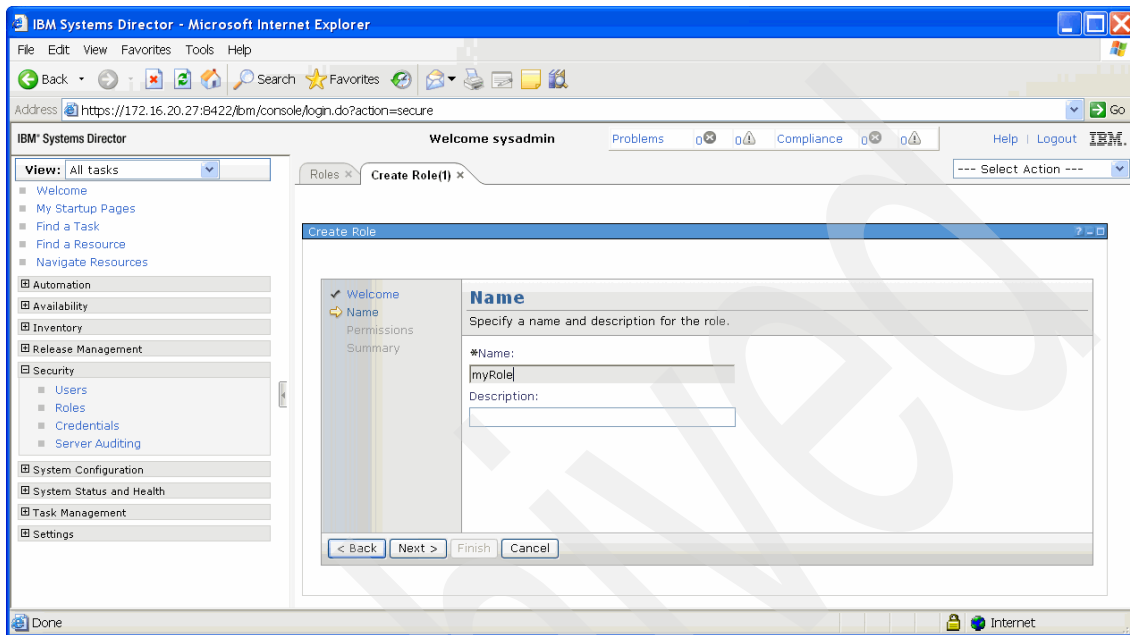


Figure 9-3 Create Role wizard: Name page

3. Clicking **Next** opens the Permissions page (Figure 9-4). You see a page with two columns, showing Available Permissions in the left column and Selected Permissions in the right column. Above the Available Permissions column, you can select either **All Permissions**, which gives all permissions to this role, or **Selected Permissions**. Any entry can be selected and added to the set of Selected Permissions by clicking **Add**.

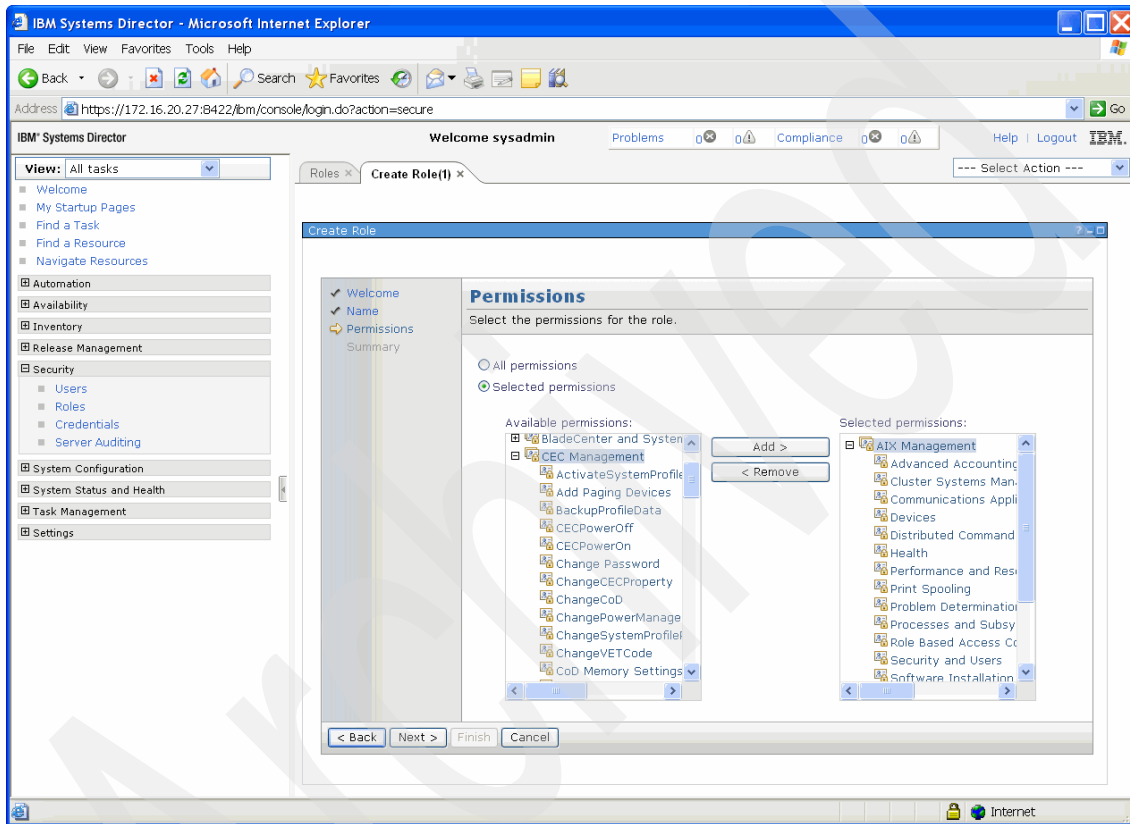


Figure 9-4 Create Role wizard: Permissions page

- Click the plus sign next to any role to expand it. All permissions collected in this set can be selected separately and added to Selected Permissions. Click **Next** to see the Summary page, which shows all the permissions for this role (Figure 9-5). Click **Finish** to create this role.

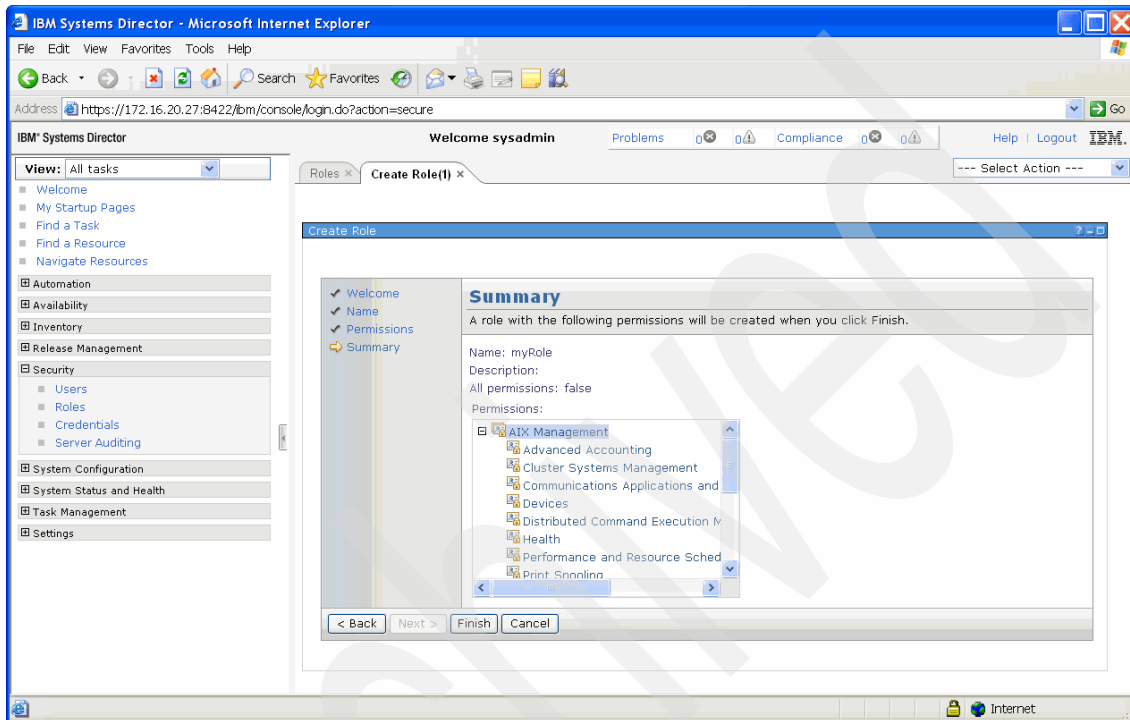


Figure 9-5 Create Roles: Summary page

To define a role using the command line, run the **smcli mkrole** command (Example 9-4). Before using this command, run **man mkrole** and **man lsperm** to obtain a deeper understanding about how roles can be created as well as a long list of options for roles.

Example 9-4 Creating a role using the smcli mkrole command

```
sysadmin@sdmca:~> smcli mkrole -p "AIX Management" myRole
```

Listing roles

Roles can be listed using the command line by running **smcli lsrole** (Example 9-5).

Example 9-5 Listing a role using the smcli lsrole command

```
ssysadmin@sdmc:~> smcli lsrole -l myRole
myUserRole:
  ObjectType: InstanceAccessRole
  DisplayName: myUserRole
  Description:
  IsDefaultRole: false
  IsSystemDefinedRole: false
  Permissions: AIX Management
```

Deleting a role

To delete a role in the GUI, go to the Roles page (Figure 9-2 on page 206). Check the check box left to the role and click **Delete**.

To delete a role using the command line, run the **smcli rmrole** command (Example 9-6).

Example 9-6 Deleting a role using the smcli rmrole command

```
sysadmin@sdmca:~> smcli rmrole myUserRole
```

Groups

The concept of groups in the SDMC is equivalent to that of Resource Roles in the HMC. Groups are a collection of resources that are applied to access resources, such as systems and Virtual Servers. Some groups are already predefined in the SDMC (Figure 9-6). To define permissions to a user, a role has to be created. By assigning a group to an user, the role assigned to this user defines the permissions that the user has on the group.

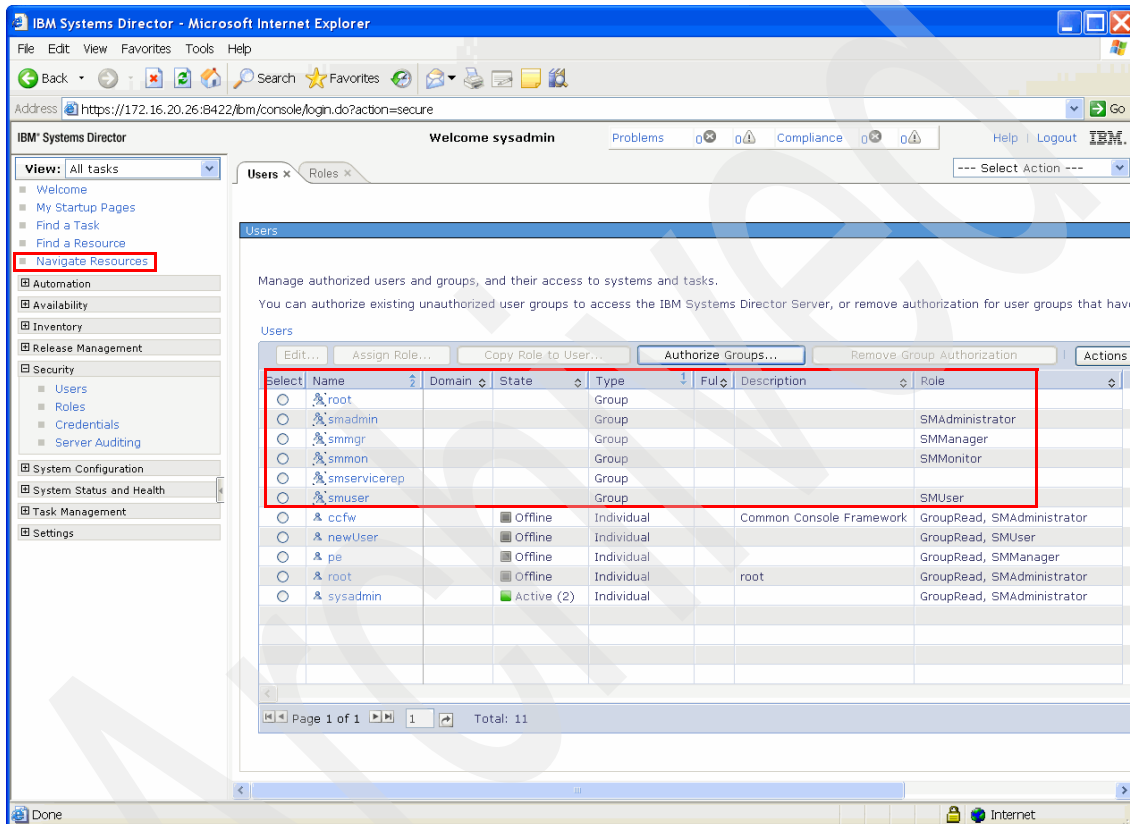


Figure 9-6 Groups in the SDMC interface

Creating a group

To create a group, perform the following steps:

1. Click **Navigate Resources** on the left side of the Welcome page. The Groups page opens and provides a view of the existing groups (Figure 9-7). There is also a description of their properties.

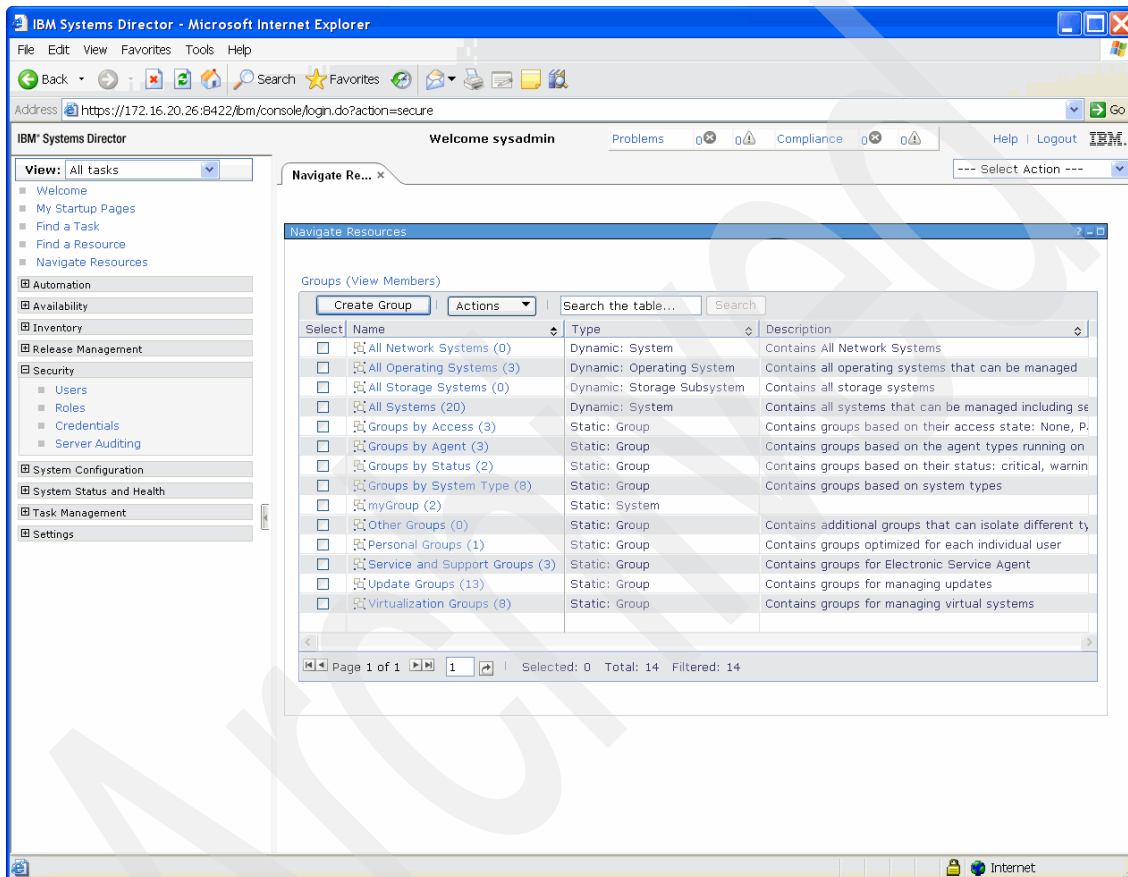


Figure 9-7 Groups page

2. Click **Create Group** to open the Welcome page of the Group Editor wizard (Figure 9-8).

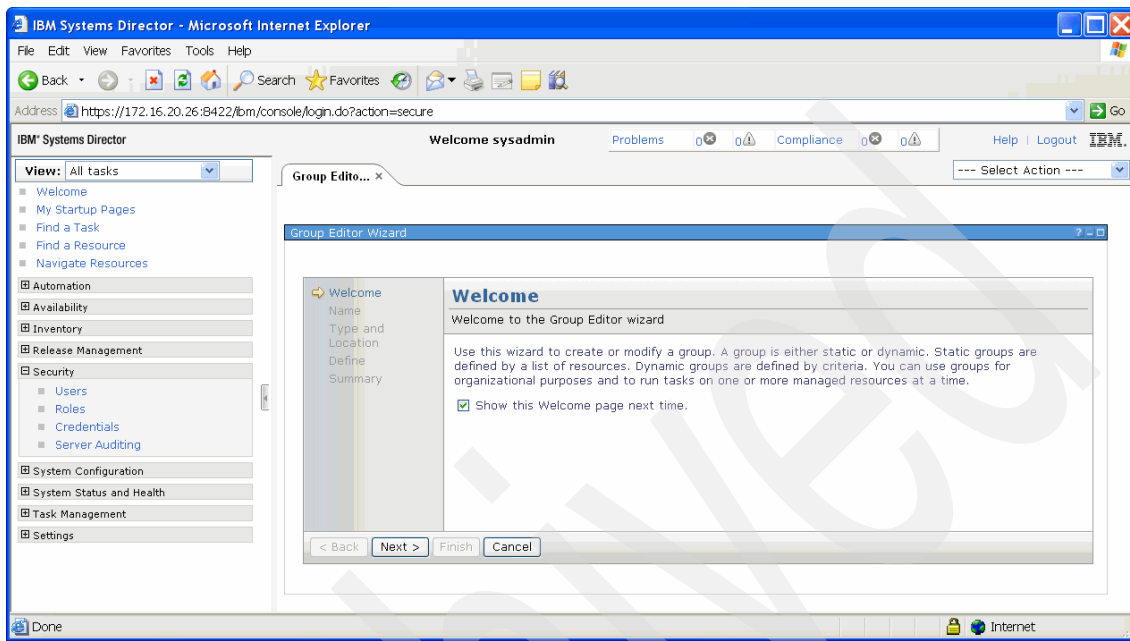


Figure 9-8 Group Editor Wizard: Initial page

3. Enter a name for the group and, optionally, a description on the Name page and click **Next**. On the Type and Location page, you can set the type of the group, either as Static or Dynamic. Static groups contain systems that are selected at the time of group creation and do not change. Dynamic groups contain systems that match defined conditions, such as State. For the type, Any has to be selected. The Location of the group to be created can be either Groups or sysadmin, as shown in Figure 9-9.

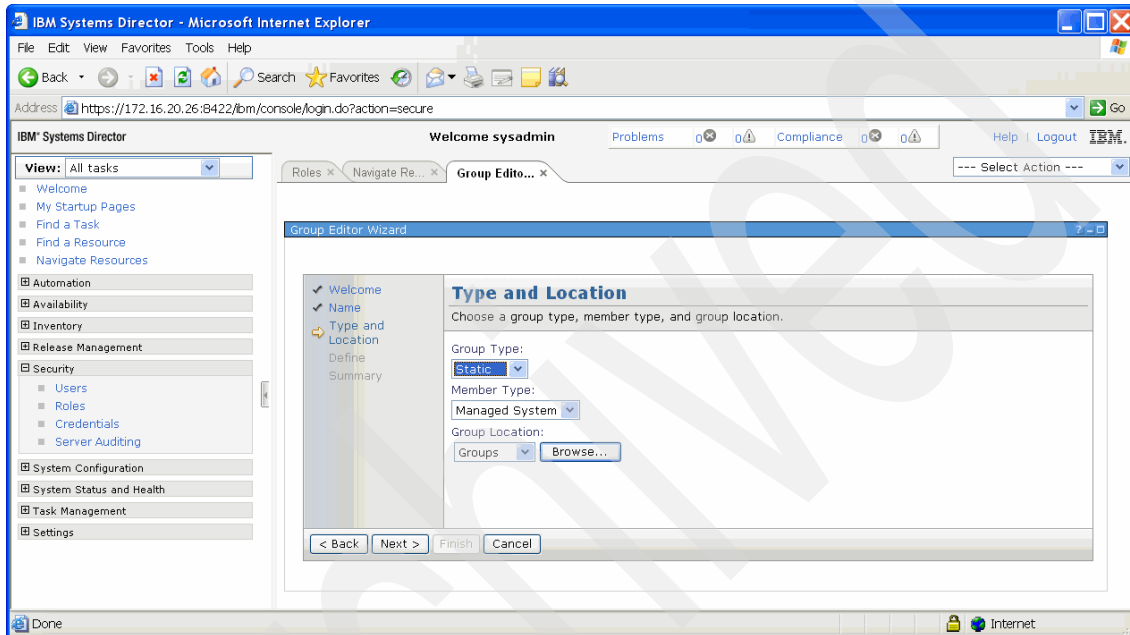


Figure 9-9 Group Editor Wizard: Type and Location

4. Click **Next** to open the Define page, which allows for a wide selection of resources. On the left side of this page, in the Groups area, you can see a tree of entries. Entries of type All or specific resources can be selected and added to the Selected area of the page immediately by clicking **Add** (Figure 9-10).

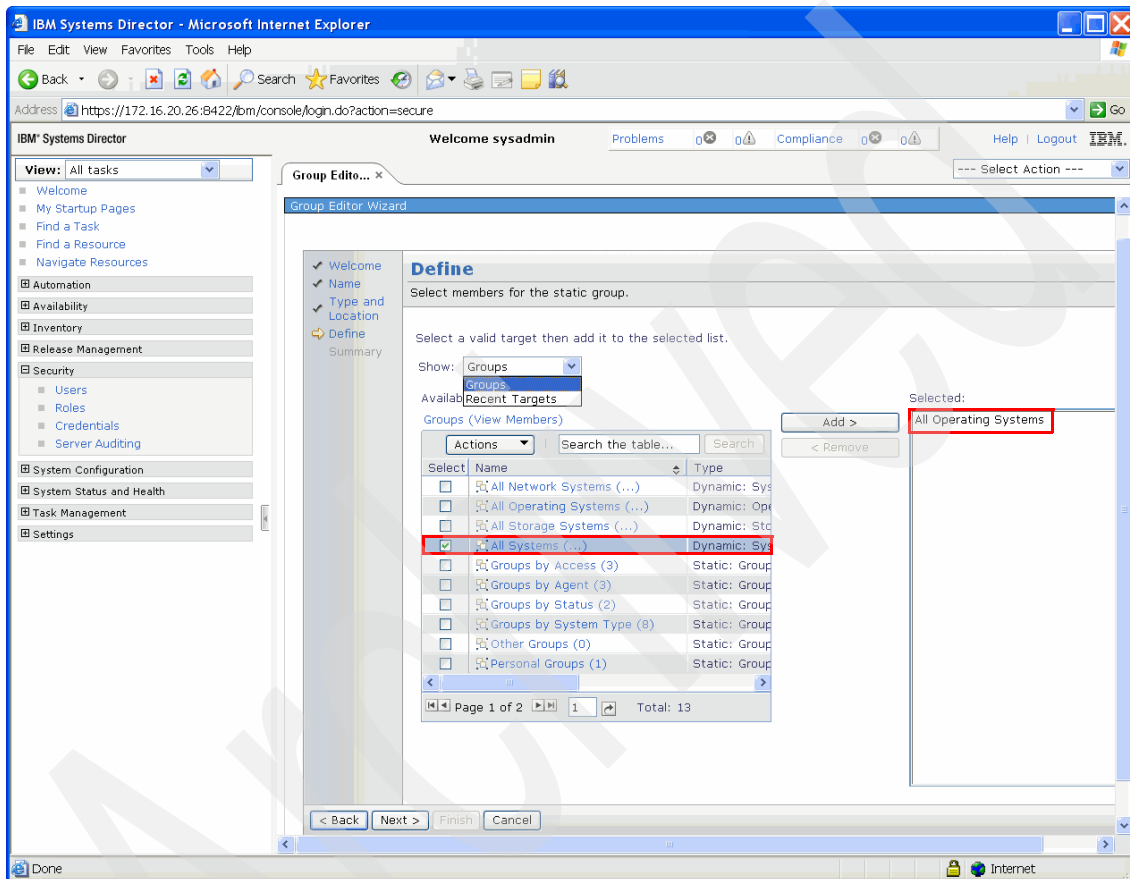


Figure 9-10 Group Edit Wizard: Define page with systems selected

5. To select a single entry, for example, a Virtual Server, click **All Systems**. A list of Virtual Servers opens. Click the list and then click **Add** to add this Virtual Server to the Selected area (Figure 9-11).

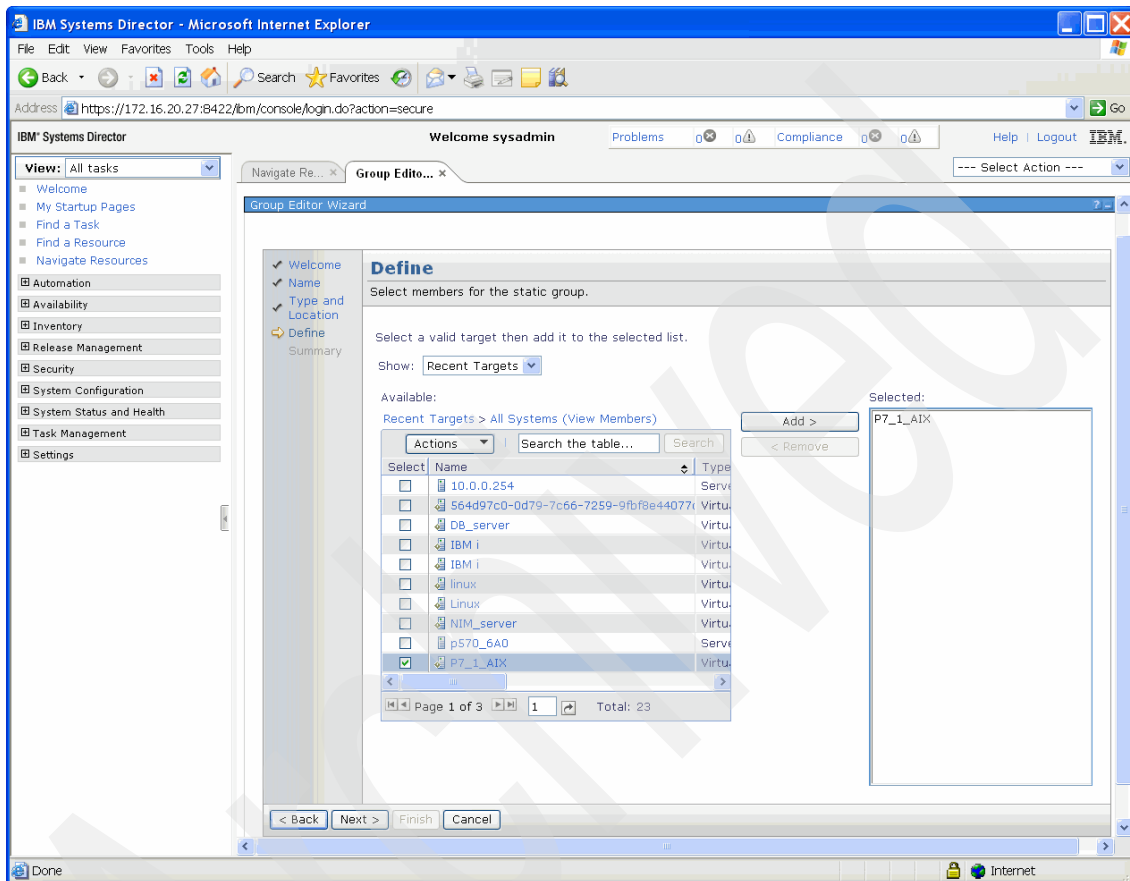


Figure 9-11 Group Edit Wizard: Select page with groups expanded

6. Click **Next**, and the Summary page that lists the resources assigned to this group opens (Figure 9-12).

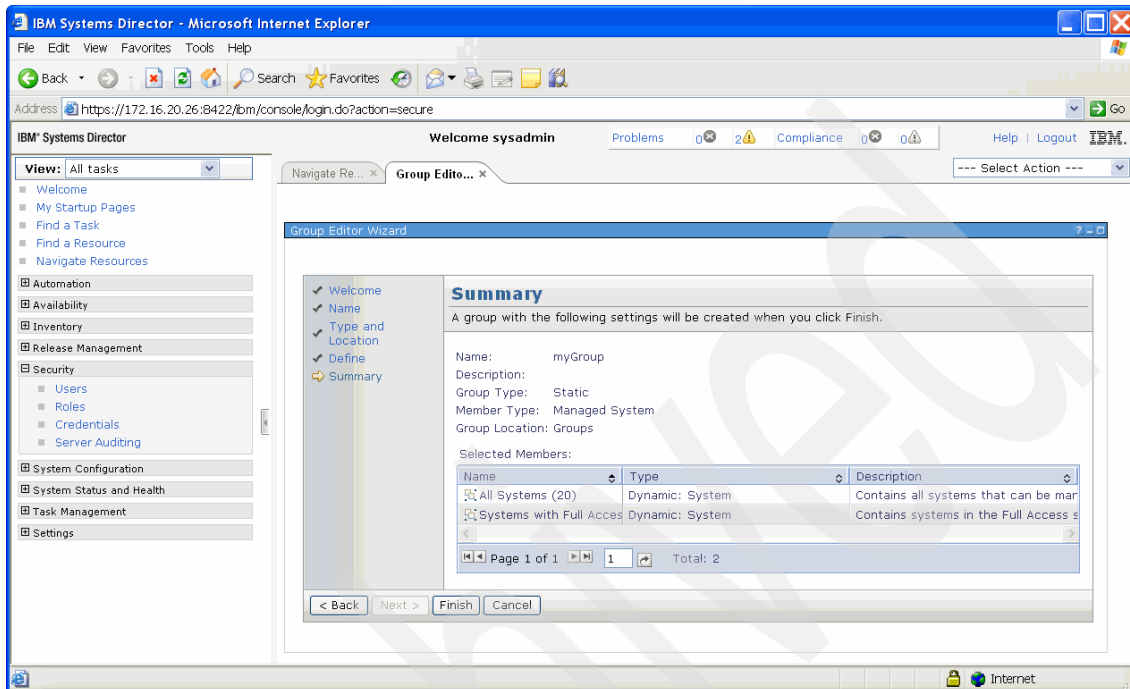


Figure 9-12 Group Edit Wizard: Summary page

After clicking **Finish**, the wizard closes and the new group is shown on the Groups page (Figure 9-13).

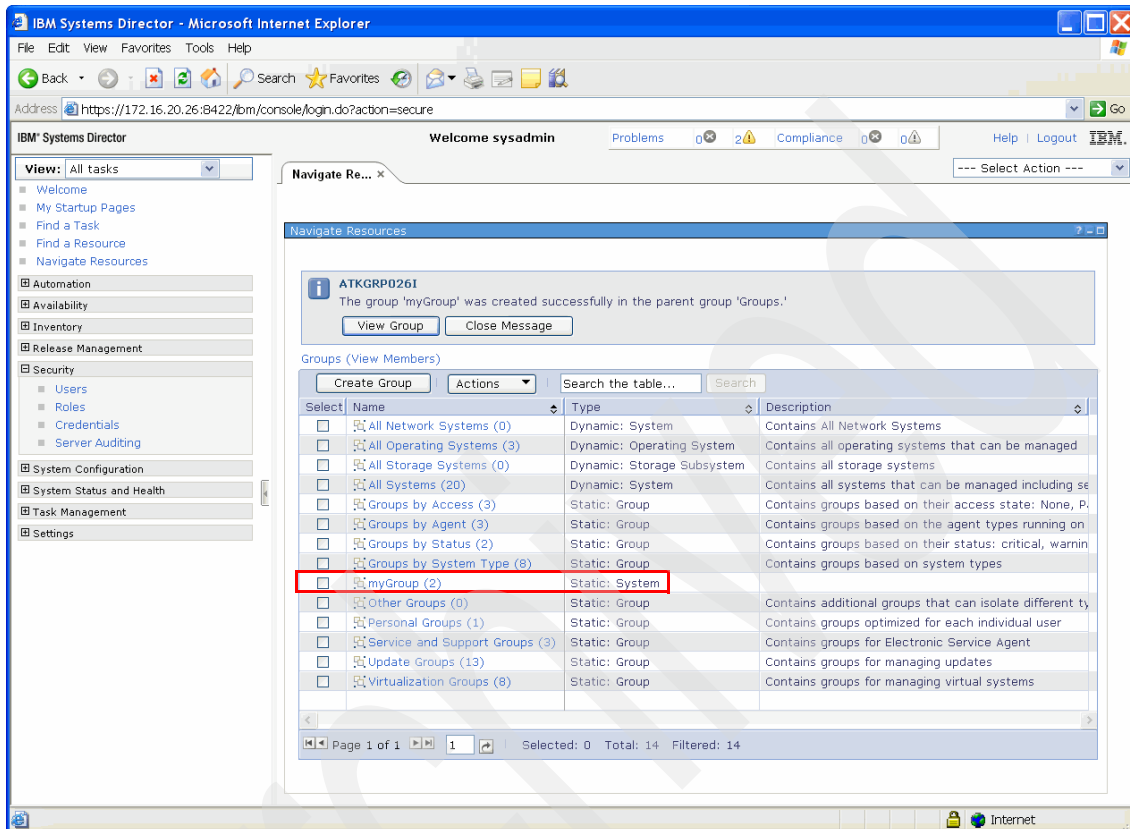


Figure 9-13 Groups page with the newly created group

9.1.3 Assigning a role to a user

Users, roles, and groups allow for a more granular assignment of permissions to a user.

To assign a role to a user, perform the following steps:

1. In the left pane of the Welcome page, click **Users** in the Security area and check the check box for the user name (Figure 9-14). Click **Assign Role**.

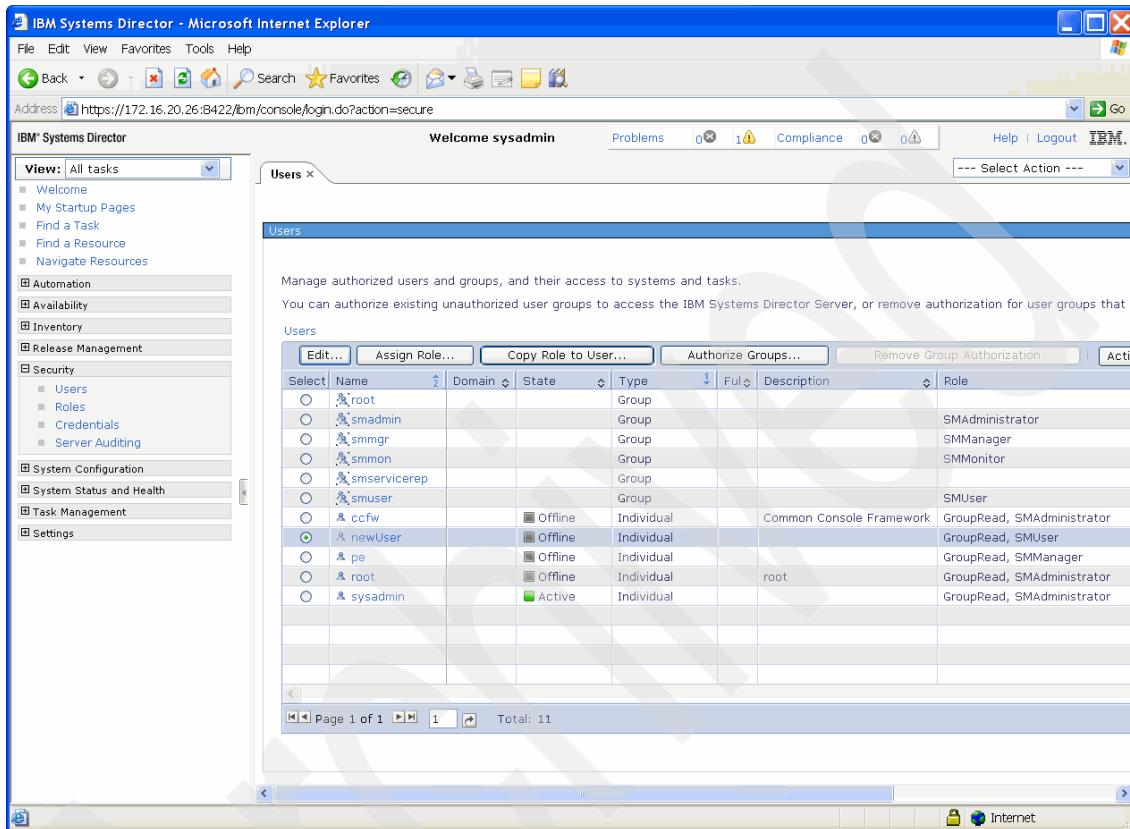


Figure 9-14 Users page: Assigning a role

- The Welcome page of the Assign Role wizard opens. Click **Next** to open the Roles page (Figure 9-15).

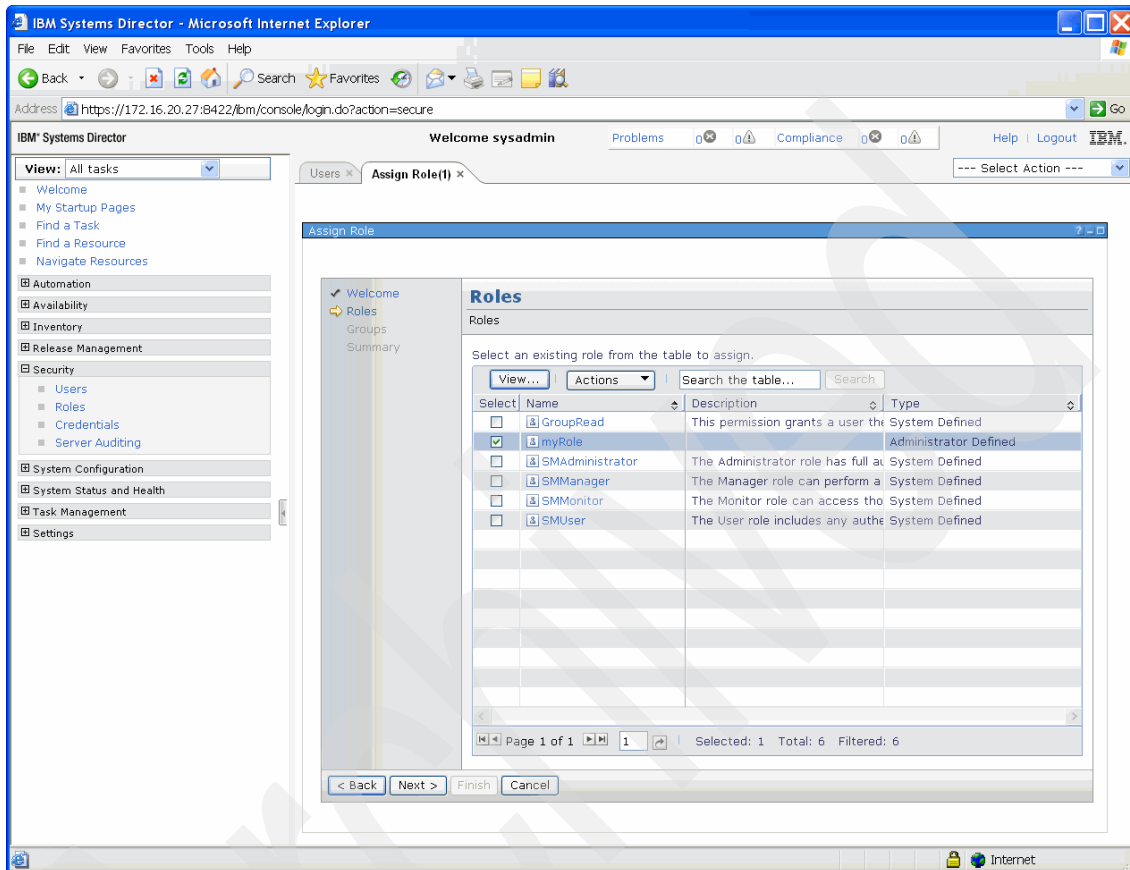


Figure 9-15 Assign Role wizard: Roles page

3. Select the roles you want to assign to this user and click **Next** to open the Groups page (Figure 9-16). Multiple groups can be selected, and their resources are added to the set of resources defined for this user.

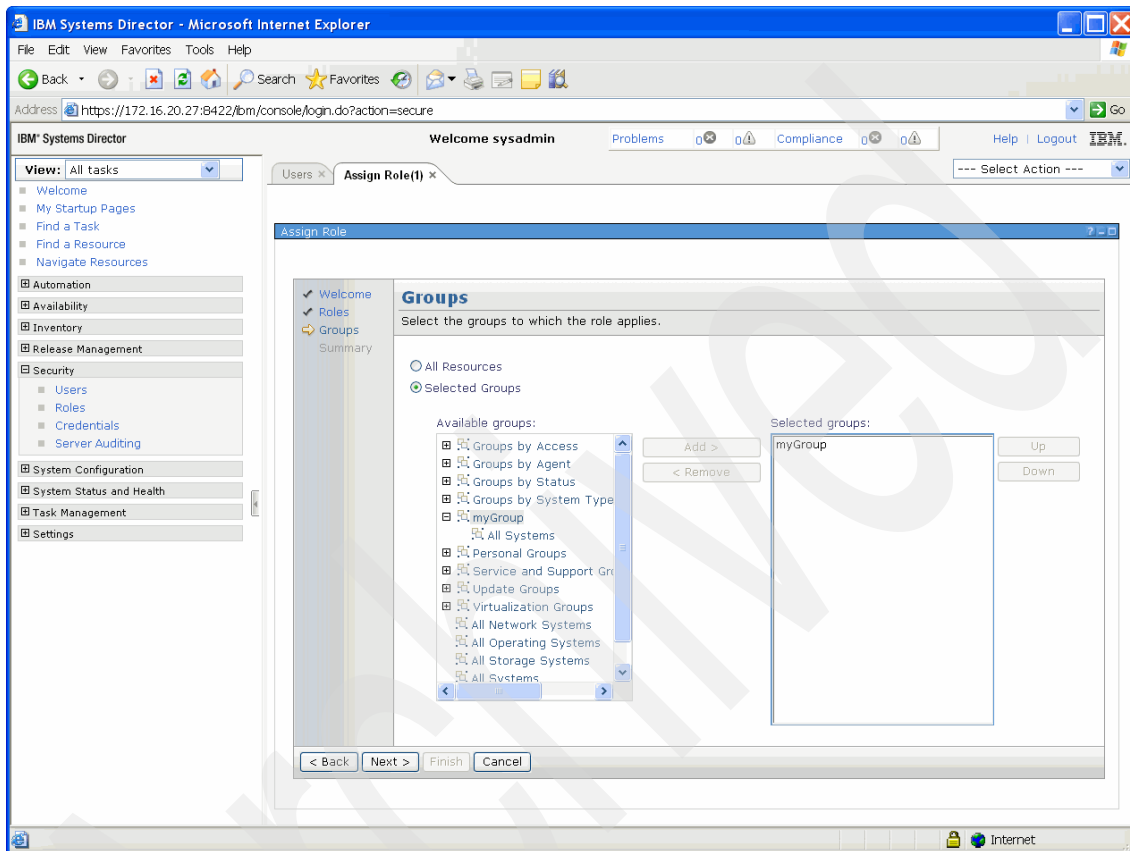


Figure 9-16 Assign Role wizard: Groups

4. Click **Next** to open the Summary page, which lists permissions and groups assigned to the user (Figure 9-17). Click **Finish** to assign the role to the user selected in the first step. This step authorizes the user to perform only those operations that are defined in this role on resources defined in the assigned group.

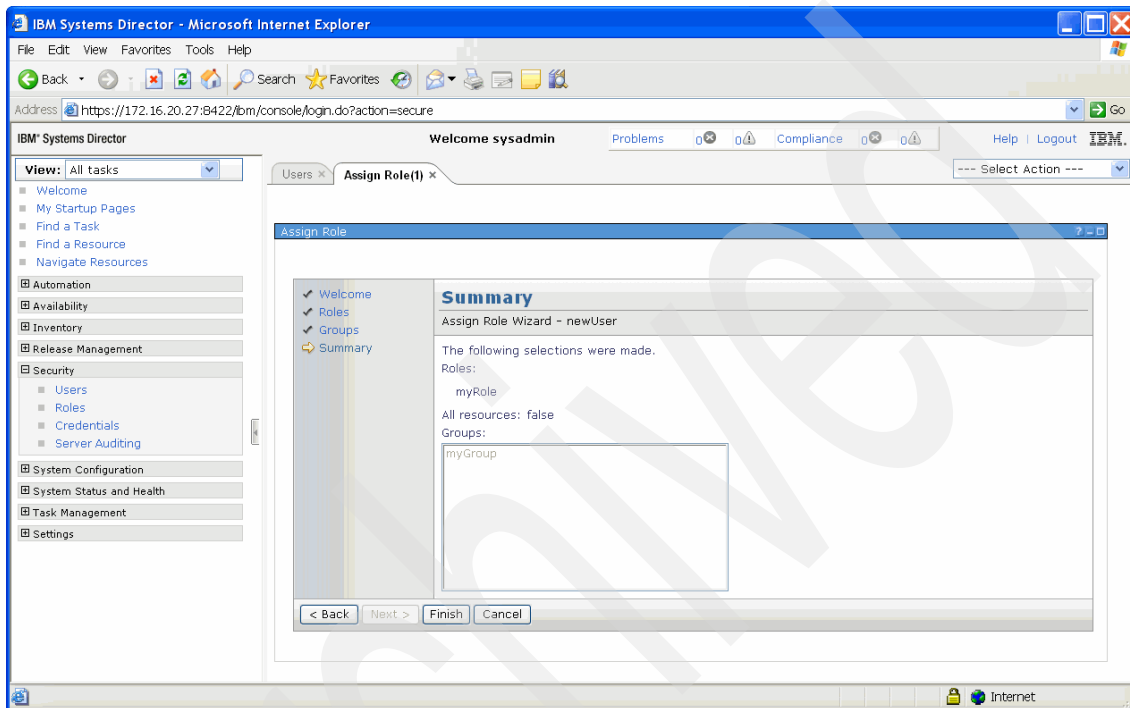


Figure 9-17 Assign Role: Summary

9.1.4 User authentication and authorization

The SDMC uses the user and group information stored in the employed user registry for the purpose of authentication.

After authentication, a user can access the system. However, to access a specific resource or perform a specific task, the user must also have the appropriate authorization. Authorization prevents unauthorized management servers or rogue managed-system applications from accessing the resources.

Authentication methods

Three different authentication methods can be used with SDMC. They are:

- ▶ Local authentication
- ▶ LDAP
- ▶ Kerberos

Note: Unlike IBM Systems Director, SDMC can create local users on the underlying operating system. Although the task in SDMC is called Create User Account, it only applies to local user accounts.

LDAP and Kerberos users must exist beforehand, using the means of user creation appropriate to those authentication methods.

9.1.5 User management

User management consists of user creation, changing attributes of the user, and removing users. In the SDMC, this job is started as a background task and handed to the appropriate agent for execution, so it can take a bit of time before the results appear in the user interface.

Creating a user

If the user does not exist in the SDMC, it can be created. This section discusses how to use the GUI to perform this task.

Local authentication

To perform local authentication, perform the following steps:

1. Log on to the SDMC as a user that has the SMAdministrator role and thus can create new users. From the Welcome page, click the **Settings** tab and then click **Create user account** (Figure 9-18).

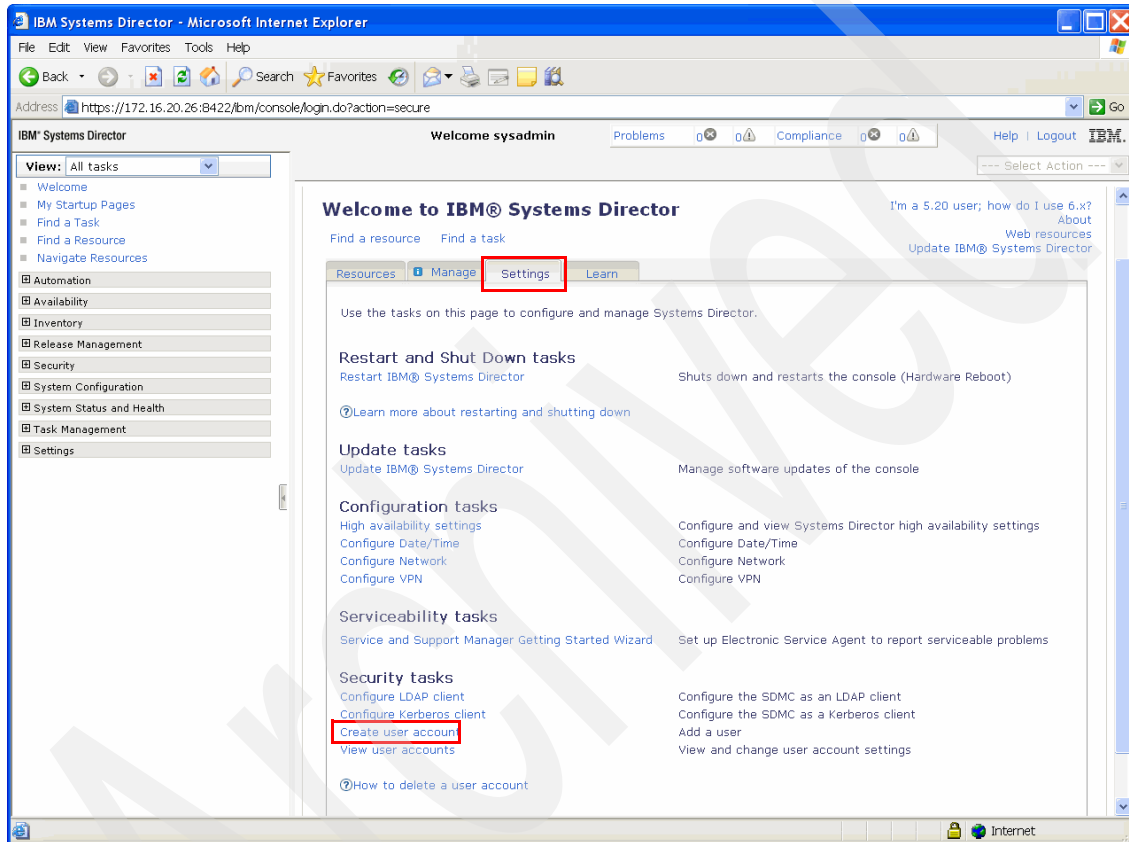


Figure 9-18 Welcome page

2. A page opens where the user credentials can be specified. Refer to Figure 9-19 for the following discussion. Enter the user credentials and click **OK**.

The following fields are required for local authentication:

- User ID
- Password
- Verify password

Note that in the annotated field the Authentication type is set to Local OS.

Welcome sysadmin Problems Compliance Help Logout

--- Select Action ---

Create User Account

Use this page to create a new Systems Director user account.

*User ID:

Description:

SSH Session time-out (minutes):

Authentication type: [Learn more...](#)

*Password:

*Verify password:

Password expires in (days):

Kerberos principle name: [Learn more...](#)

User groups: [Learn more...](#)

☐ smadmin Systems Director Server Administrators
☐ smmgr Systems Director Server Managers
☒ smuser Systems Director Server Users (default)
☐ smmon Systems Director Server Monitors

Figure 9-19 Create User Account page

Optionally, you can specify a user description (Description), an SSH session timeout (the default is 0, which means no SSH session timeout), and an password expiration (the default is 180 days).

By default, the box for membership in the smuser local OS group is checked. If necessary, the group membership can be changed or added to by checking the boxes for the smadmin, smmgr, and smmon local OS groups.

The **mkuser** command can also be used to create a user. Example 9-7 shows an example of how to accomplish this task. For detailed information about the command's options, refer to Table A-31 on page 383 or run the **smcli mkuser --help** command.

Example 9-7 Creating a user using the CLI

```
sysadmin@sdmca:~> smcli mkuser -u newUser -p newPassword -g smadmin
User created successfully
```

To list the newly created user and their properties using the command line, issue the **smcli lsuser** command (Example 9-8).

Example 9-8 Listing a user using smcli lsuser

```
sysadmin@sdmca:~> smcli lsuser
newUser
pe
root
sysadmin
```

LDAP

SDMC can use an LDAP server to authenticate and authorize a user logging in. LDAP is an open protocol that uses TCP/IP to provide access to directories that support an X.500 model. Managing user information with LDAP instead of the local operating system is particularly useful when there is a large number of users who use the SDMC.

Additionally, there are advantages to user handling in LDAP, even if the number of users in SDMC is small:

- ▶ Many companies already have existing LDAP directories of employees that can be used for SDMC user management. These existing directories save the time and effort required to create new user accounts on the management server.
- ▶ An administrator can immediately modify or terminate a user's access on all instances of SDMC by changing the user's LDAP group memberships or by removing the user's LDAP entry.

- Users need only one user ID and password, as opposed to multiple accounts for each management server.

Note: Order might matter when configuring the SDMC as an LDAP client. If LDAP authentication and authorization is switched on, all user authentication and authorization relies on it. To avoid unwanted effects, make sure that users with sufficient properties exist in LDAP beforehand.

Important: You are required to gather at least the following information before configuring LDAP authentication for SDMC. Run `man cfgldap` to learn more information regarding LDAP configuration if you use the `smcli cfgldap` command to configure LDAP.

- LDAP server host name or IP address.
- LDAP port number: Default open port =389, SSL port =636.
- LDAPAdminUser or the binding distinguished name (dn) and password.

This is the user that SDMC uses to bind to the LDAP server using non-anonymous binding. Both anonymous and non-anonymous binding are supported on IBM Systems Director.

- Search Base information

Essentially, this should be the scope of search for user accounts on an LDAP server. Typically, it will be the root portion or the search base of the directory hierarchy that you want to search.

For successful configuration, the attributes of search filter, user filter, group filter, and login attribute are required, as shown in Example 9-9. The administrator for the LDAP server in question should be able to give you the information needed.

If you enabled SSL, refer to *Implementing IBM Systems Director 6.1*, SG24-7694.

Before LDAP authentication for a new user can be used, the LDAP client needs to be configured. To configure an LDAP Server for the SDMC using the command line, a user in the smadmin group can use the `cfgldap` command. A sample output is shown in Example 9-9.

Example 9-9 Structure of the cfgldap command

```
cfgldap --operation s --server ldapserver.mycompany.com --port 389
--base ou=People,dc=ldapserver,dc=mycompany,dc=com
--searchfilter '(&(uid=%v)(objectclass=ePerson))'
--binddn cn=Administrator,dc=ldapserver,dc=mycompany,dc=com
```

```
--bindpw password --loginattr uid
--groupfilter '(|(objectclass=groupOfNames)(objectclass=groupOfUniqueNames))'
--userfilter '(objectclass=ePerson)'
--memberattr member --descattr description
```

Note: After configuring SDMC for LDAP authentication and authorization using the **cfgldap** command, restart SDMC so that the changes can take effect.

Use the **smcli lsldap** command to display information about the current LDAP configuration of the SDMC.

Another method to configure SDMC for LDAP user management is by using a GUI. In the Welcome page, select **Security Tasks** → **Configure LDAP client**, as shown in Figure 9-20, to start LDAP client configuration.

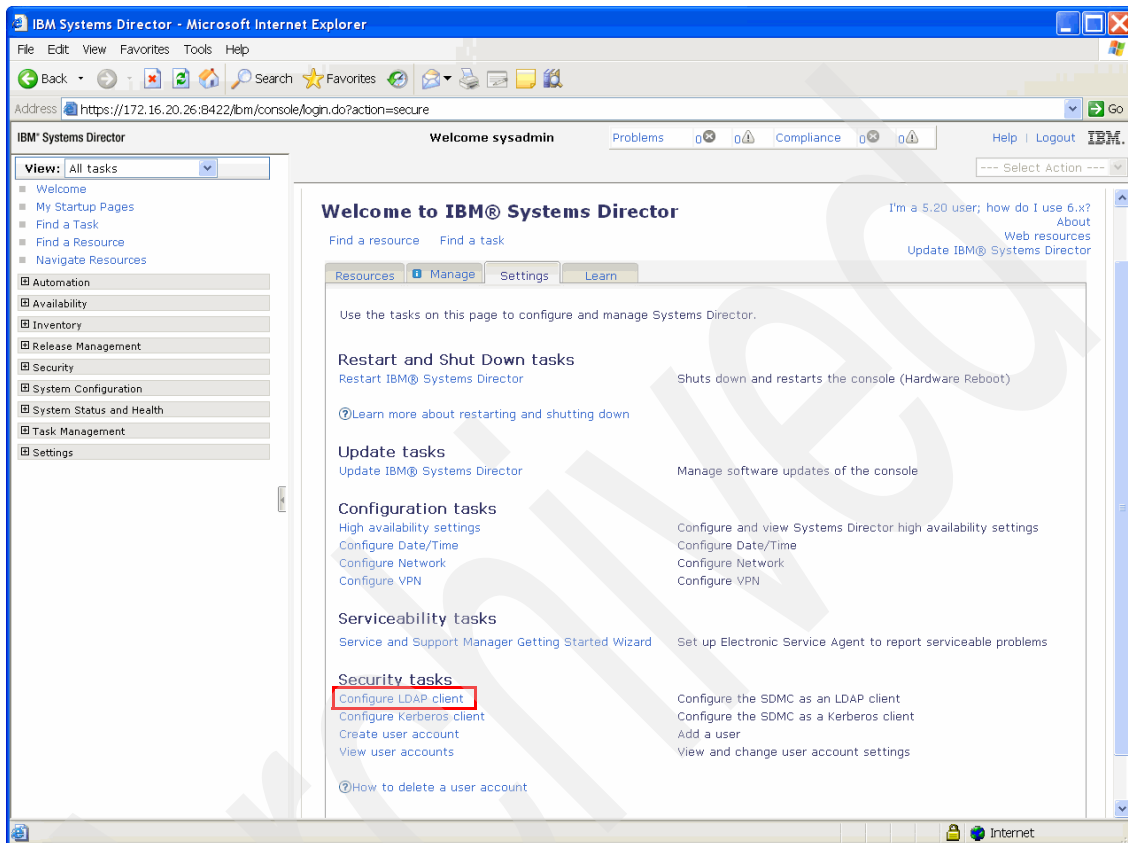


Figure 9-20 Configure an LDAP client

After clicking the link, the Welcome page of the Configure LDAP client wizard walks you through the required steps to access information on the LDAP server. Because this configuration is exactly the same as in IBM Systems Director, refer to the information provided in *Implementing IBM Systems Director 6.1*, SG24-7694.

The Welcome page of the LDAP client configuration wizard is shown in Figure 9-21.

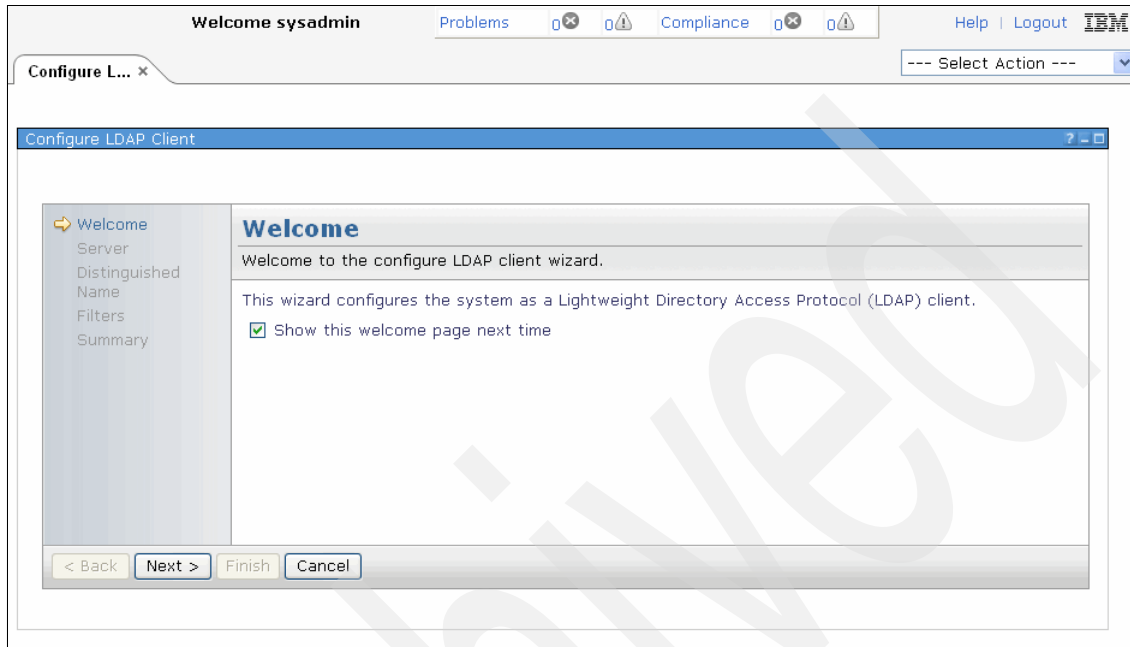


Figure 9-21 Configure LDAP client wizard

After configuring the LDAP client, a user can be added to the SDMC by clicking **Create user account** on the Welcome page (Figure 9-18 on page 224). You must instruct the Create User Account wizard to use LDAP as the authentication method by clicking the **Authentication type** drop-down menu and selecting **LDAP**. You do this task because SSH access to the SDMC is only possible with a user defined to the base operating system. Therefore, you should also define a SSH timeout to that user while creating it. The Pluggable Authentication Modules (PAM), a modular user authentication method on Linux and other operating systems) on the base operating system then uses LDAP for user authentication and authorization.

Figure 9-22 shows how to create a user for LDAP authentication. No other information is needed besides the user name that must already exist on the configured LDAP server, so all the other input fields are disabled.

The screenshot shows the 'Create User Account' window in the IBM Systems Director Management Console. The window title is 'Create User Account'. Below the title bar, there's a message: 'Use this page to create a new Systems Director user account.' The form contains several fields:

- *User ID:** A text field containing 'newUser'.
- Description:** A large, empty text area.
- SSH Session time-out (minutes):** A text field containing '0'.
- Authentication type:** A dropdown menu with 'LDAP' selected. This field is highlighted with a red rectangular box.
- Password:** A disabled text field.
- Verify password:** A disabled text field.
- Password expires in (days):** A text field containing '180'.
- Kerberos principle name:** A disabled text field.
- User groups:** A section with a 'Learn more...' link and four checkboxes:
 - ☐ smadmin Systems Director Server Administrators
 - ☐ smmgr Systems Director Server Managers
 - ☒ smuser Systems Director Server Users (default)
 - ☐ smmon Systems Director Server Monitors

 At the bottom of the window are three buttons: 'OK', 'Cancel', and 'Help'.

Figure 9-22 Create User Account: LDAP

For command-line usage, Example 9-10 gives an example of how to use the **mkuser** command with LDAP authentication for the specified user.

Example 9-10 mkuser command with LDAP credentials

```
sysadmin@sdmca:~> smcli mkuser -u newUser -x usertype=ldap
User created successfully
```

Note: A user with LDAP authentication can be created anytime, regardless of the LDAP client configuration. However, access to the system is denied as long as the LDAP client for the SDMC is not configured. To avoid unwanted effects, make sure that the user created has sufficient privileges to access the SDMC after the LDAP client has been configured because all authentication and authorization is then switched to LDAP!

Kerberos

SDMC allows for Kerberos authentication. A detailed configuration walkthrough is out of the scope of this book. Refer to *Implementing IBM Systems Director 6.1*, SG24-7694 for a thorough explanation about how to perform this task.

To configure a Kerberos Server for the SDMC on the command line, a user in the smadmin group can issue the **cfgkrb** command. A sample output is shown in Example 9-11.

Example 9-11 Structure of the cfgkrb command

```
sysadmin@sdmca:~> cfgkrb -o s -r MYREALM.COM -s kerberos.mycompany.com  
Operation completed successfully.
```

SDMC can be configured as a Kerberos client in the GUI by clicking the **Configure Kerberos client** link on the Welcome page (Figure 9-23).

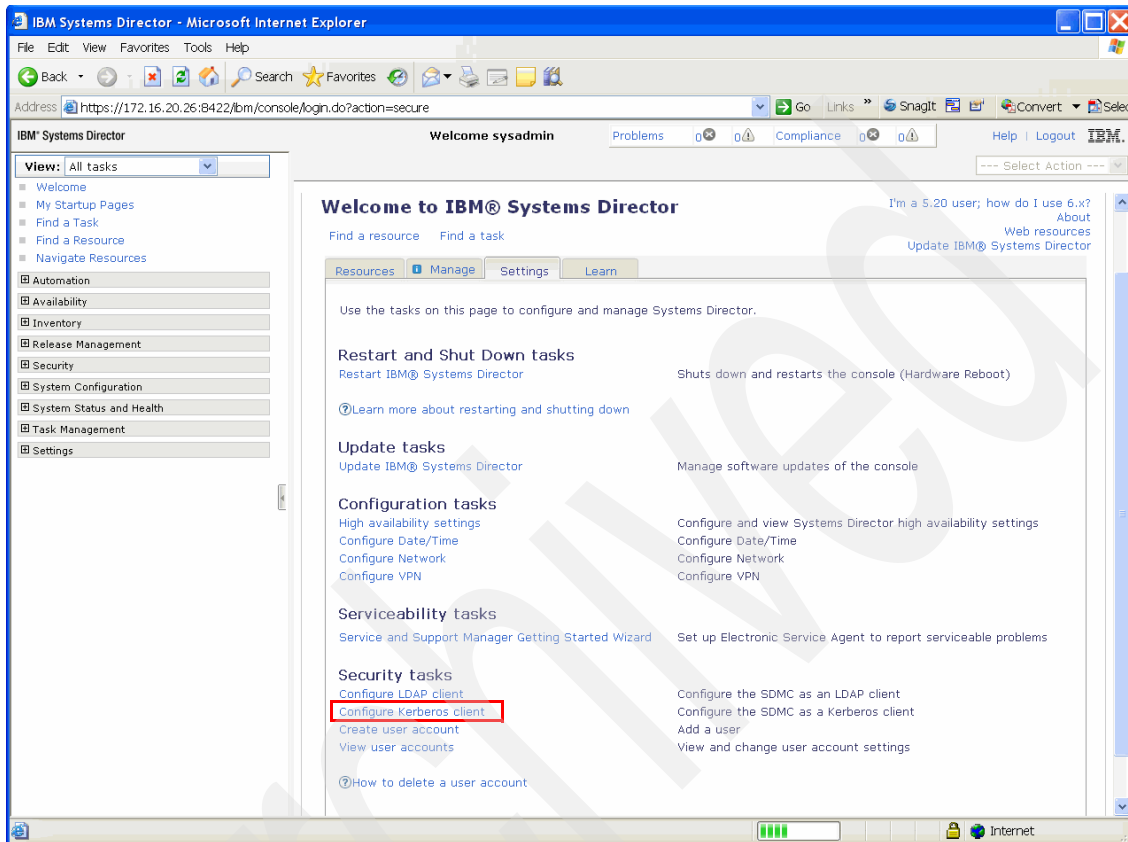


Figure 9-23 Configure Kerberos client page

After clicking the link, a wizard walks you through the required steps to complete this task (Figure 9-24).

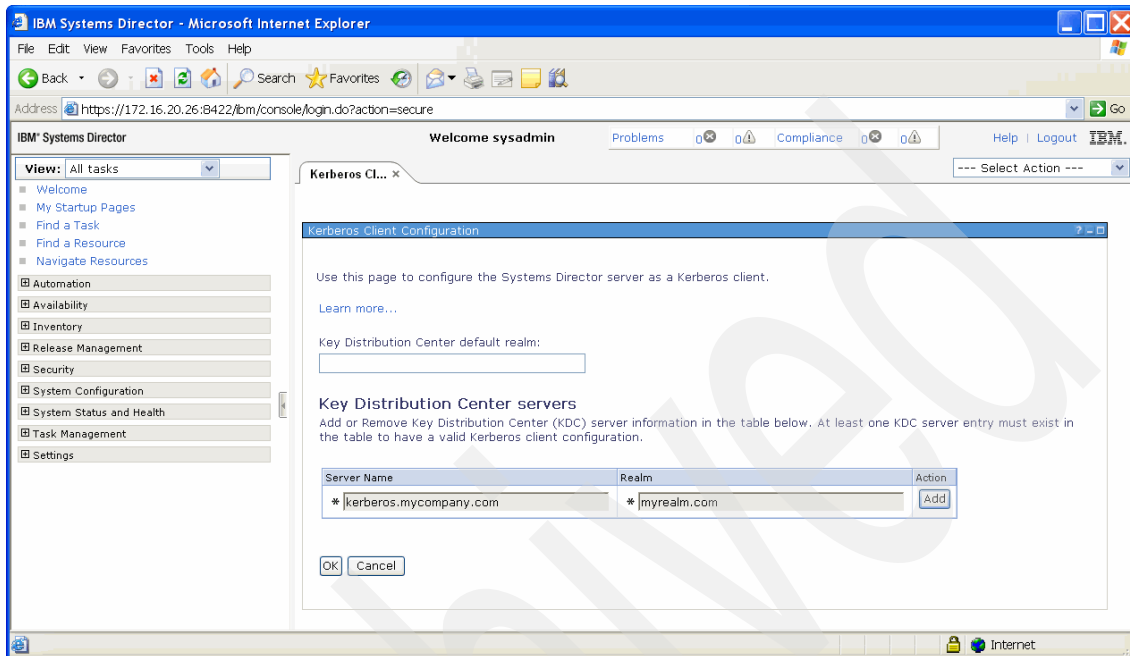


Figure 9-24 Kerberos Client Configuration wizard

After configuring the Kerberos client, a user can be added to the SDMC by clicking **Create user account** in the Welcome page (Figure 9-18 on page 224). The Create User Account wizard then must be instructed to use Kerberos as authentication method by setting the Authentication type select box to **Kerberos** (Figure 9-25). Kerberos is used then for authentication only, and authorization takes place with the values retrieved from the user registry, for example, the local user registry in the base operating system or LDAP. Only the password is retrieved from the Kerberos server.

Welcome sysadmin Problems Compliance Help | Logout

--- Select Action ---

Create User Account

Use this page to create a new Systems Director user account.

*User ID:

Description:

SSH Session time-out (minutes):

Authentication type: [Learn more...](#)

Password:

Verify password:

Password expires in (days):

Kerberos principle name: [Learn more...](#)

User groups: [Learn more...](#)

☐ smadmin Systems Director Server Administrators
☐ smmgr Systems Director Server Managers
☒ smuser Systems Director Server Users (default)
☐ smmon Systems Director Server Monitors

Figure 9-25 Create user account: Kerberos

Example 9-12 provides an example about how to use the **mkuser** command with Kerberos authentication for the specified user.

Example 9-12 mkuser command with Kerberos credentials

```
sysadmin@sdmca:~> smcli mkuser -u newUser -x usertype=kerberos  
User created successfully
```

Note: A user with Kerberos authentication can be created anytime, regardless of the Kerberos client configuration. However, access to the system is denied as long as the Kerberos client for the SDMC is not configured.

Modifying user properties

After the new user account has been created, its properties can be modified.

To accomplish this task, expand **Security** in the left pane of the SDMC interface. Click **Users** to open the Users page (Figure 9-26).

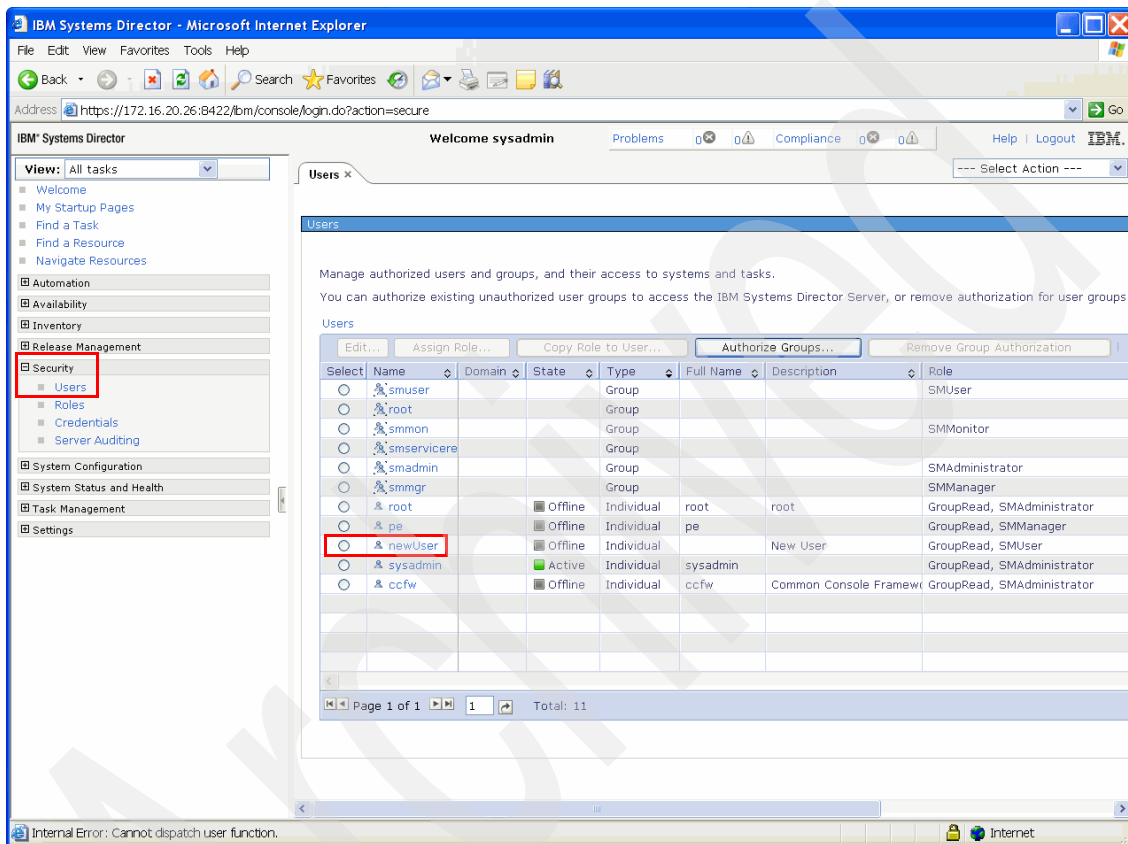


Figure 9-26 Users page

Click the newly created user to open the User properties page (Figure 9-27). In this figure, the general properties of the user are shown and can be modified by clicking **Edit**.

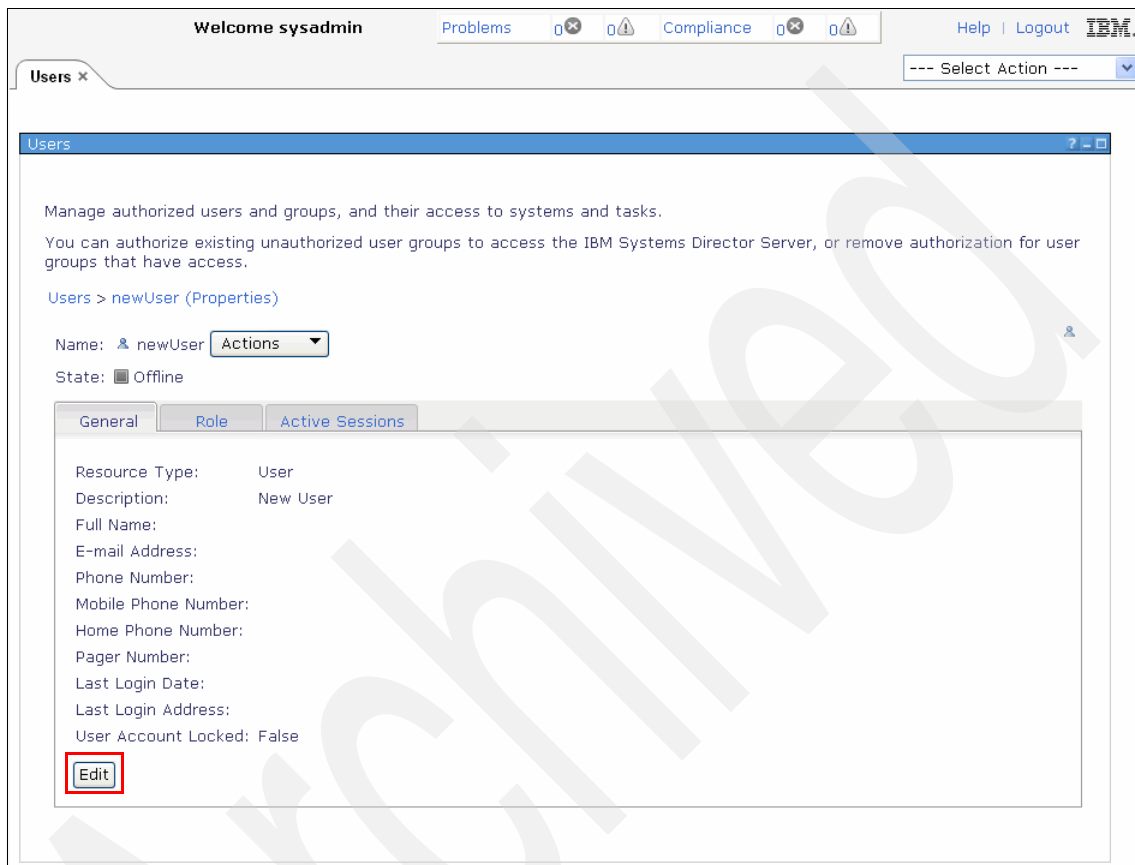


Figure 9-27 User properties page

All of the listed attributes can be changed except the first two, which were defined when the user was created. Figure 9-28 shows how you can change those attributes.

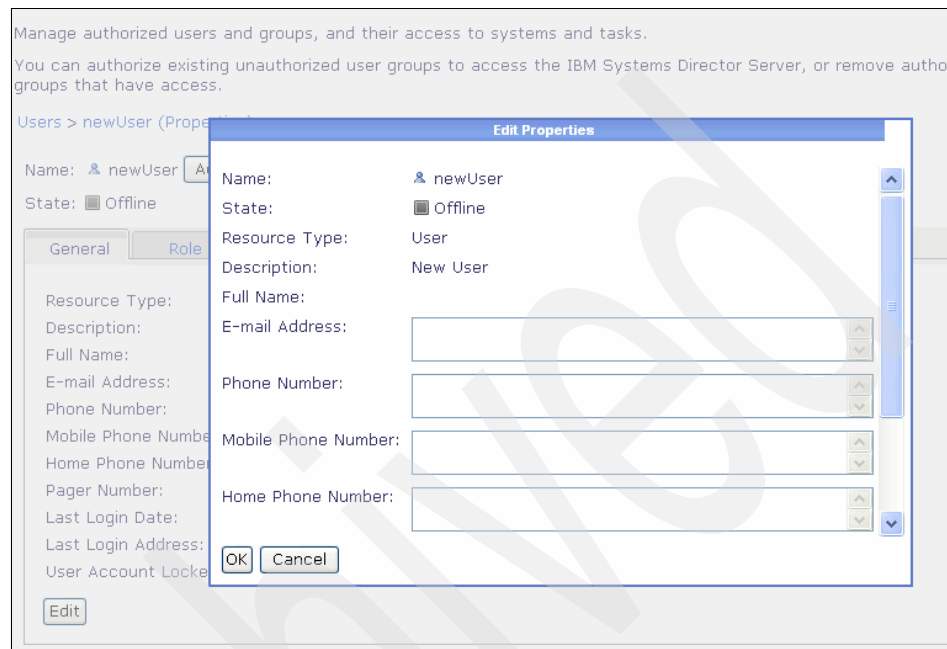


Figure 9-28 Edit user properties: General tab

It is also possible to modify the user information using the **smcli chuser** command (Example 9-13). This addresses another set of user attributes, namely those that can be set with the **mkuser** command. Be aware that this is nearly the same set of attributes that are in the HMC, whereas the GUI wizard allows you to change user attributes in the IBM Systems Director component of the SDMC.

Example 9-13 Changing a user using the smcli chuser command

```
sysadmin@sdmca:~> smcli chuser -u newUser -d "SDMC user" -p "password"
User modified successfully
```

For a list of user attributes that can be changed by using the **smcli chuser** command, run **man chuser**.

Deleting users

To remove a user using the command line, run `smcli rmuser` (Example 9-14).

Example 9-14 Deleting a user with the smcli rmuser command

```
sysadmin@sdmca:~> smcli rmuser -u newUser  
User deleted successfully
```

In the GUI, there is a link at the bottom of the **Welcome** → **Settings** page that explains how to remove a user.

9.2 Network configuration

This section describes the network configuration of the SDMC with the GUI and the CLI and how to test the network configuration.

The connection between the SDMC and its managed systems can be implemented either as a private or open network (see Figure 2-1 on page 18). The term open refers to any general, public network that contains elements other than SDMCs and service processors (FSP) that is not isolated behind a firewall.

In a private service network, however, the only elements on the physical network are the SDMC and the service processors of the managed systems. In addition, the SDMC provides Dynamic Host Configuration Protocol (DHCP) services on that network, which allow it to automatically discover and assign IP configuration parameters to those service processors. You can configure the SDMC to select one of several different address ranges to use for this DHCP service, so that the addresses provided to the service processors do not conflict with addresses used on the other networks to which the HMC is connected. The DHCP services allow the elements on the private service network to be automatically configured and detected by the SDMC, while at the same time preventing address conflicts in the network.

On a private network, therefore, all of the elements are controlled and managed by the SDMC. The SDMC also acts as a functional firewall, isolating that private network from any of the open networks to which the SDMC is also attached. The SDMC does not allow any IP forwarding; clients on one network interface of the SDMC cannot directly access elements on any other network interface.

To take advantage of the additional security and ease of setup, implement service network communications through a private network. However, in some environments, this is not feasible because of physical wiring, floor planning, or control center considerations. In this case, the service network communications can be implemented through an open network. The same functionality is available on both types of networks, although the initial setup and configuration on an open network require more manual steps.

Recommendation: For the SDMC, set up a private network with DHCP managed by the SDMC or an open network if using a static IP address.

9.2.1 Configuring network settings

Here are the steps for how to set up the network. These can be done either for the private or the open network or for both of them in one step.

Note: Eventually you have to do further steps for network setup on the hypervisor host configuration (VMware or KVM), if you use a Director software appliance. Refer to 2.3, “Installation of the software appliance” on page 19 for more information about this topic.

To view and change the network settings go to the **Settings** tab on the Welcome page and, under Configurations tasks, select **Configure Network** (Figure 9-29).

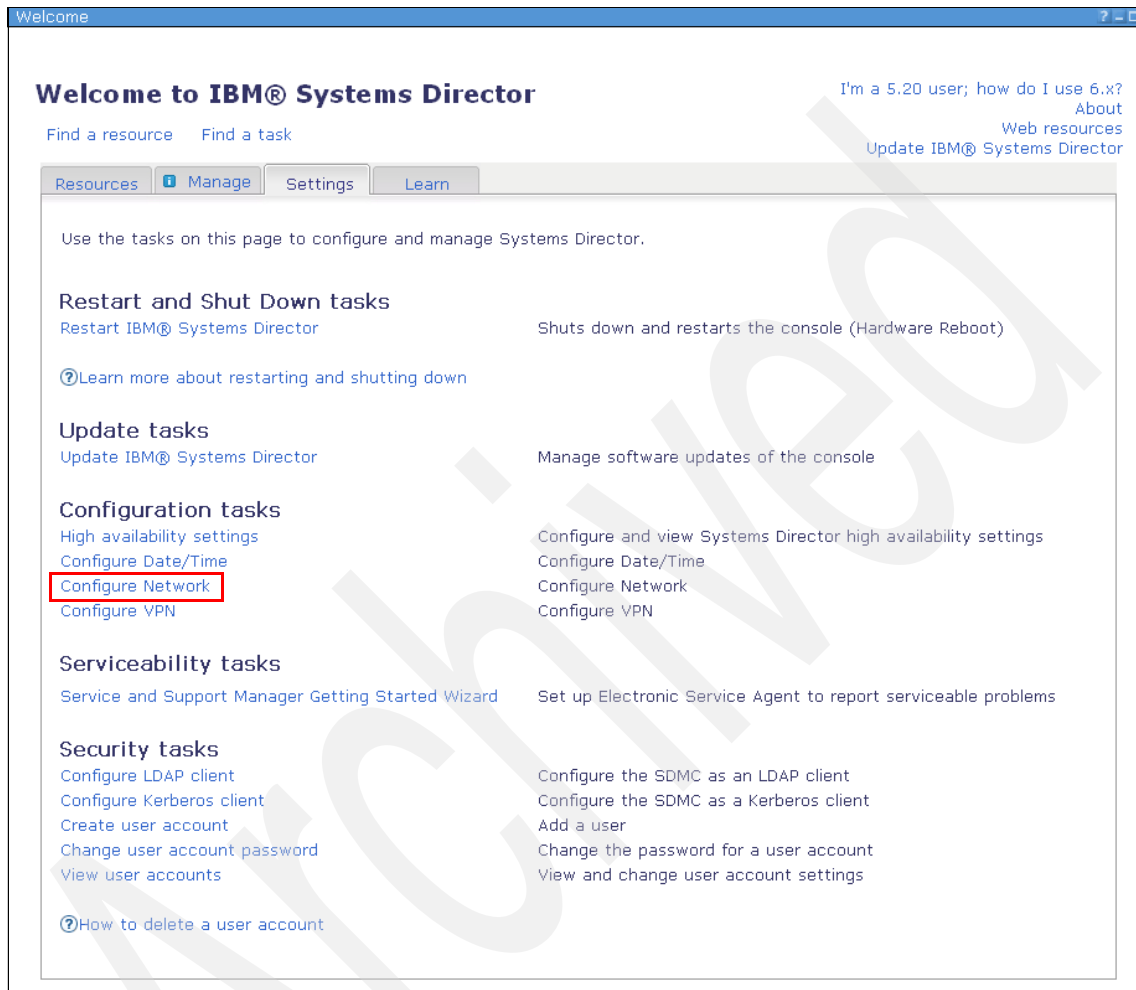


Figure 9-29 Configure Network on the Welcome page

When you select it, the network configuration wizard starts (Figure 9-30).

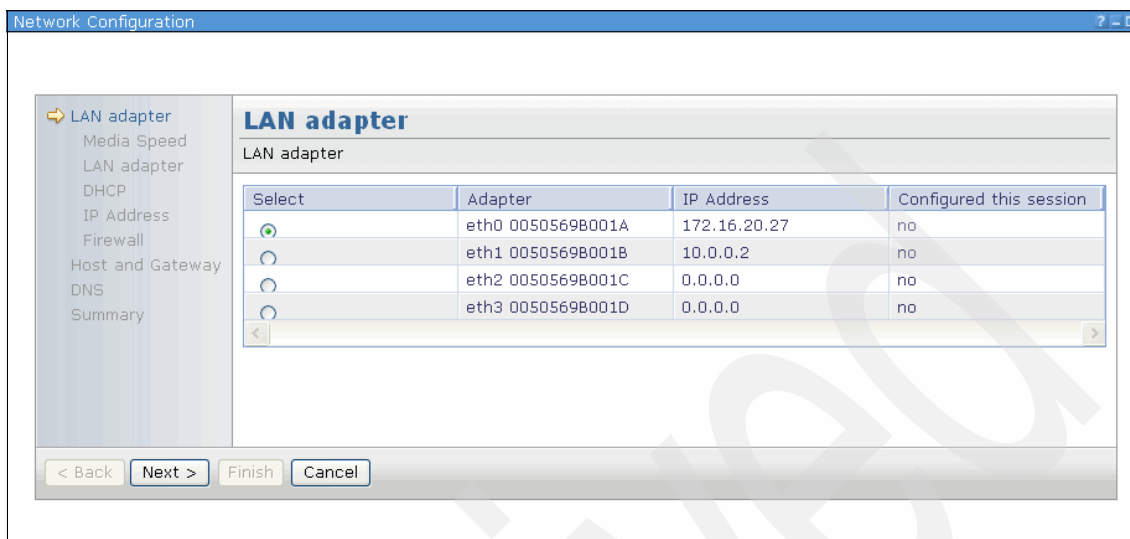


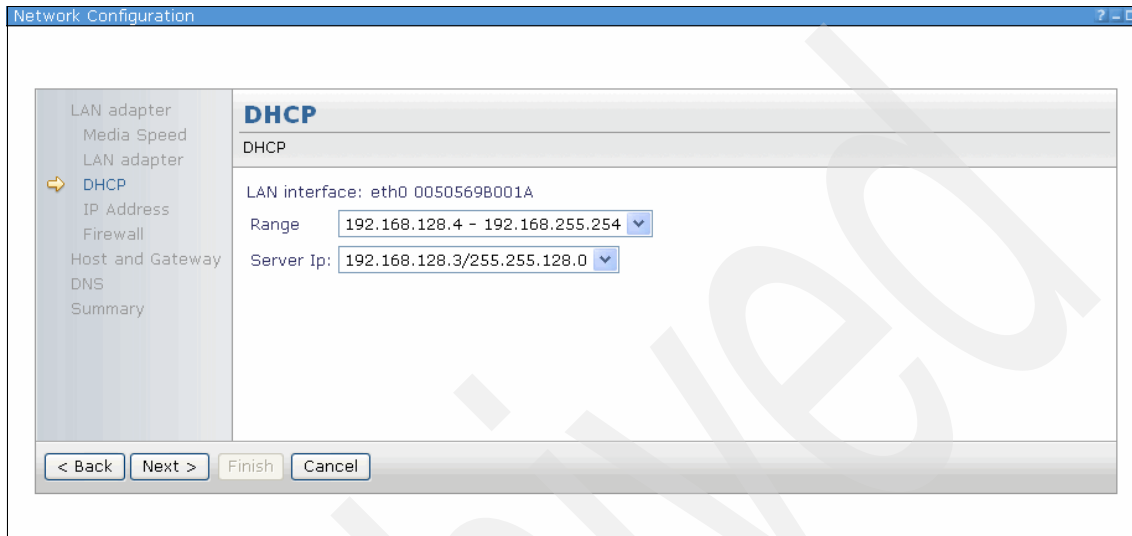
Figure 9-30 Network Configuration wizard

LAN adapter

In the first page, you have to select the LAN adapter you want to configure. After selecting and clicking **Next**, you have to decide if you will use **Standard network interface** or **Configure System as a DHCP server**.

DHCP

If you select **Configure System as a DHCP server**, you get a page where you can select a range for the DHCP server and select an address for the LAN adapter that serves as a DHCP server (Figure 9-31).



The screenshot shows a window titled "Network Configuration". On the left is a sidebar with a list of configuration options: "LAN adapter", "Media Speed", "LAN adapter", "DHCP" (highlighted with a yellow arrow), "IP Address", "Firewall", "Host and Gateway", "DNS", and "Summary". The main area is titled "DHCP" and contains the following fields:

- LAN interface: eth0 0050569B001A
- Range: 192.168.128.4 - 192.168.255.254 (with a dropdown arrow)
- Server Ip: 192.168.128.3/255.255.128.0 (with a dropdown arrow)

At the bottom of the window are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Figure 9-31 DHCP server

IP address

If you select **Standard network interface**, you get a page where you can select if you want to use IPv4 or IPv6 and if the interface will be a DHCP client or have a static IP address (Figure 9-32). If you select a static IPv4 address, you can specify the IP address and the network mask. In the case of a static IPv6 address, you can give the address and a list of prefix lengths.

Network Configuration

LAN adapter
Media Speed
LAN adapter
DHCP
➔ IP Address
Firewall
Host and Gateway
DNS
Summary

IP Address

IP Address

LAN interface: eth0 0050569B001A

☒ IP Address(IPV4)

☐ DHCP client

☒ Use the following IP v4 address

Static IP address:

Network mask:

☐ IPv6 Address

☐ DHCPv6 client

☒ Use the following IP v6 address

Add new static IPv6 address:

IPv6 address:

Prefix length:

Static IPv6 address table:

| Static IPv6 address | Prefix length | Remove |
|------------------------------|---------------|--------|
| There is no data to display. | | |

< Back Next > Finish Cancel

Figure 9-32 Setting a static IP address

Firewall

After selecting a DHCP or static IP address, the Firewall menu opens, where you can select which ports are allowed for the interface and which are not. You can restrict for which hosts traffic over a given port is allowed. Table 9-3 provides a list of the standard ports that are available for configuration with the application that corresponds to it and if it is allowed by default.

Recommendation: For the firewall settings, leave them at their defaults for the appliance. You can enable ports without harm if you have to, but if you turn off a port that is enabled by default, that action can interfere with the standard operations of the SDMC.

Table 9-3 Table of ports for the SDMC firewall

| Application | Port(s) | Allowed |
|----------------------------------------------------|---------------------|---------|
| Northbound remote interfaces default JMS ports | 61616:TCP,61617:TCP | Yes |
| Common Information Model (CIM) server ports | 15988:TCP,15989:TCP | Yes |
| Secure Shell | 22:TCP | Yes |
| Simple Network Management Protocol | 162:TCP,162:UDP | No |
| Service Location Protocol | 427:TCP,427:UDP | Yes |
| Microsoft® SQL Server Database | 1433:TCP | No |
| Oracle Database | 1521:TCP | No |
| Apache Derby Database | 1527:TCP | Yes |
| IBM Systems Director Interprocess Communication | 2033:TCP,4066:TCP | Yes |
| Smcli command-line interface | 2044:TCP | No |
| File Transfer Protocol | 20:TCP,21:TCP | No |
| Trivial File Transfer Protocol | 69:TCP | No |
| Serial Attached SCSI Switch | 6641:TCP | No |
| Common Information Model (CIM) Listener | 6988:TCP,6989:TCP | Yes |
| IBM Systems Director Console HTTPS Access | 8422:TCP | Yes |

| Application | Port(s) | Allowed |
|------------------------------------------------|----------------------------|---------|
| IBM Systems Director Console HTTP Access | 8421:TCP | No |
| Common Agent Service(CAS) | 9510:TCP | Yes |
| Agent Manager | 9511:TCP,9512:TCP,9513:TCP | Yes |
| LWI Nonstop Port | 9514:TCP,9515:TCP | Yes |
| Event Received Port | 13991:UDP | No |
| IBM DB2® Universal Database™ databases | 50000:TCP | No |
| Storage Event Port | 10000:TCP | No |
| CAS Event Port | 20000:TCP | Yes |
| IPC Support | 14251:UDP | Yes |
| Virtual Network Computing | 5901:TCP | No |
| IPC Support for Director 5.20 | 14247:UDP | Yes |
| CIM Server Port | 5988:TCP,5989:TCP | Yes |
| Incoming Ping | echo-request:ICMP | Yes |
| Incoming IPv6 Ping | echo-request:ICMPv6 | Yes |
| Network Time Protocol | 123:UDP | No |
| ibminfocenter_NAME | 8091:TCP | Yes |
| IBM Tivoli System Automation for Multiplatform | 12347:UDP,12348:UDP | Yes |
| Resource Monitoring and Control | 657:UDP,657:TCP | Yes |
| Distributed Replicated Block Device | 7788:TCP | Yes |
| Java™ Message Service High Availability Port | 61619:TCP | Yes |
| FCS (Redundancy communication services) | 9920:TCP,9900:UDP | Yes |
| Virtual TTY | 9735:TCP | Yes |
| Virtual TTY Proxy | 2302:TCP | Yes |
| 5250 Console Terminal | 2300:TCP,2301:TCP | Yes |

| Application | Port(s) | Allowed |
|-------------------------------------|----------|---------|
| HW Server | 8899:TCP | Yes |
| Distributed Replicated Block Device | 7789:TCP | Yes |
| Remote Web Access (HTTP) | 80:TCP | Yes |
| Remote Web Access (HTTPS) | 443:TCP | Yes |
| Information Center | 8091:TCP | Yes |

After configuring the firewall, the LAN adapter page opens again, where you can choose to configure another Interface using the **Select another Adapter** option. If you do not want to configure another interface, click **Continue Wizard**.

Host and gateway

In the next page, you can specify a host name, a domain name, and a gateway address (Figure 9-33).

The screenshot shows a 'Network Configuration' window with a sidebar on the left containing 'LAN adapter', 'Host and Gateway' (selected), 'DNS', and 'Summary'. The main area is titled 'Host and Gateway' and contains the following fields:

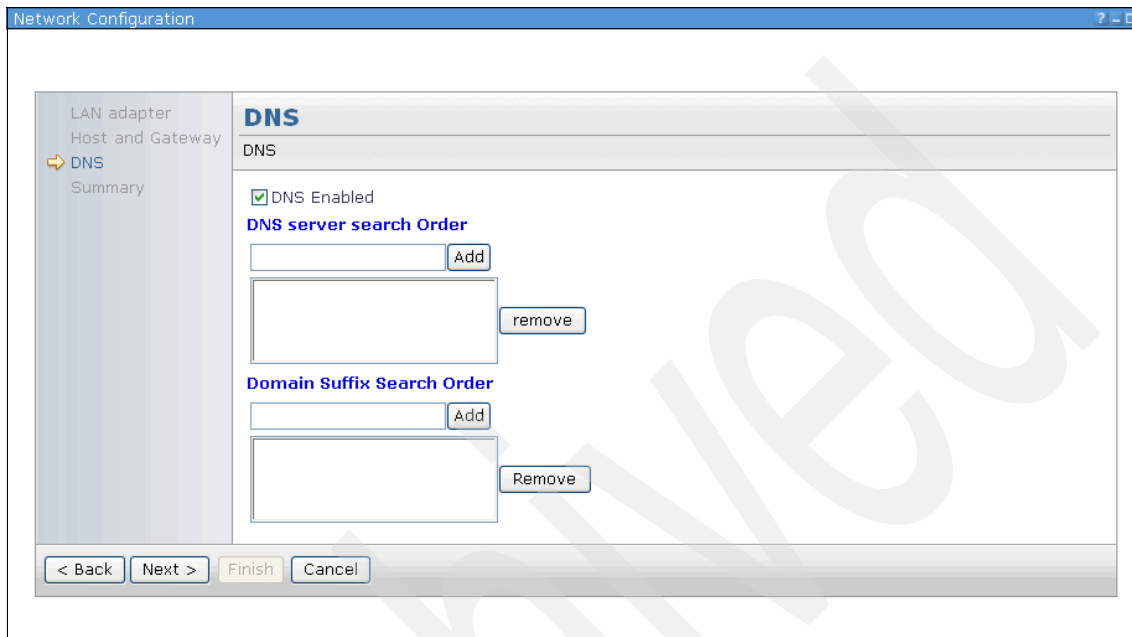
- Specify IP for Hostname: 172.16.20.27 (dropdown)
- Host Name: sdmc2 (text box)
- Doman Name: itsot1.ibm.com (text box)
- Gateway Address: 172.16.20.1 (text box)
- IPv6 gateway: (empty text box)
- eth0 (dropdown)
- ☐ Enable 'routed'

At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

Figure 9-33 Host and Gateway menu

DNS

In the next page, you can specify one or more Domain Name Services (DNS) server and build a domain search order (Figure 9-34).



The screenshot shows a window titled "Network Configuration" with a sidebar on the left containing the following items: "LAN adapter", "Host and Gateway", "DNS" (highlighted with a yellow arrow), and "Summary". The main content area is titled "DNS" and contains the following elements:

- A checkbox labeled "DNS Enabled" which is checked.
- A section titled "DNS server search Order" with an input field and an "Add" button.
- A list box containing one empty entry, with a "remove" button to its right.
- A section titled "Domain Suffix Search Order" with an input field and an "Add" button.
- A list box containing one empty entry, with a "Remove" button to its right.

At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Figure 9-34 DNS menu

Summary

In the last page of the wizard, you receive a summary of your selections. You can always go back and make some changes to your selections. If you are satisfied with your selection, click the **Finish** button.

Network reconfiguration

In the next page, a job is scheduled for the reconfiguration of the network (Figure 9-35).

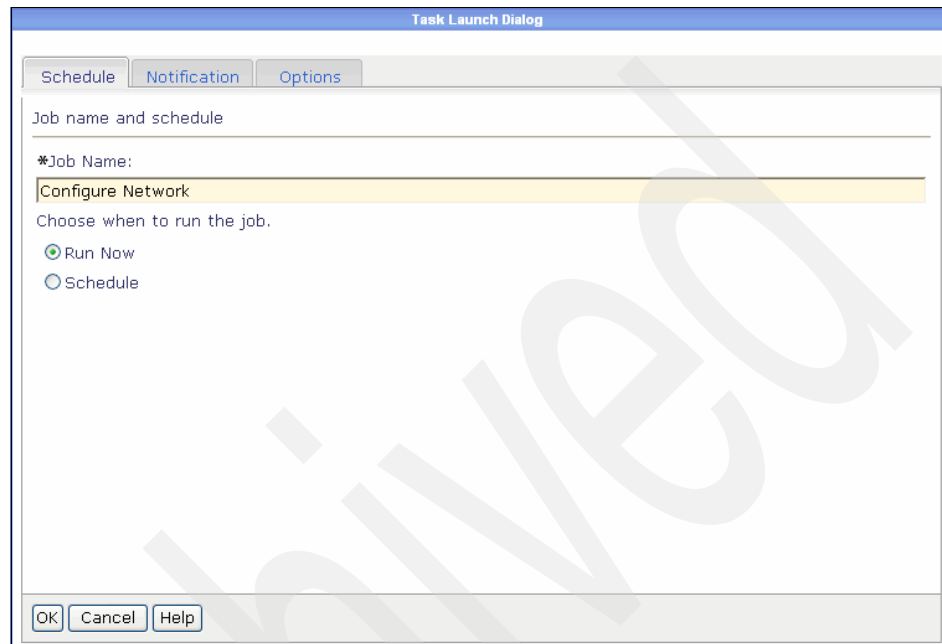


Figure 9-35 Job for network configuration

You should select **Run Now** and click **OK**.

You receive a notification about the scheduled job (Figure 9-36).

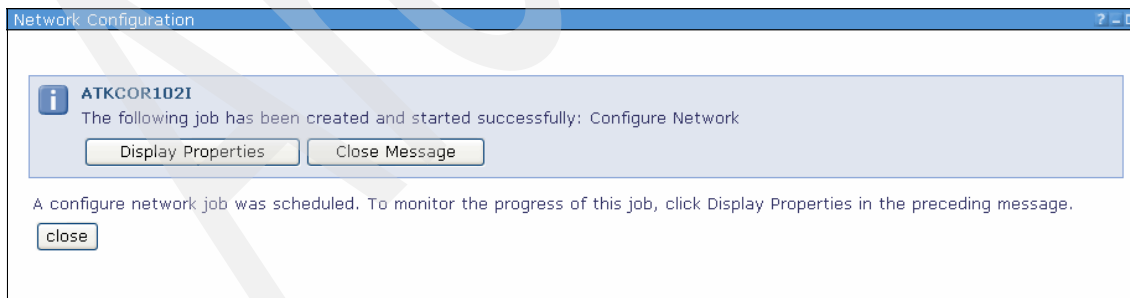


Figure 9-36 Job scheduled notification

You can close this page by clicking **close**. You can see the status of the job by selecting **Task Management** → **Active and Scheduled Jobs** (refer to Chapter 11, “Schedule operations” on page 289 for more information).

Most network changes require a reboot of the SDMC. When you get back to Configure Network page, you see the “Recent changes require a restart to be performed” message and an exclamation mark in front of the Configure Network task when a reboot is necessary (Figure 9-37).

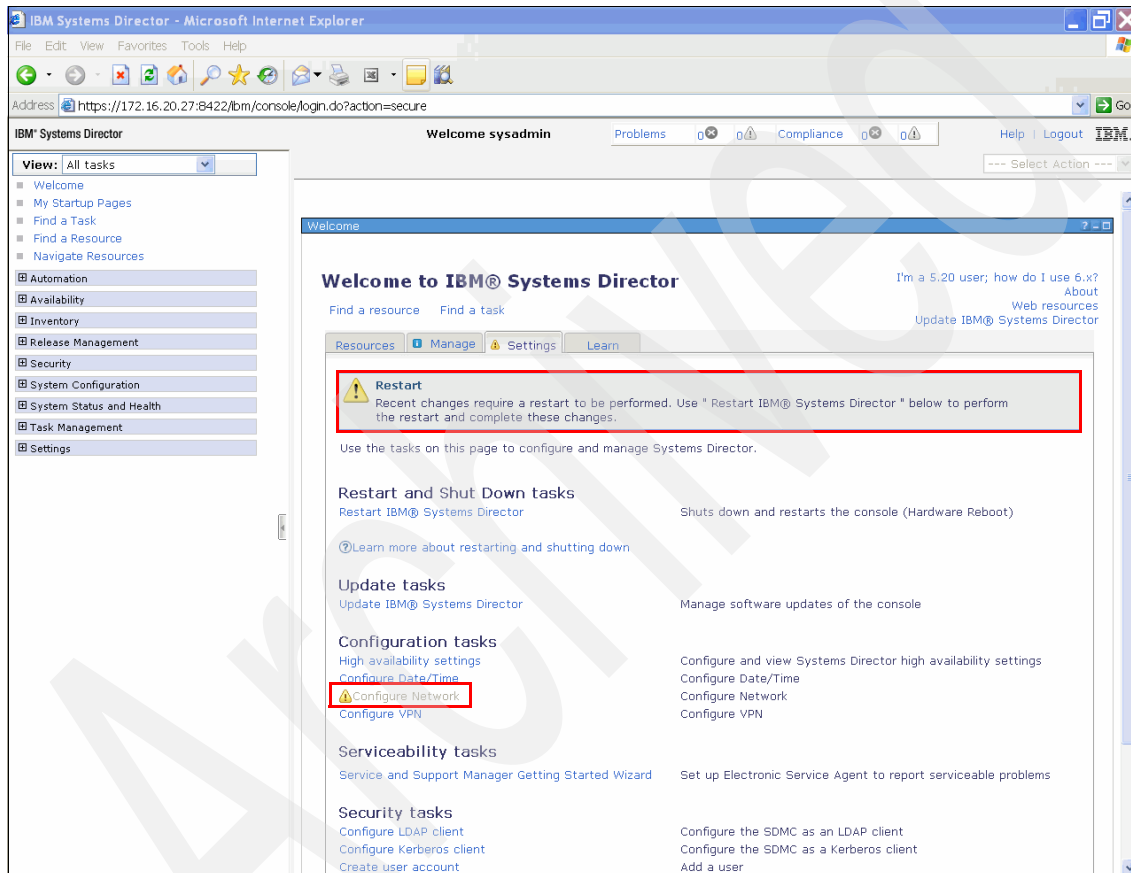


Figure 9-37 Restart necessary

Perform the steps under Restart IBM Systems Director as indicated.

9.2.2 Configuring network settings using the SDMC CLI

You can also view and change network settings using the SDMC CLI.

Viewing network settings

To view the network settings, use the **lsnetcfg** command. For example, to view all network settings, except the firewall settings, run the following command:

```
lsnetcfg -n
```

To view all the firewall settings, run the following command:

```
lsnetcfg -f
```

For further options, refer to the man page for **lsnetcfg**.

Note: The **lsnetcfg** command has to be used without the **smcli** prefix.

Changing network settings

To change network settings, you have to use the **chnetcfg** command. Using the **chnetcfg** command, you can add, modify, or remove entries, and you can enable and disable network services.

For example, to set the IP address and netmask for the network interface eth1, run the following example command:

```
chnetcfg -s modify -i eth1 -a 10.0.0.1 --netmask 255.255.255.0
```

To add DNS settings, run the following example command:

```
chnetcfg -s add -ns 172.16.20.1 -ds itso.ibm.com
```

To enable the Network Time Protocol (NTP), run the following example command:

```
chnetcfg -c xntp -s enable
```

For further examples and options, refer to the man page for **chnetcfg**.

Note: The **chnetcfg** command has to be used without the **smcli** prefix.

9.2.3 Testing network connectivity

The network connectivity can only be tested by using the **ping** command (Example 9-15); you cannot perform this function from the GUI, as you could in the HMC.

Example 9-15 Testing network connectivity using ping

```
sysadmin@sdmc2:~> ping sdmcl.itso.ibm.com
PING sdmcl.itso.ibm.com (172.16.20.26) 56(84) bytes of data.
64 bytes from sdmcl.itso.ibm.com: icmp_seq=1 ttl=64 time=0.075 ms
64 bytes from sdmcl.itso.ibm.com: icmp_seq=2 ttl=64 time=0.045 ms
64 bytes from sdmcl.itso.ibm.com: icmp_seq=3 ttl=64 time=0.052 ms
64 bytes from sdmcl.itso.ibm.com: icmp_seq=4 ttl=64 time=0.040 ms
64 bytes from sdmcl.itso.ibm.com: icmp_seq=5 ttl=64 time=0.069 ms
64 bytes from sdmcl.itso.ibm.com: icmp_seq=6 ttl=64 time=0.078 ms
```

9.3 Backup and restore

The SDMC provides the capability to back up the whole virtual machine on to a USB device or a remote secure FTP (SFTP) server, and restore the backup file from the USB device or remote FTP server. The restore is a full image deployment, and all existing virtual machine files are replaced by the backup files.

Both the SDMC hardware appliance and software appliance have different methods for backup and restore. The user uses the SDMC command line to back up the hardware appliance, and uses the backup tools provided by the underlying VMware or KVM hypervisor environments to back up the software appliance.

9.3.1 SDMC hardware appliance backup and restore

To back up or restore the Hardware Appliance, use the **backup** and **restore** commands to back up or restore the whole virtual image to the attached USB device or remote secure FTP (SFTP) server. The USB device can either be flash memory or an HDD.

At the time of writing, there is no GUI support for backup and restore.

Backup

To perform the backup, perform the following steps:

1. Check if the system is a Hardware Appliance.

If the system is Virtual Appliance, the backup method is different based on the hypervisor used on the host (RHEV-H Blue or VMWare). So the backup operation is permitted only when the system is a Hardware Appliance. Refer to 9.3.2, “SDMC software appliance backup and restore on VMWare” on page 256 and 9.3.3, “SDMC software appliance backup and restore on KVM” on page 261 for more information about software appliance backup and restore.

2. Check that the user who runs the backup has the authority to do so. It is predefined in the `role_permission.xml` file that only the root role has the authority to run backup and restore.
3. Before performing the backup, the appliance tests if the USB diskette driver or the remote secure FTP (SFTP) server are accessible.

Note: During testing, it was found that the rear USB ports were best at detecting USB media.

Note: If you are saving to a USB device, the USB device will be unmounted at the start of the backup. Do not mount the USB device while the backup is taking place. After the backup has completed, the drive can be mounted.

4. Optionally, stop the IBM Systems Director server. You can use the **backup** command to perform this task.
5. Run **backup** on the Systems Director Management Console.

The command has the following syntax:

```
backup [-l usb | sftp] [-s] [-d] [-u] [-p] [-Y] [-h | --help]
```

Where:

| | |
|-----------|----------------------------------------------------------------------------------------------------------------|
| -Y | Say Yes to all questions. |
| -l | The location to store the backup file. If sftp is specified, the -s argument is needed to set the SFTP server. |
| -s | Specify SFTP server when -l sftp is specified. |
| -n | Specify the restore file name with the abstract path, for example, data/backup/20101011.tar.gz. |
| -u | The user used to connect to the SFTP server. |
| -p | The password used to connect to the SFTP server. |

Here is our example of this command:

```
backup -l usb -Y
```

6. The **backup** command starts the IBM Systems Director in the background.
7. If you back up the system to a USB disk, remount the drive to see the backup file. Obtain the device name of the USB disk and mount it by running the following commands:

```
lsmediadev  
device=/dev/cdrom,mount_point=/media/cdrom,type=1,description=CD/DVD  
device=/dev/vdh1,mount_point=/media/vdh1,type=3,description=USB  
flash memory device
```

```
mount /media/vdh1  
ls -lah /media/vdh1
```

Restore

During a restore, the current appliance update version of the software must match the version of the backup up media, that is, during a full system recovery, the client may have to reload the system from the recovery media and then perform software updates until they are at the current version before a restore can be performed.

To perform the restore, perform the following steps:

1. Optionally, stop the IBM Systems Director server. You can use the **restore** command to perform this task.
2. Mount the device
 - To mount CD or DVD media, insert the media in the drawer
Run the **mount /media/cdrom** command
 - For a USB device, insert the media in the rear USB port
Run **lsmediadev** to determine the mount point.
Run the **mount /media/XXXX** command where XXXX is the mount point determined from the **lsmediadev** command
3. Run **restore** on the host.

The command has the following syntax:

```
restore [-l usb | sftp] [-s] [-d] [-u] [-p] [-Y] [-h | --help]
```

Where:

-Y Say Yes to all questions.

- l** The location to store the backup file. If sftp is specified, the -s argument is needed to set the SFTP server.
- s** Specify SFTP server when -l sftp is specified.
- n** Specify the restore file name with the abstract path, for example, /data/backup/20101011.tar.gz.
- u** The user used to connect to the SFTP server.
- p** The password used to connect to the SFTP server.

Here is our example of this command:

```
restore -l usb -Y
```

4. Restart the IBM Systems Director in the background.

Note: If you

9.3.2 SDMC software appliance backup and restore on VMware

The backup and restore of the SDMC software appliance is done by using the facilities provided by VMware and KVM to back up client virtual machines. In this section, we give the basic steps for performing this task in both VMware and KVM using the Snapshot™ capabilities of both; however, there are other tools and methods for backing up virtual machines that the user may also use for this purpose.

Note: The software appliance must be shutdown prior to taking a backup.

Steps for backup using VMware vSphere Client

Backup and restore for the SDMC software appliance on VMware is done by taking VMware snapshots using the vSphere Client.

Note: vSphere Client is only available for Windows and can be downloaded from either the VMware website or the web address of your local ESX(i) Server.

To perform a snapshot backup, perform the following steps:

1. Start the vSphere Client and log in.

2. Select the virtual machine which want to back up, right-click it, and select **Snapshot** → **Take Snapshot** (Figure 9-38).

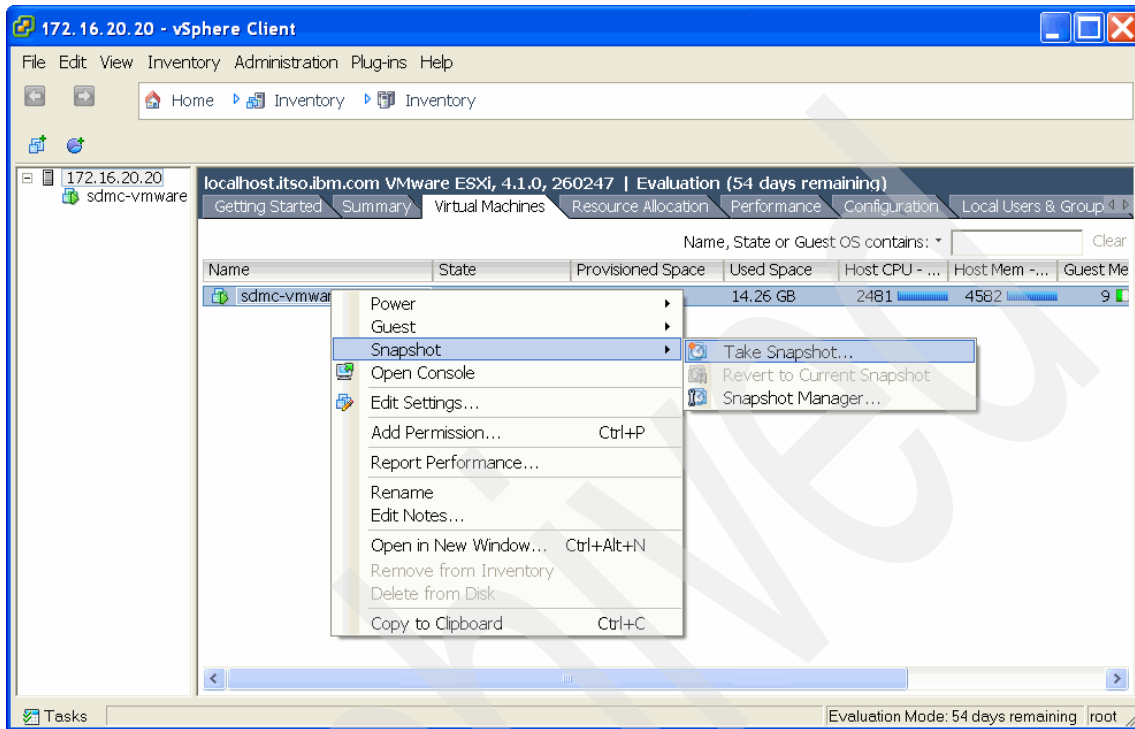


Figure 9-38 Take snapshot from vSphere client

3. Enter the snapshot name and description, and create a new snapshot of the selected VM (Figure 9-39).

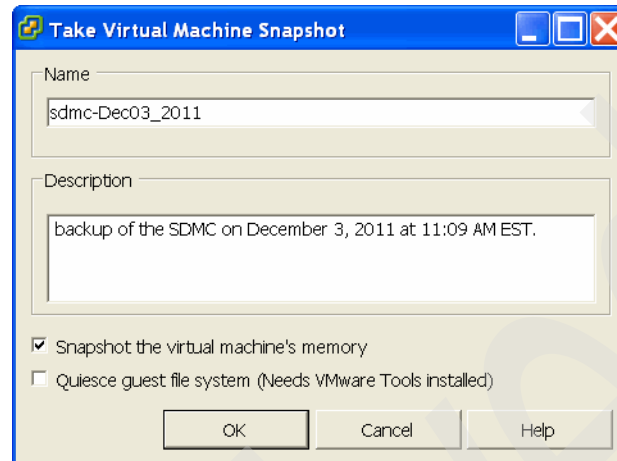


Figure 9-39 Take Virtual Machine Snapshot page

- The snapshot is stored on the host. To copy it to another reliable location, select the host in the vSphere Client, and click the **Summary** tab in the right column. In the Datastore section, right-click the **datastore1** item and select **Browse Datastore...** to open the Datastore Browser page (Figure 9-40).

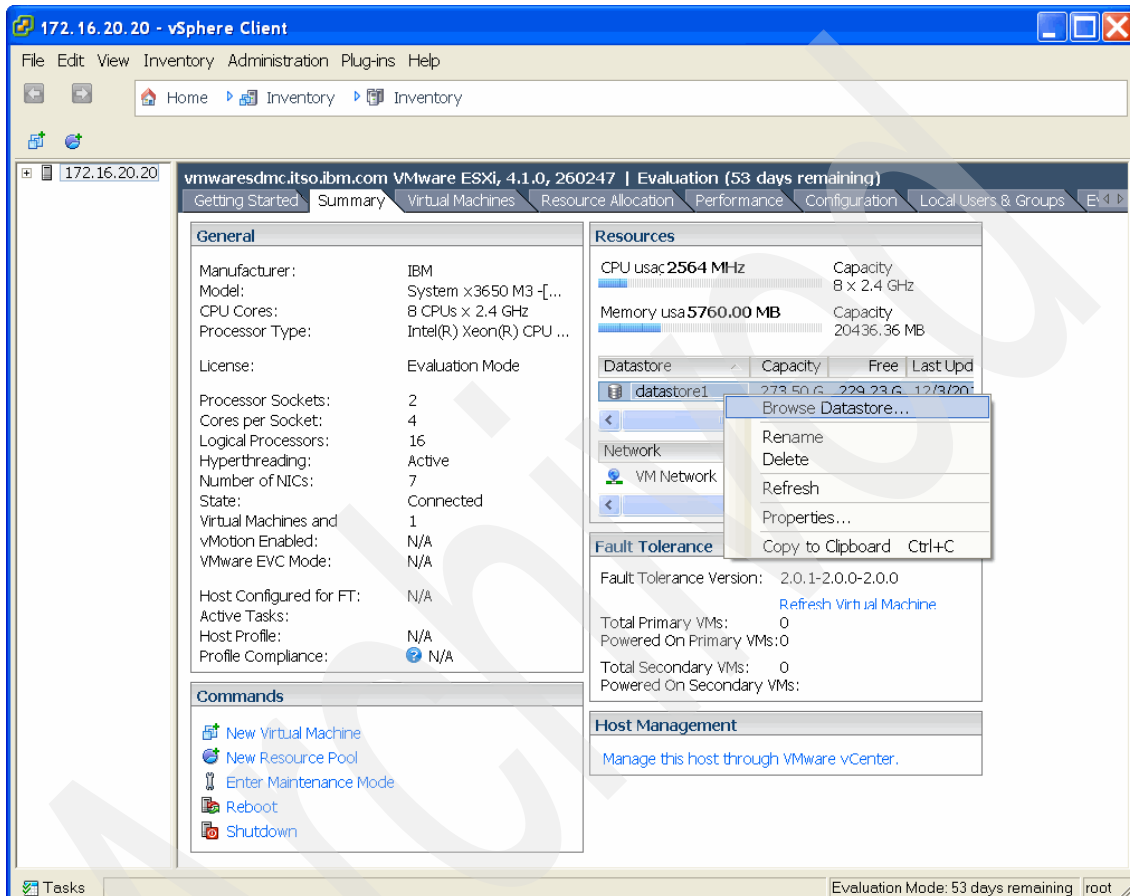


Figure 9-40 Selecting data store

- In the Datastore Browser, download the virtual disk and the associated snapshot files to any location. You can right-click the files you want to download and select **Download**.

Steps for restore using the VMware vSphere Client

To perform a restore using the VMware vSphere Client, perform the following steps:

1. Select the virtual machine that you want to restore using a specific snapshot.
2. Right-click the virtual machine and select **Inventory** → **Virtual Machine** → **Snapshot** → **Revert to Current Snapshot** to restore the most current snapshot (Figure 9-41).

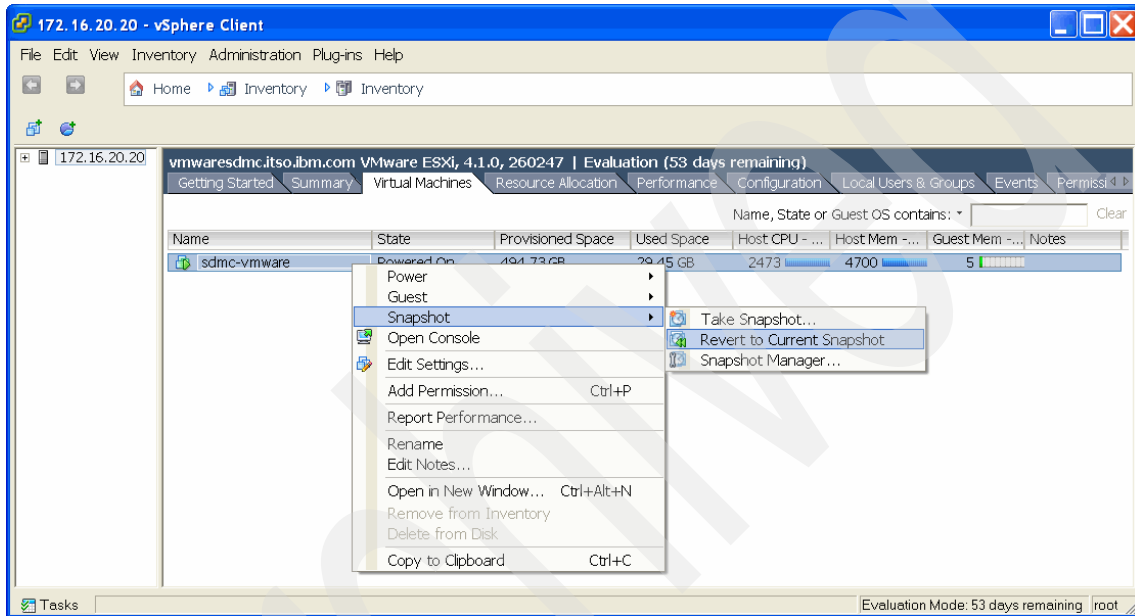


Figure 9-41 Revert to Current Snapshot

3. You can also select to restore from other snapshots by selecting the **Snapshot Manager** and choosing to restore from a specific snapshot. Select the snapshot to be restored and click the **Go to** button (Figure 9-42).

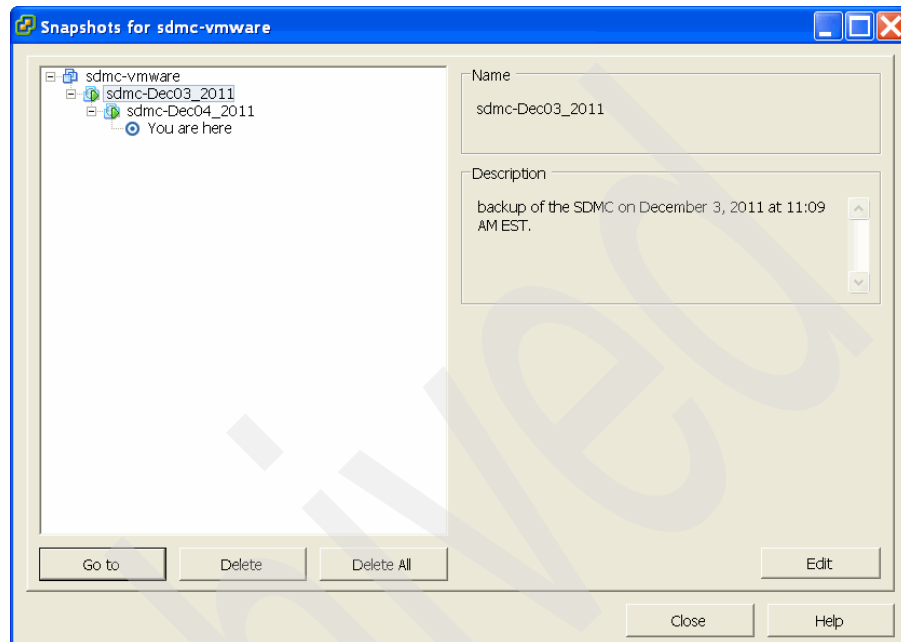


Figure 9-42 Snapshot manager

Note: The current state of the virtual machine is lost if you do not perform a snapshot of the current environment before restoring from another snapshot.

9.3.3 SDMC software appliance backup and restore on KVM

Backup and restore for the SDMC software appliance on KVM is done by using KVM LVM snapshots taken from the KVM command-line interface.

Note: The software appliance must be shutdown prior to taking a backup.

Note: The SDMC software appliance backup on KVM requires LVM support on the KVM host environment.

KVM backup procedure

The SDMC software appliance back up on KVM requires LVM support in the host environment. The system administrator must check if the host file system has at least 150 GB free disk space for the snapshot.

To back up the SDMC software appliance on KVM, complete the following steps:

1. Check for a minimum of 150 GB of available space by running the following command:

```
vgfs -o +vg_free_count,vg_extent_count
```

2. List the logical volumes by running the following command:

```
lvdisplay
```

3. Check for the logical volume with the /home directory by using the output of the **lvdisplay** command and by running the **mount** command:

```
mount
```

4. Create a logical volume snapshot of a virtual machine by running the following command:

```
lvcreate -L 150G -s -n vmisnapshot /dev/vg_kvmpel/1v_home
```

5. Check for the available space again by running the following command:

```
vgfs -o +vg_free_count,vg_extent_count
```

6. List the new snapshot logical volume:

```
lvdisplay |grep vmisnapshot
```

7. Create the */Snapshot_LV_Dir* directory to mount the snapshot logical volume by running the following command:

```
mkdir /Snapshot_LV_Dir
```

```
mount /dev/vg_kvmpel/vmisnapshot /Snapshot_LV_Dir
```

8. List the */Snapshot_LV_Dir* directory by running the following command. This is same as the listing for the */home* directory.

```
ls -l /Snapshot_LV_Dir
```

9. Check the disk space by running the following command:

```
df
```

10. Create the backup directory for the backup tarball or the */home/Backup_dir* directory if more space is required by running the following command. Alternatively, the tarball can be compressed directly to a USB key (16 GB minimum).

```
mkdir /Backup_Dir
```


11. Create the SDMC ***/Snapshot_LV_Dir/sdmc/data/images*** directory by running the following command:

```
cd /Snapshot_LV_Dir/sdmc/data/images/
```
12. Compress the ***Snapshot_LV_Dir/sdmc/data/images/**** directory and time it by running the following command:

```
time tar -Spczf /Backup_Dir/vmidata.tar.gz *
```
13. List the ***/Backup_Dir*** directory by running the following command:

```
ls -l /Backup_Dir/
```
14. If the tarball is not created directly on the USB key, insert a 16 GB USB key and look for the device to mount by running the following command:

```
fdisk -l  
mkdir /mnt/usb  
mount /dev/sdb1 /mnt/usb
```
15. Copy the backup tarball to a USB key by running the following command:

```
cp /Backup_Dir/vmidata.tar.gz /mnt/usb/.
```
16. Unmount and remove USB key by running the following command:

```
umount /mnt/usb
```
17. Unmount and delete the logical snapshot volume for future backups by running the following command:

```
cd  
umount /Snapshot_LV_Dir  
lvremove /dev/vg_kvmpELE/vmisnapshot  
Do you really want to remove active logical volume vmisnapshot?  
[y/n]: y
```

Restoring on KVM

To restore the SDMC software appliance on KVM, complete the following steps:

1. Copy the backup tarball to the ***/Backup_Dir*** directory from a mounted USB key if there is enough space by running the following command or directly extract from the USB key:

```
cp /mnt/usb/vmidata.tar.gz /Backup_Dir/.
```
2. Destroy the running virtual machine by running the following command:

```
virsh destroy sdmc-pele
```
3. Delete the ***/home/sdmc/data/images/**** directory by running the following commands:

```
cd /home/sdmc/data/images
```

```
ls
rm -rf *
```

4. Extract the tarball to the images directory and time it by running the following command:

```
time tar -zxvf /Backup_Dir/vmidata.tar.gz
```

5. Check the disk usage by running the following command:

```
dfStart the virtual machine by running the following command:
virsh start sdmc-pele
```

9.4 Problem determination

This section describes the various logs available for problem determination, how to view the logs, how to configure them, and how to capture them for transmitting them to IBM.

9.4.1 Available logs

SDMC has most of the same log files that were available on the HMC. The locations of the log files in SDMC are the same as on the HMC. Apart from these logs, SDMC has additional log files for IBM Systems Director.

Existing log files

Table 9-4 provides a quick snapshot of the log files available in SDMC. These log files existed on the HMC as well.

Table 9-4 Log files

| Log file | Description |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| /var/hsc/log/cimserver.log | This log file contains information related to command-line operations and core implementation logic. |
| /var/hsc/log/aca.log | This log file contains information related to security and user management. |
| /var/hsc/log/gui_server.log | This log files contains information related to SDMC operations using the graphical user interface. |
| /var/hsc/log/hdwr_svr.log | This log file contains information related to SDMC-managed system communication. This information includes the FSP commands and their responses. |

| Log file | Description |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------|
| /var/hsc/log/izdtrac.trm | This log files contains information related to Common Console Framework (CCFW). This framework is part of the SDMC GUI. |
| /var/hsc/log/hmclogger.log | This log file contains generic information about all operations done using SDMC. |

Trace logs in GUI

You can view the trace logs of the SDMC using the graphical user interface. This task is available only for the pe predefined user. The trace logs information opens a browser page. You can select the classes or you can specify the log file name to view specific log information. This interface is exactly the same as it was on HMC.

You can launch this task from the Settings tab of the Welcome page. When you click **View Trace Logs**, you should see the trace log information in a separate browser page (Figure 9-43).

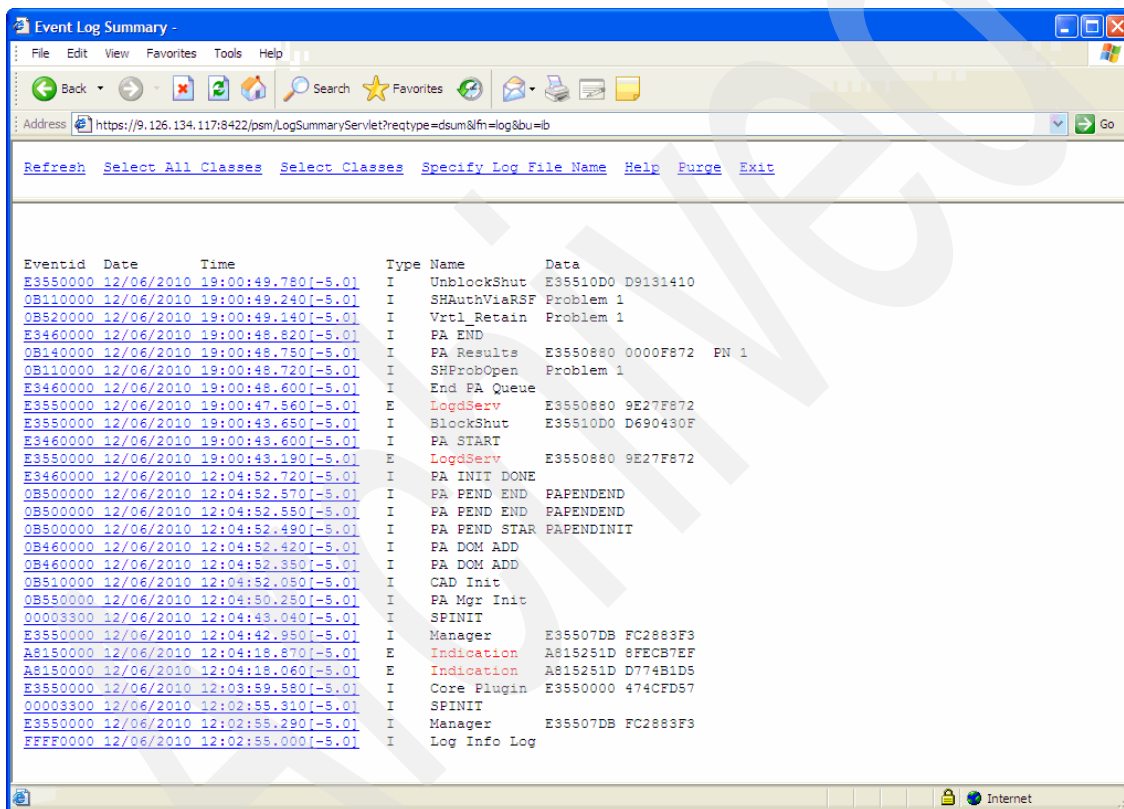


Figure 9-43 View Trace Logs

9.4.2 IBM Systems Director logs

The log files related to IBM Systems Director are located in the `/opt/ibm/director/lwi/logs/`. These log files are critical in determining and analyzing problems, mostly problems related to the GUI in SDMC. The available log files and their description are given in the Table 9-5.

Table 9-5 IBM Systems Director logs

| Log file | Description |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>/opt/ibm/director/lwi/logs/trace-log-*.html</code> | This file has trace information of all operations performed using the SDMC, which includes trace information about various managers of IBM Systems Director. |
| <code>/opt/ibm/director/lwi/logs/error-log-*.html</code> | This file contains information about all the errors scenarios that occurs in SDMC and other managers in IBM Systems Director. |
| <code>/var/hsc/log/izdtrac-director.trm</code> | This file contains information from the Director process running on SDMC. |

SDMC allows you to configure the settings for the trace and error logs. This task is available for the users with the SAdministrator role. Select **Console Logging and Tracing** under **Settings** in the navigation area. You should see the **Console Logging and Tracing Configuration** page as shown in Figure 9-44.

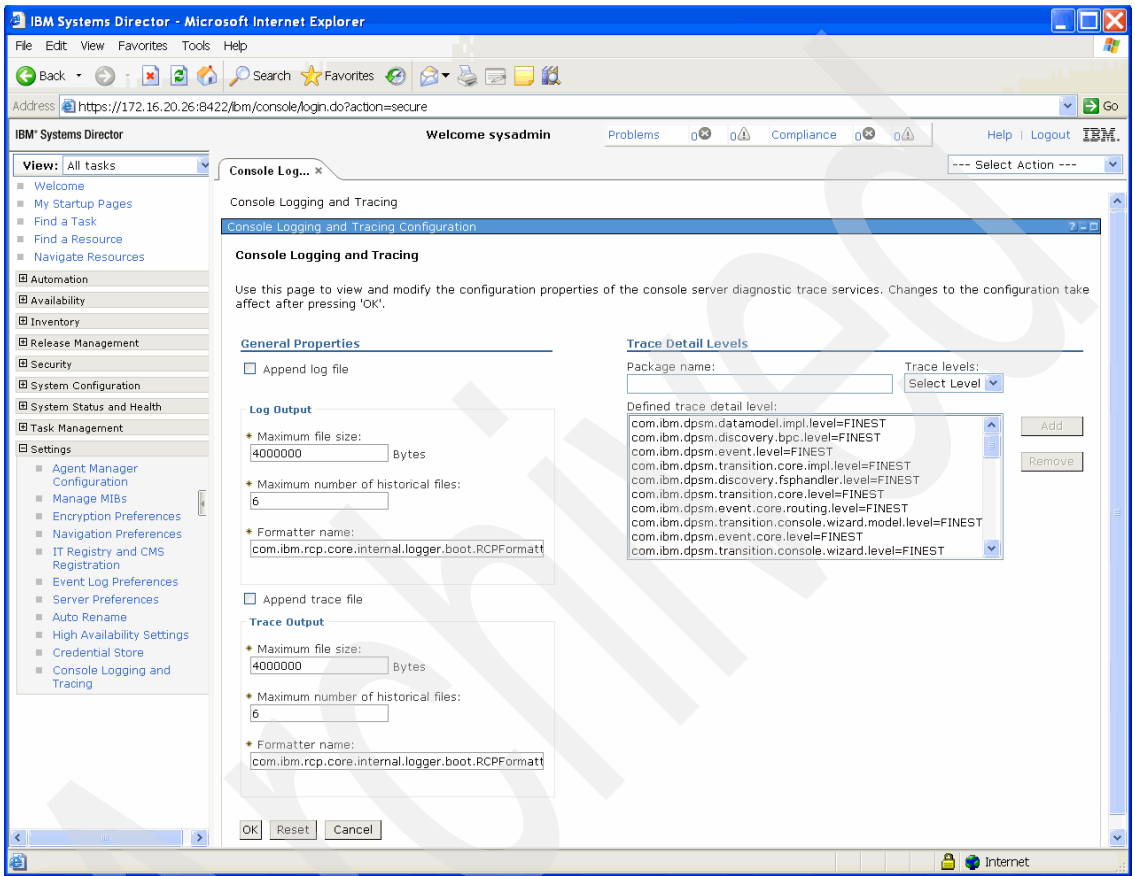


Figure 9-44 Console Logging and Tracing Configuration

Table 9-6 provides the details about the changes that you can make to logging and tracing configuration.

Table 9-6 Tracing and Logging settings

| Setting | Description |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Maximum file size | Changes the maximum file size of the log file beyond which the file is rotated and the information is logged into a new log file. |

| Setting | Description |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| Maximum number of historical files | Changes the maximum number of historical or rotated log files that you want to retain in the file system. |
| Formatter name | Changes the formatter to change the format of the log information in the log file. |
| Trace Detail Levels | You can enable or disable logging for individual components or managers in SDMC and also define their trace levels. |

Here are the available trace levels:

- ▶ Severe
- ▶ Warning
- ▶ Info
- ▶ Fine
- ▶ Finer
- ▶ Finest

By default, the log entries with Severe and Warning trace levels are logged both in the trace logs and the error logs.

9.4.3 Audit logs

Audit logs are logs that record all the information about operations performed using the SDMC. This log information is logged into the `/var/hsc/log/iqyylog.log` file in the binary format. The audit information is available on the GUI in the Event Log page. You can launch the Event Log page by clicking the **Common Task** drop-down menu in the Resources tab of the Welcome page.

An audit log entry contains the time stamp, the user name, and the task being performed. When a user logs in to the SDMC locally or from a remote client, the information is also recorded in this file. For a remote login, the client host name or IP address is also captured as part of the audit logs.

9.4.4 Using pedbg

You have to send the Product Engineer (PE) debug data to IBM Remote Support from the SDMC connected to servers with problems using the **pedbg** command. The command provides debug tools for the Product Engineer or support personnel for capturing the PE debug data. Only the pe predefined user can execute this command.

The usage of the **pedbg** command is as follows:

```
pedbg [ -d [on | off] | -c | [-c & -q [n]] | -r ] ]
```

Where:

- | | |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -d on off | Controls debug tracing by restarting subsystems to start or stop internal tracing. |
| -c | Collects various logs and core files. |
| -D data_directory | Specifies the directory to which to save collected data. If this option is not specified, the current home directory is used. |
| -q log_option | Specifies that logs are to be collected in quiet mode with the specified log option: |
| 1 | Specifies to collect network information (ifcfg, dhcpd, and arp) |
| 2 | Specifies to collect network information and appliance information only (Java core files, high availability information, and appliance level). |
| 3 | Specifies to collect network, appliance, and embedded operating system information (processes, disk usage, and CPU usage). |
| 4 | Specifies to collect network, appliance, embedded operating system, management server information (Director Logs), and SDMC specific information. This will capture FFDC and audit logs as well. |

Note: The -c option is required when using the -q option.

- | | |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| -r | Removes all log files collected under the directory specified with the -D option. If the -D option is not specified, the current home directory is used. |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------|

9.4.5 Using pesh

The **pesh** command can be used to obtain an unrestricted shell on the SDMC and log on as root. The pesh password has to be obtained from IBM Support and will be eight characters long with alphabetical characters in lower case. You must have the UVMID of the SDMC to execute a **pesh** command. You can log in to the pesh utility using the predefined pe user only.

Run the **lsconfig -v** command to obtain the UVMID:

```
sysadmin@dd174:~> lsconfig -v
vpd=*FC ????????
*N2 Tue Jan 18 19:31:05 CST 2011
*DS SDMC
*TM System x3550 M3 -[7042CR6]-
*SE 10F39AB
*MN IBM
*OS Embedded Operating Systems
*NA 9.3.116.174
*RM 6.730.1052
*UUID 7036A9AB-CDCB-4DEA-A10F-1B6ED666325D
*UVMID ce7f:5e01:1390:aaaa
```

Run the **pesh** command to the unrestricted shell:

```
pesh <SDMC UVMID>
```

The UVMID will be accepted with or without the **:** separators:

```
pesh ce7f:5e01:1390:aaaa
```

or

```
pesh ce7f5e011390aaaa
```

Enter the pesh password provided by IBM Support. Log on as root by entering the following command:

```
su -
```

Enter the password provided by IBM. This password is longer than eight characters with alphabetical characters in lower case.

9.5 SDMC appliance update

The SDMC Update Manager is used to monitor, install, and manage updates, interim fixes, and upgrades on the SDMC appliance.

The Update Manager manages and installs all of the updates for the SDMC's hypervisor components, operating system components, and system management software as a single comprehensive SDMC appliance update (as opposed to individual updates for each component).

There are three types of SDMC appliance updates:

- ▶ Service pack updates
- ▶ Interim fix/hot fixes
- ▶ Upgrade/Release levels

Service pack updates are cumulative, while interim fixes are not.

As with the updates for other types of target systems, you need to acquire the appropriate update downloads and collect inventory on the SDMC appliance to determine the updates that should be applied.

Upgrades are published in two media formats:

- ▶ Recovery Image (OVA and DVD)
- ▶ Release Update (Update Manager package)

As with the managed Power Systems, updates can also be downloaded from the IBM Fix Central website at the following address:

<http://www.ibm.com/support/fixcentral/>

To auto-check and download applicable updates (which is easiest if the SDMC has access to the Internet), click the **Update IBM Systems Director** link from either the Update Manager page or the top left side of the Welcome page (Figure 9-45). This action initiates the process to download and install the latest applicable updates; simply follow the subsequent panels.

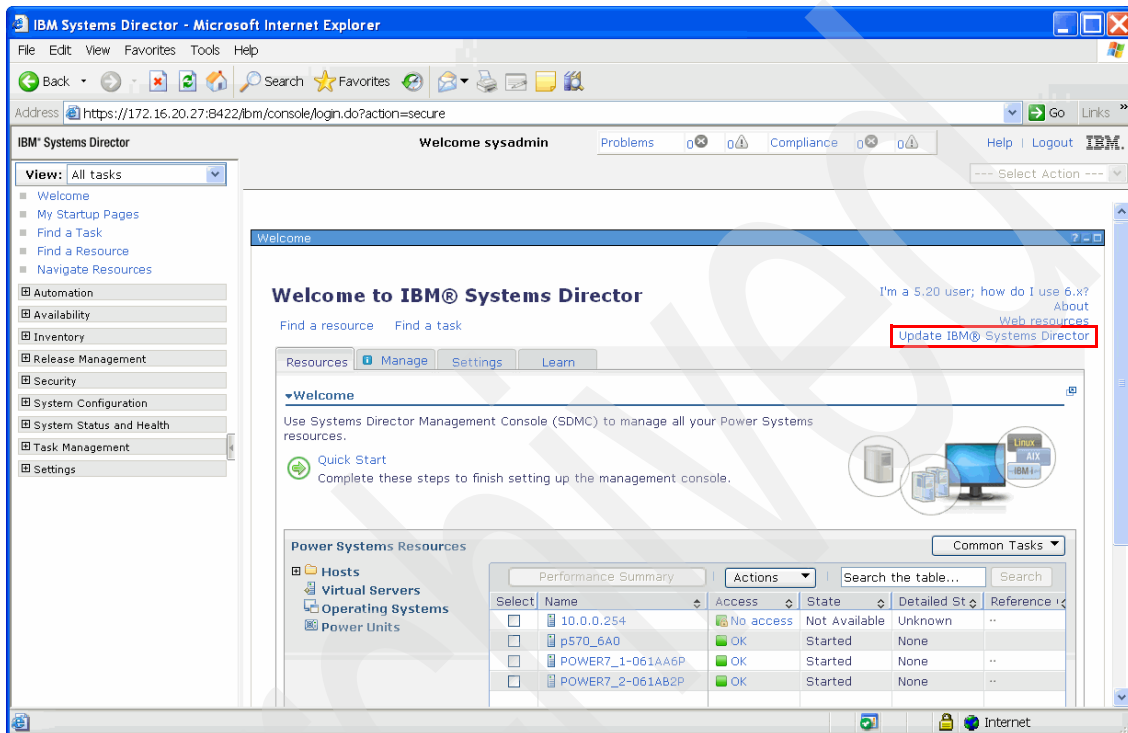


Figure 9-45 Update IBM Systems Director link

If the SDMC does not have access to the internet, the manual procedures for installing and managing SDMC appliance updates are similar to using the Update Manager for Power System server update operations. The only difference is that you download the appropriate SDMC appliance updates and, within the Update Manager Install Wizard, select the SDMC appliance as the target system for the update operation (Figure 9-46).

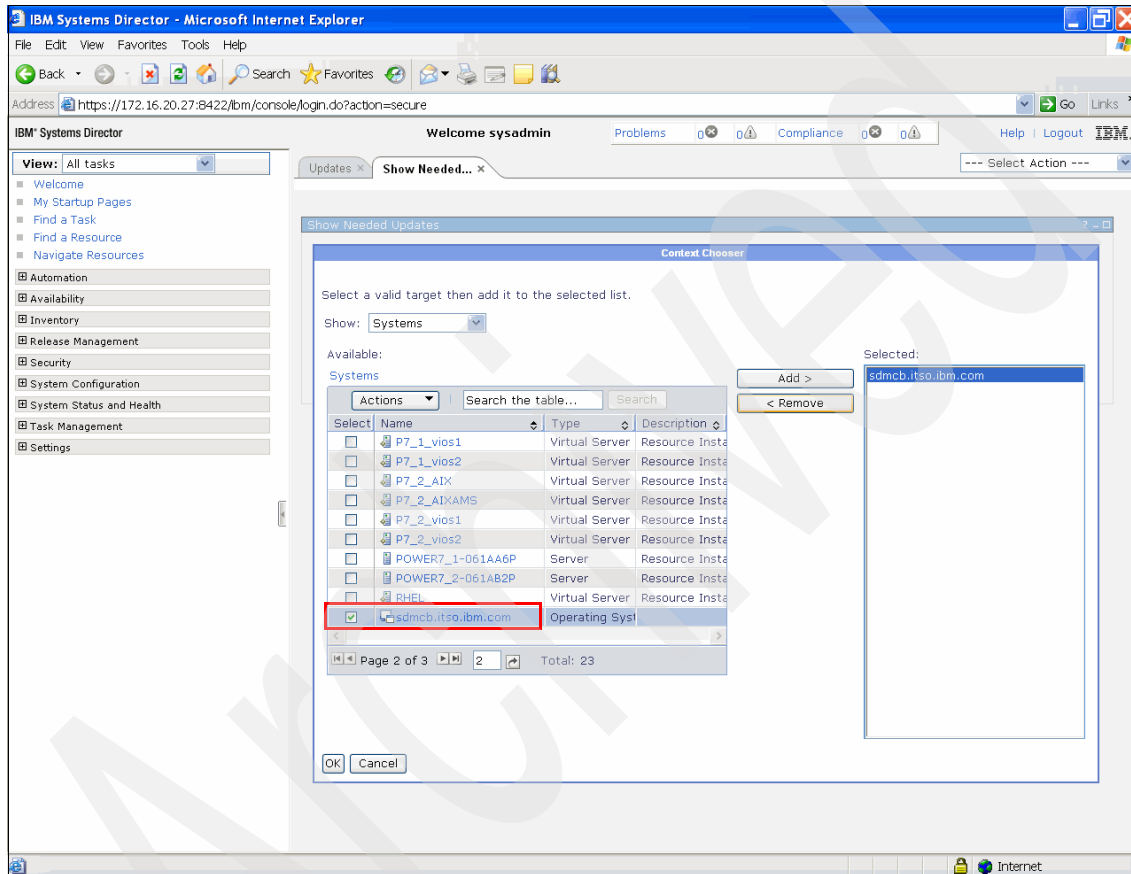


Figure 9-46 Select the SDMC appliance from the Context Chooser

You then proceed through the Install Wizard pages for Show Needed Updates in the same manner as for other types of target systems.

Refer to Chapter 7, “Firmware updates” on page 107 for more information about using Update Manager and for step-by-step procedures for installing updates.

Command-line interface

This chapter discusses the command-line interface (CLI) of the IBM Systems Director Management Console (SDMC) with regard to the Hardware Management Console (HMC) CLI. We explain the three different kinds of commands available in the SDMC:

- ▶ IBM Systems Director appliance commands
- ▶ IBM Systems Director application commands
- ▶ Power Systems management commands

Furthermore, we provide listings of important Director commands, HMC commands that are supported in SDMC, and those HMC commands that are no longer supported.

10.1 SDMC command-line interface

In the SDMC CLI there are three types of commands:

- ▶ IBM Systems Director appliance commands
- ▶ IBM Systems Director application commands
- ▶ Power Systems management commands

The IBM Systems Director appliance commands, as the name indicates, are the commands that allow you to manage and maintain the appliance.

The IBM Systems Director application commands typically allow users to discover, view, and manage resources in the Director. These commands form the base Director command line and their extensions.

The Power Systems management commands are basically the HMC commands. As part of the SDMC, these HMC commands are now integrated with the IBM Systems Director application commands. It is through this integration that the old HMC commands along with the Director commands are collectively available to the SDMC user through the Director command-line (`smcli`) utility.

There are two ways to get to the SDMC CLI:

- ▶ Local
- ▶ Remote

For local access, right-click the SDMC desktop and select **Terminal**. For remote access, can make a Secure Shell (`ssh`) connection to the SDMC (interactive or non-interactive). Unlike on the HMC, you do not have to enable **Remote Command Execution** or **Remote Virtual Terminal** anymore for remote access; they are enabled by default.

10.1.1 IBM Systems Director appliance commands

The IBM Systems Director appliance commands can be used directly on the command line. These are commands that manages the Director itself.

For nearly all IBM Systems Director appliance commands, there is a man page that can be accessed by running `man command name`.

Table 10-1 provides a listing of the most important IBM Systems Director appliance commands and their usage. For the syntax, refer to the man page for each command or go to the following address and select **Reference** → **Commands** → **smcli**:

<http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp/>

Table 10-1 Listing of IBM Systems Director appliance commands

| IBM Systems Director appliance command | Note |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cfgkrb | This command configures Kerberos for the SDMC. |
| cfgldap | This command configures LDAP for the SDMC. |
| chconfig | This command gives you the ability to make changes to: <ul style="list-style-type: none"> ▶ System date ▶ Time ▶ Time zone ▶ Locale |
| chnetcfg | This command gives you the ability to make changes to: <ul style="list-style-type: none"> ▶ Routes ▶ Firewall settings ▶ DNS ▶ IP addresses ▶ Domain ▶ Gateway ▶ Host name ▶ NTP server ▶ Syslog |
| lsconfig | This command lists the system configuration information. |
| lskrb | This command lists the Kerberos information for the SDMC. |
| lsldap | This command lists the LDAP information for the SDMC. |
| lsmediadev | This command lists the media devices that are available. |
| lsnetcfg | This command lists the system network settings. |
| mkauthkeys | This command adds or removes SSH key authentication. |
| pedbg | This command provides debug tools for Product Engineer/support personnel. |
| pesh | This command allows the pe user to gain access to the root shell. |
| rmloginmsg | This command removes the text displayed at login. |

| IBM Systems Director appliance command | Note |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------|
| sendfile | This command transfers a file to a remote system by using File Transfer Protocol (FTP) or secure FTP (SFTP). |
| setloginmsg | This command sets the text displayed at login. |
| smha | This command administers the high availability configuration. |
| smhastatus | This command displays the status of the high availability configuration. |
| smstart | This command starts the Director server. |
| smstatus | This commands shows the status of the Director server. |
| smstop | This command stops the Director server. |

10.1.2 IBM Systems Director application commands

The IBM Systems Director application commands are called with **smcli** as a prefix. These are commands that come with the SDMC extension of the Director. Run the **lsbundle** command to see a list of all the available application commands (Example 10-1).

Example 10-1 lsbundle listing (excerpt)

```
sysadmin@sdmc1:~> smcli lsbundle
snmp/addsystem
snmp/get
snmp/getbulk
snmp/getnext
snmp/help
snmp/inform
snmp/list
snmp/listsystems
snmp/set
snmp/startdiscovery
snmp/trap
snmp/walk

Availability/chfarm
Availability/chvsmfarm
Availability/mkfarm
Availability/mkrelocatetask
```



```
Availability/mkvsmfarm
Availability/mkvsmmigratetask
LEDCLI/chled
LEDCLI/lsled
auditing/chaudit
auditing/lsaudit
```

As you can see, the IBM Systems Director application commands have different paths. Every application command can also be called using its respective path:

```
smcli <path> <command>
```

Some application commands are identical (for example, **list** and **lsled**), but have different paths. They have to be called with their path used as a prefix, for example:

```
smcli scheduler list
smcli event list
```

For nearly all IBM Systems Director application commands, there is a man page that can be accessed by running **man *command name***. Furthermore, all IBM Systems Director application commands have a short version of their help text that can be accessed by using the **--help** option. The man page is for detailed help; the **--help** option is the shorter version of the command help.

Table 10-2 provides a listing of the most important IBM Systems Director application commands and their usage. For the commands' syntax, refer to the man page for each command or go to the following address and select **Reference** → **Commands** → **smcli**:

<http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp/>

There are some IBM Systems Director application commands that are not listed at that website. You can find them in “IBM Systems Director application commands” on page 370.

Table 10-2 Listing of IBM Systems Director application commands

| IBM Systems Director application command | Note |
|------------------------------------------|--------------------------------------------------|
| accesssys | This command requests secured access to systems. |
| chgp | This command modifies a group. |
| chrole | This command changes the properties of a role. |
| chuser | This command modifies a user. |

| IBM Systems Director application command | Note |
|------------------------------------------|------------------------------------------------------------|
| configureHA | This command configures nodes for high availability. |
| discover | This command discovers resources. |
| lsbundle | This command lists all the available application commands. |
| lsgp | This command lists the currently defined groups. |
| lsresources | This command lists the available resources. |
| lsrole | This command lists the roles in IBM Systems Director. |
| lssys | This command lists the systems. |
| lsuser | This command lists an IBM Systems Director user. |
| mkgp | This command creates a group (static and dynamic). |
| mkrole | This command creates a new role. |
| mkuser | This command creates a user. |
| removeha | This command removes the high availability configuration. |
| rmgp | This command deletes a group. |
| rmrole | This command removes a role. |
| rmsys | This command removes a managed system. |
| rmuser | This command deletes a user. |

10.1.3 Power Systems management commands

The Power Systems management (**psm**) commands are the commands which you are familiar with from the HMC. They are also called using **smcli** as a prefix (there are exceptions, which are shown in Table 10-3 on page 282). You can list these commands by running **smcli lsbundle | grep psm** (Example 10-2), because they are all located in the **psm** directory.

Example 10-2 Listing of psm commands (excerpt)

```
sysadmin@sdmc1:~> smcli lsbundle | grep psm
psm/asmmenu
psm/bkprofdata
psm/chcod
psm/chhwres
```

```
psm/chled  
psm/chlparstate  
psm/chlparutil  
psm/chpwrmgmt  
psm/chstat  
psm/chsvc  
psm/chsyscfg  
psm/chsyspwd  
psm/chsysstate  
psm/chtunecfg  
psm/chvet  
psm/cpdump  
psm/cpsysplan  
psm/deploysysplan  
psm/dump  
psm/getdump  
psm/impdata  
psm/lpcfgop  
psm/lscod
```

The Power Systems management commands can also be prefixed with the **smcli psm** keyword. Alternatively, most of the Power Systems management commands are aliased, so that they could be run directly without the **smcli** or **smcli psm** prefix as well. For example, if you want to run the **lssyscfg** command, you can use any of the following three formats:

- ▶ **lssyscfg**
- ▶ **smcli lssyscfg**
- ▶ **smcli psm lssyscfg**

All three commands work the same on the command line. For the scripts based on the old HMC commands, you should prefix the commands with **smcli** before using the script in SDMC. The only exceptions to this usage would be those **psm** commands that do not require the **smcli** prefix in SDMC (Table 10-3 on page 282).

Note: The aliasing is there to support legacy scripts, but the best practice is to use the **smcli** prefix.

The output of the Power Systems management commands on the SDMC is the same as it used to be on the HMC, as shown in Example 10-3.

Example 10-3 SDMC command output

```
sysadmin@sdmc2:~> smcli lssyscfg -r sys -F name,state
p570_170,Operating
POWER7_1-061AA6P,Operating
p570_6A0,Operating

sysadmin@sdmc2:~> smcli lshwres -r virtualio --rsubtype fc --level sys
-m p570_6A0
num_wwpns_remaining=65496,wwpn_prefix=C0507600096A
```

For nearly all Power Systems management commands, there is a man page that can be accessed by running **man *command name*** or **man *psm.command name***.

There are two new commands introduced in SDMC:

- ▶ **impdata**
- ▶ **mk5250**

You can find a description of them in “IBM Power Systems management commands” on page 368.

10.2 HMC commands supported on the SDMC

Table 10-3 lists the HMC commands supported in the SDMC along with their purpose and details about what has changed, if anything, for each command in the SDMC. For the syntax of these commands, refer to the man pages or go to the following address:

<http://www14.software.ibm.com/webapp/set2/sas/f/hmc1/resources.html>

There are some commands that are not listed at the website for the HMC. You can find these commands in “IBM Power Systems management commands” on page 368.

Table 10-3 HMC commands supported at the SDMC

| HMC command | Usage of command | Changed |
|-------------|---------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| asmmenu | Launches the Advanced Systems Management Interface (ASMI) for a managed system using the browser on the SDMC. | This command must be run without the smcli prefix. |

| HMC command | Usage of command | Changed |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| bkprofdata | Backs up profile data for the managed system. | The -o option will be ignored by SDMC. |
| chcod | Performs Capacity on Demand operations on the managed system. | No change. |
| chhwres | Changes the hardware resource configuration of the managed system. It is also used to perform dynamic logical partitioning operations. | A new attribute, pend_mem_region_size, is added. |
| chled | Changes the state of an LED on the managed system. | The man page for this command must be run as man psm.chled . |
| chlparstate | Changes the state of a partition (on, off, shutdown, suspend, and resume). | No change. |
| chlparutil | Changes the SDMC settings for utilization data collection for managed systems. | No change. |
| chpwrmgmt | Configures the power management settings for the managed system. | No change. |
| cpsysplan | Copies a system plan file between the SDMC and either removable media or a remote host. | No change. |
| chstat | Changes the SDMC settings for statistics collection for managed systems. | No change. |
| chsvc | Changes the configuration of a service, such as SNMP, on the SDMC. | No change. |
| chsyscfg | Changes the attributes of partitions, partition profiles, or system profiles for the managed system. | No change. |
| chsyspwd | Credentials are updated in the Director CTS through the Director API. | No change. |
| chsysstate | Changes the state of a partition, the managed system, or the managed frame. | No change. |
| chvet | Performs activation of Capacity on Demand advanced functions on the managed system. | No change. |

| HMC command | Usage of command | Changed |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| cpdump | Copies managed system dumps and managed frame dumps from the SDMC to DVD or a remote FTP site. | No change. |
| deploysysplan | Deploys a managed systems partition plan from a system plan file. | No change. |
| dump | Sets the system dump parameters for the managed system. | No change. |
| getdump | Off loads a dump from the managed system or the managed frame to the SDMC. | No change. |
| getriotopology | Shows the topology of the RIO cabling. | No change. |
| installios | Installs the Virtual I/O Server. | No change. |
| lpar_netboot | Retrieves the MAC address and physical location code from network adapters for a partition or instructs a partition to network boot. | No change. |
| lpcfgop | Clear or dumps partition configuration data on the managed system. | No change. |
| lscod | Lists Capacity on Demand information for the managed system. | No change. |
| lsdump | Lists the dumps that are available for the managed system. | No change. |
| lsfru | Lists selected service processor field-replaceable unit (FRU) information for the managed system. | No change. |
| lshwinfo | Lists environmental information, such as input power levels, for the managed frame. | No change. |
| lshwres | Lists the hardware resources of the managed system. | No change. |
| lsled | Lists LED information for the managed system. | The man page for this command has to be run as man psm.lsled . |
| lslic | Lists Licensed Internal Code (LIC) levels installed, activated, and accepted. | No change. |

| HMC command | Usage of command | Changed |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lslock | Lists which SDMC owns the lock on the managed frame. | No change. |
| lslparmigr | Lists partition migration information. | No change. |
| lslparutil | Lists utilization data collected for a managed system and the SDMC. | <ul style="list-style-type: none"> ▶ The new states <code>primary_state</code> and <code>detailed_state</code> are added. These attributes are listed by default ▶ The old state attribute is displayed only when queried with the <code>-F</code> option. ▶ The <code>-r hmc</code> option is not supported. |
| lsmemdev | Lists block storage devices that can be used as reserved storage devices for the managed system. | No change. |
| lsmemopt | Lists information, including status and progress information, about the most recent memory optimization operation that was started on the managed system. | No change. |
| lspwrmgmt | Lists the power management settings for the managed system. | No change. |
| lsrefcode | Lists reference codes for the managed system or for the partitions in the managed system. | No change. |
| lsstat | Lists statistics collected for a managed system. | No change. |
| lssvc | Lists the settings for a service, such as SNMP, on the SDMC. | No change. |
| lssyscfg | Lists the attributes of partitions, partition profiles, or system profiles for the managed system. | <ul style="list-style-type: none"> ▶ The new states <code>primary_state</code> and <code>detailed_state</code> are added. These attributes are listed by default ▶ The old state attribute is displayed only when queried with the <code>-F</code> option. |
| lssysconn | Lists connection information for all of the systems and frames managed by the SDMC. | No change. |
| lssysplan | Lists the system plan files in the system plan file directory on the SDMC. | No change. |

| HMC command | Usage of command | Changed |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| lsvet | Lists Capacity on Demand advanced functions activation information for the managed system. | No change. |
| migr1par | Performs Virtual Server migration operations. | No change. |
| mkauthkeys | Manages SSH authentication keys. | No change. |
| mksyscfg | Creates partitions, partition profiles, or system profiles for the managed system. | No change. |
| mksysconn | Establishes a connection from the SDMC to a system in the network and adds the system to the systems managed by the SDMC. | The --ip option and the -r and --passwd parameters are not supported. Use the smcli discover and smcli accesssys commands instead. Only mksysconn -o auto [--help] is supported. |
| mksysplan | Creates a system plan file that represents the information known about the hardware, partitions, and profiles for the managed system. | No change. |
| mkvterm | Opens a virtual terminal session for an AIX, Linux, or virtual I/O server. | This command has to be run without the smcli prefix. |
| optmem | Performs memory optimization operations, such as mirrored memory defragmentation operations, on the managed system. | No change. |
| pedbg | Provides debug tools for Product Engineer/Support Personnel. | No change. |
| pesh | Provides full shell access to Product Engineer/Support Personnel. | No change. |
| rmdump | Removes a dump file. | No change. |
| rmlock | Forces a SDMC lock on the managed frame to be released. | No change. |
| rmlparutil | Removes the utilization data collected for a managed system from the SDMC. | No change. |
| rmprofdata | Removes a profile data backup file for the managed system. | No change. |
| rmsyscfg | Removes a partition profile, or a system profile from the managed system. | No change. |

| HMC command | Usage of command | Changed |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| rmsysconn | Removes or resets a connection from the SDMC to a managed system or a managed frame. | The -o remove option is no longer supported. Use the smcli rmsys command instead. |
| rmsysplan | Removes a system plan file from the system plan file directory on the SDMC. | No change. |
| rmvterm | Forces the closure of a virtual terminal session for an AIX, Linux, or virtual I/O server. | No change. |
| rsthwres | Restores the hardware resource configuration of partitions in the managed system. | No change. |
| rstprofdata | Restores profile data for the managed system from a backup file. | No change. |
| startdump | Initiates a dump on the managed system or the managed frame. | No change. |
| updlic | Updates Licensed Internal Code (LIC) on the managed system, managed frame, or on all managed frames that contain High Performance Switches. | No change. |
| viosvr cmd | Issues an I/O server command-line interface (ioscli) command to a virtual I/O server. | This command must be run without the smcli prefix. |
| vtmenu | Interactive menu with which you can get a virtual terminal session for an AIX, Linux, or virtual I/O server. | This command must be run without the smcli prefix. |

10.3 HMC commands not supported on the SDMC

Table 10-4 lists the HMC commands listed that are no longer supported on the SDMC, because of the differences between HMC and SDMC. Some of the functionality is still supported through other SDMC commands, which is also reflected Table 10-4.

Table 10-4 HMC commands not supported by the SDMC

| HMC command | SDMC replacement |
|-------------------|------------------------------------------------|
| bkconsdata | No replacement available. Done through backup. |

| HMC command | SDMC replacement |
|-------------|-------------------------------------------|
| chaccfg | smcli chrole. |
| chhmc | chnetcfg. |
| chhmcencr | No replacement available. |
| chhmcfs | No replacement available. Done by a task. |
| chhmcldap | cfgldap. |
| chusrtca | setloginmsg. |
| expdata | No replacement available. |
| getfile | No replacement available. |
| getupgfiles | No replacement available. |
| hmcshutdown | No replacement available. |
| hmcwin | No replacement available. |
| lshmcusr | smcli lsuser. |
| lslogon | No replacement available. |
| lsmmediadev | lsmmediadev (Director version). |
| lspwdpolicy | No replacement available. |
| lssacfg | smcli lsrole. |
| lssvcevents | smcli lssvcproblem. |
| monhmc | No replacement available. |
| rmaccfg | smcli rmrole. |
| rmfile | rm. |
| rmhmcusr | smcli rmuser. |
| rmpwdpolicy | No replacement available. |
| rnvi | No replacement available. |

Schedule operations

In this chapter, we describe how to schedule operations for certain tasks, such as activating a system or partition using a specific profile, backing up profile data, or turning on off a managed system without operator assistance.

A lot of IBM Systems Director commands can be scheduled, and schedule operations allows you to schedule a select number of Power Systems specific commands.

11.1 Scheduling operations for managed systems and Virtual Servers

To schedule operations for managed systems and Virtual Servers, right-click the managed system or the Virtual Server and select **Operations** → **Schedule Operations** (Figure 11-1).

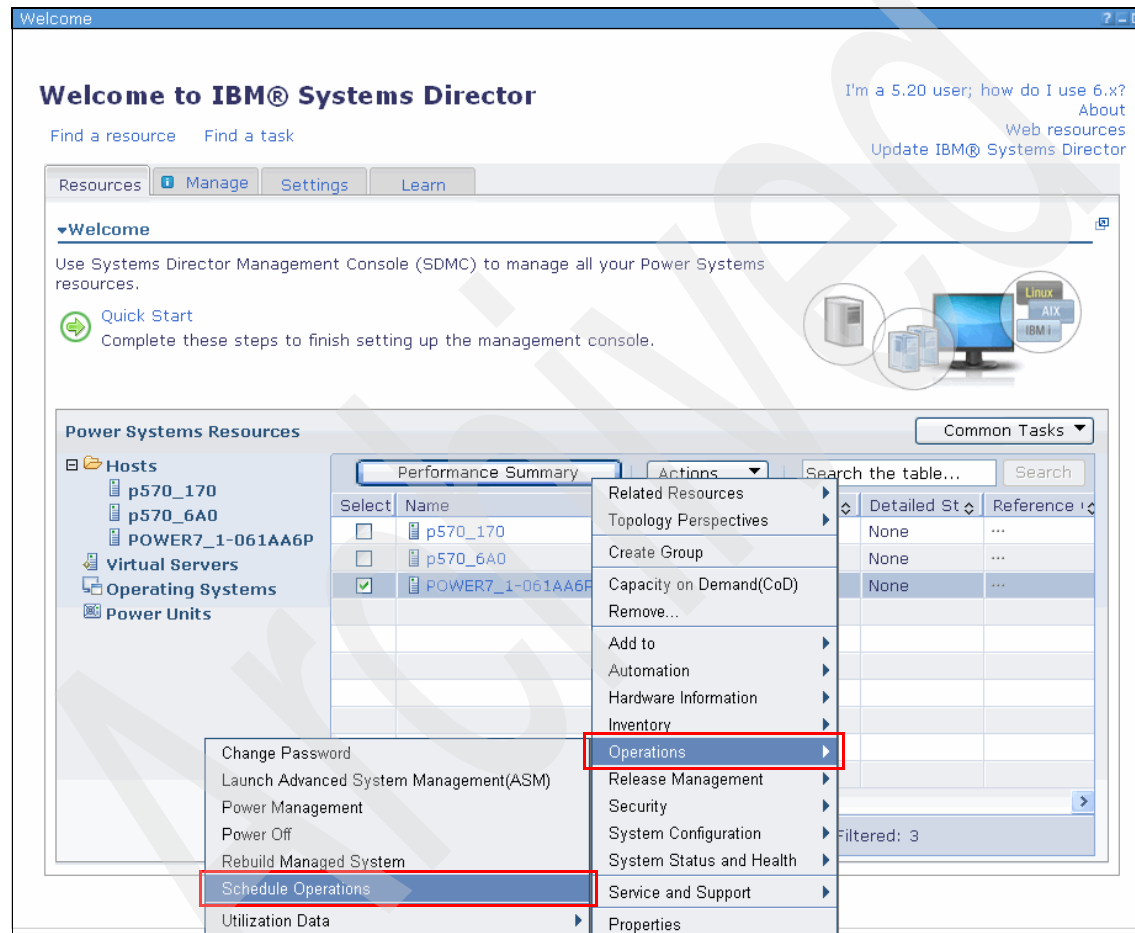


Figure 11-1 Scheduling operations for managed systems example

For managed servers, you get a selection list that has following task options:

- ▶ Activate System Profile
- ▶ Backup Profile Data
- ▶ Power Off

- ▶ Power On
- ▶ Manage Utility CoD
- ▶ Modify Shared Processor Pool
- ▶ Modify Virtual Server Pool Assignment
- ▶ Modify Power Saver Mode

For Virtual Servers, you get a selection list that has following task options:

- ▶ Activate
- ▶ Shutdown
- ▶ Change/O
- ▶ Change Processors
- ▶ Move Processors
- ▶ Change Memory
- ▶ Move Memory

For some of the tasks, you have further options you can specify. For example, for the Backup Profile Data task you can specify a file name (Figure 11-2).

Schedule Operations: POWER7_2-061AB2P

Scheduled operations allow you to perform tasks on the managed system at a later time. To begin, select the type of operation you would like to schedule.

Managed system name: POWER7_2-061AB2P

Operations:

Backup Profile Data

Schedule Power Systems Task: Backup Profile Data

Enter a name for the new backup file that will be created and click OK to continue.

Backup file name:

OK Cancel

Figure 11-2 Scheduling Backup Profile Data

Click **OK**, and the Task Launch Dialog page opens (Figure 11-3).

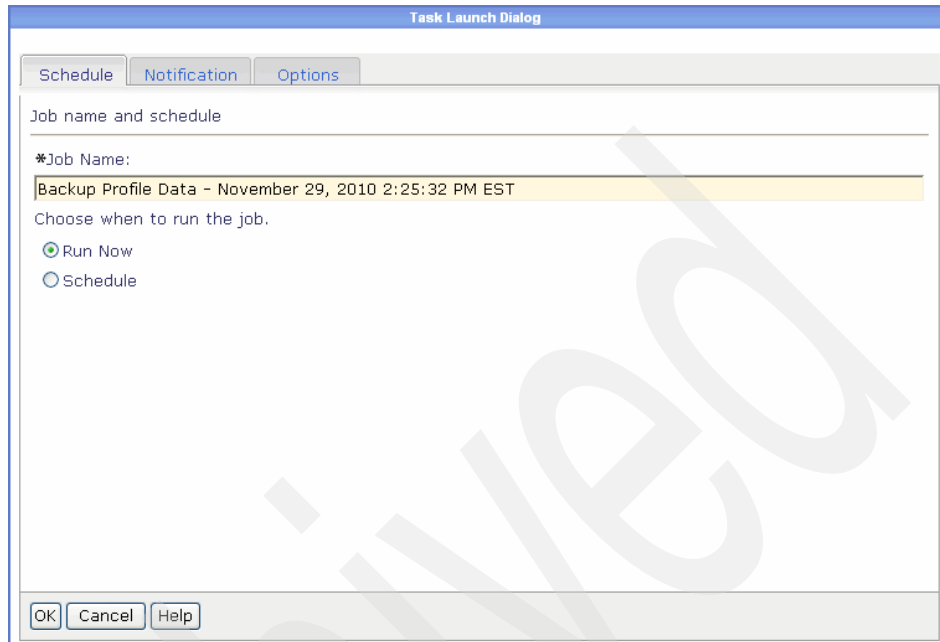
The screenshot shows a 'Task Launch Dialog' window with three tabs: 'Schedule', 'Notification', and 'Options'. The 'Schedule' tab is active. It contains a section titled 'Job name and schedule' with a text field for '*Job Name:' containing 'Backup Profile Data - November 29, 2010 2:25:32 PM EST'. Below this is a label 'Choose when to run the job.' followed by two radio buttons: 'Run Now' (which is selected) and 'Schedule'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Help'.

Figure 11-3 Task Launch Dialog page

Here you can schedule a job for the task, set notifications, or set further options.

11.1.1 Schedule tab

On the Schedule tab, you can specify a job name and when to run the job. For the job to run, you can select between **Run Now** or **Schedule**. If you schedule it, you can select between different repeat options:

- | | |
|---------------|-------------------------------------------------------------------------------------------------------------------|
| Once | You can specify a specific date and time when to run the task. |
| Hourly | You can specify the duration of how long the job repeats and if the job should run on weekends. |
| Daily | You can specify the duration of how long the job repeats and if the job should run on weekends. |
| Weekly | You can specify the duration of how long the job repeats and you can select on which weekdays the job should run. |

| | |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Monthly | You can specify the duration of how long the job repeats, if the job should run on weekends, and on which day of the month the job should run. |
| Yearly | You can specify the duration of how long the job repeats and if the job should run on weekends. |
| Custom | You can make your own list of dates of when the job should run. |

11.1.2 Notification

On the Notification tab, you can choose to receive an email notification:

- ▶ When the job begins
- ▶ When the job is completed
- ▶ When the job fails:
 - On any error
 - On a percentage targets with errors
 - On a number of targets with errors

If you choose to have a notification, you have to specify an email address, an email server, and the port of the email server.

11.1.3 Options

On the Options tab, you can specify the following additional options:

- ▶ System Time
 - Use the management server time (default).
 - Use the local system time.
- ▶ Unavailable Systems
 - Fail if the system is not available (default).
 - Run when the system becomes available.
- ▶ Maximum job instances in history (default is 100)

11.1.4 Creating the job

When you have made your selections in the Task Launch Dialog page, click **OK**. A notification about the successful creation of your job opens (Figure 11-4).

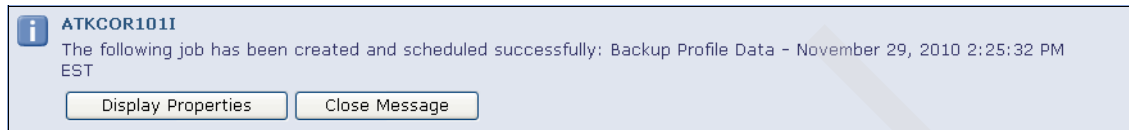


Figure 11-4 Successful creation of a job

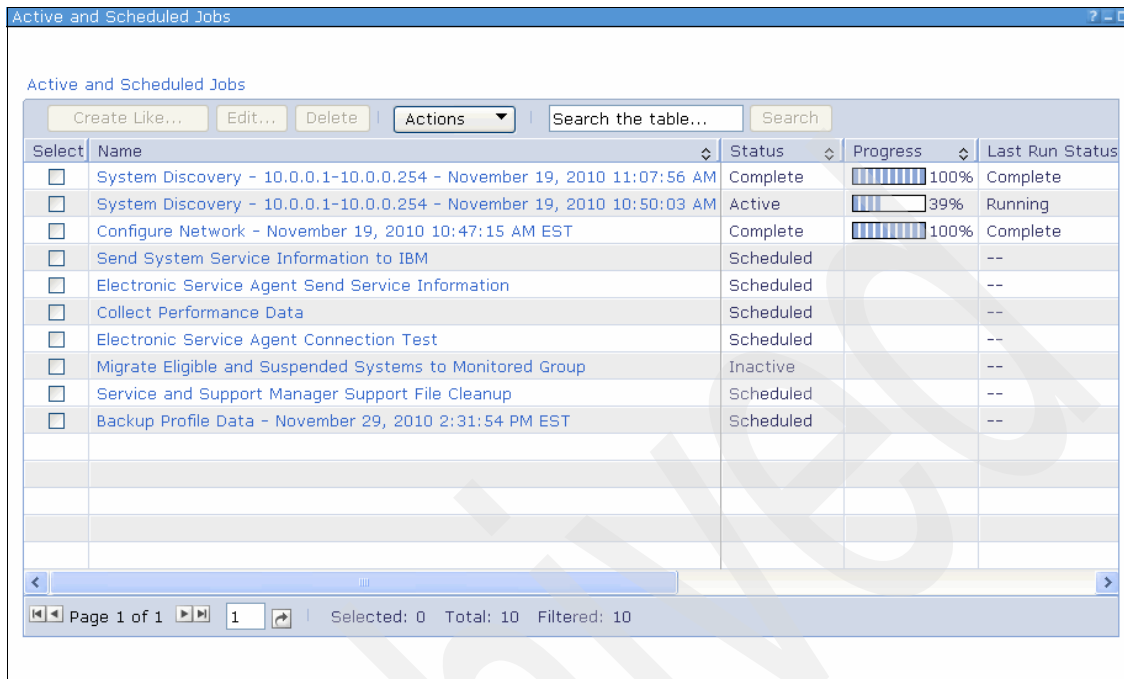
If you click **Display Properties**, you can see the properties of the job you just created.

11.2 Editing, deleting, and copying, and viewing the properties of a scheduled operation

To edit, delete, or copy a scheduled operation, you have to go to the Active and Schedule Jobs task. There are two ways to access this task:

- ▶ Use the task list under Task Management
- ▶ Use the Manage tab under Automation Manager.

Figure 11-5 shows an overview over the scheduled, active, and completed jobs.



The screenshot shows a window titled "Active and Scheduled Jobs" with a toolbar containing "Create Like...", "Edit...", "Delete", and an "Actions" dropdown. A search bar is also present. The table below lists various jobs with their status and progress.

| Select | Name | Status | Progress | Last Run Status |
|--------------------------|------------------------------------------------------------------------|-----------|----------|-----------------|
| <input type="checkbox"/> | System Discovery - 10.0.0.1-10.0.0.254 - November 19, 2010 11:07:56 AM | Complete | 100% | Complete |
| <input type="checkbox"/> | System Discovery - 10.0.0.1-10.0.0.254 - November 19, 2010 10:50:03 AM | Active | 39% | Running |
| <input type="checkbox"/> | Configure Network - November 19, 2010 10:47:15 AM EST | Complete | 100% | Complete |
| <input type="checkbox"/> | Send System Service Information to IBM | Scheduled | | -- |
| <input type="checkbox"/> | Electronic Service Agent Send Service Information | Scheduled | | -- |
| <input type="checkbox"/> | Collect Performance Data | Scheduled | | -- |
| <input type="checkbox"/> | Electronic Service Agent Connection Test | Scheduled | | -- |
| <input type="checkbox"/> | Migrate Eligible and Suspended Systems to Monitored Group | Inactive | | -- |
| <input type="checkbox"/> | Service and Support Manager Support File Cleanup | Scheduled | | -- |
| <input type="checkbox"/> | Backup Profile Data - November 29, 2010 2:31:54 PM EST | Scheduled | | -- |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Page 1 of 1 | 1 | Selected: 0 Total: 10 Filtered: 10

Figure 11-5 Active and Schedule Jobs overview

When you select a job, you can edit or delete it, or you can create a new job by copying the selected job.

If you click a job, you can view the properties of the selected job (Figure 11-6).

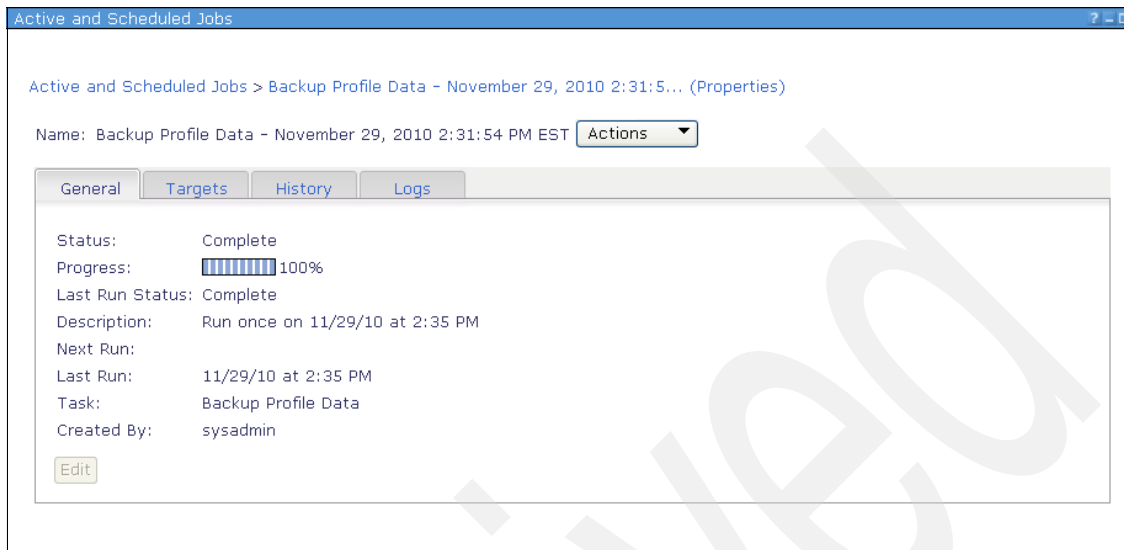


Figure 11-6 Job Properties page

Under the General tab, you can view the status of the job and other general properties. The Targets tab shows the specified managed system(s) or Virtual Server(s) to which the job is assigned. The History tab shows when the specified job has been run and with which status. The **Logs** tab shows a detailed output of the job.

Figure 11-7 shows the output of a successful backup of the profile data.

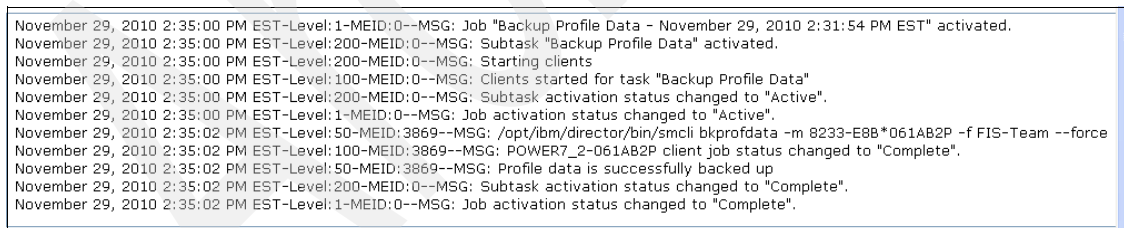


Figure 11-7 Log of the job

11.3 Automation Manager

If you select the **Automation Manager** on the main Manage tab, you get an overview over the jobs (scheduled, completed, and failed) in the last 30 days. You see the three next jobs that will be running and you see the three most recent jobs, as shown in Figure 11-8.

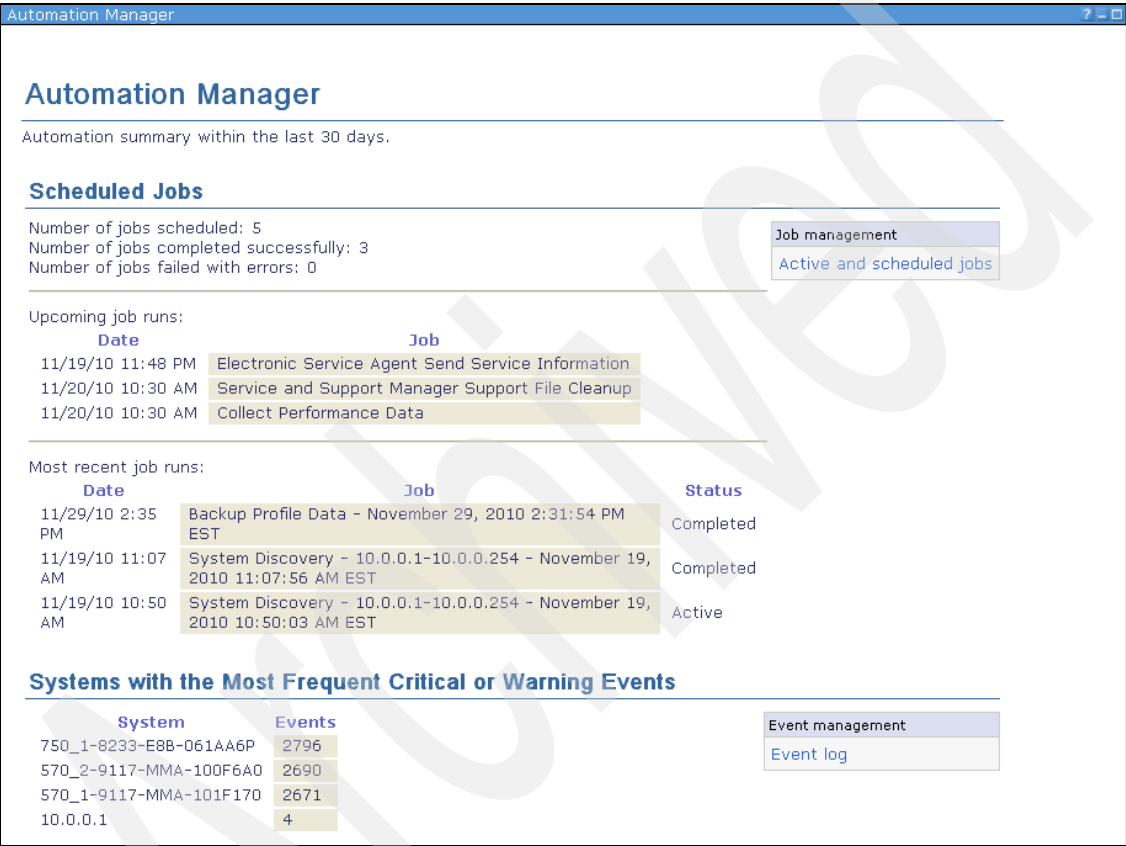


Figure 11-8 Automation Manager

From within the Automation Manager, you can go to the Active and scheduled Jobs task, from where you can manage the jobs, as described in 11.2, “Editing, deleting, and copying, and viewing the properties of a scheduled operation” on page 294.

Archived

High availability and redundancy

Implementing IBM Systems Director Management Console (SDMC) in a high availability (HA) or a redundant setup can provide improved serviceability to the SDMC appliance and provides backup to the system in case of a disaster.

12.1 Systems Director Management Console High Availability versus redundant setup

Users familiar with the redundant HMC setup in their Power Systems environment can use the same setup in SDMC, as multiple SDMCs can connect to and actively manage a single managed server.

Users can also implement SDMC High Availability, which provides active/passive failover capability, with one active SDMC and one passive SDMC on standby to take over in case of failure. Figure 12-1 shows both options for SDMC High Availability and redundancy.

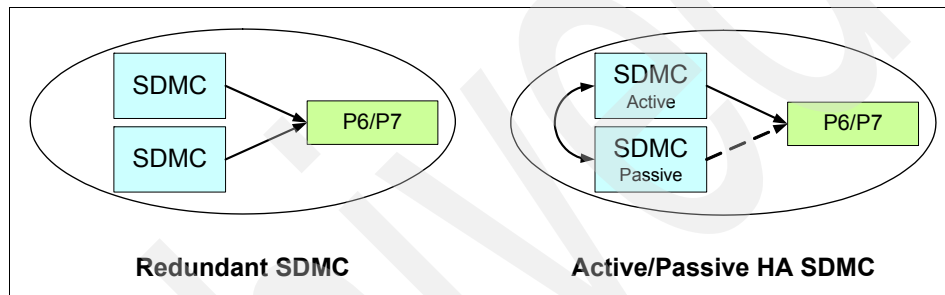


Figure 12-1 Redundant versus active/passive SDMC High Availability

In addition to providing the management capabilities currently in the HMC for the managed Power System servers, the SDMC also can manage the operating systems of the servers themselves by connecting to the Common Agent Services (CAS) agent on the managed systems through an agent manager. However, the CAS agent is limited to a single connection to an agent manager and is not capable of a redundant connection. Therefore, the SDMC High Availability feature is provided to eliminate this single point of failure for users that require high availability for this functionality.

The choice between a redundant setup versus an active/passive High Availability implementation depends on your planned usage of the SDMC:

- In an environment where the SDMC is used for HMC-like management functionality, the redundant setup provides the most availability and is the easiest to set up and administrate. Both SDMCs are active and can continue to provide functions for the managed systems should one of them fail. The setup of a redundant SDMC environment only involves adding the managed system to both SDMCs.

- For an environment where the SDMC is used for agent OS management and there is a high availability requirement for that functionality, SDMC High Availability is needed. If your active SDMC fails, the passive standby SDMC automatically takes over and management functionality for the managed systems is restored in about 10 minutes. There are some extra planning, setup, and administrative steps required to implement SDMC High Availability.

Table 12-1 shows the differences between redundant HMCs and IBM Systems Director high availability setup.

Table 12-1 Differences between a redundant and a replication High Availability environment

| | HMC | SDMC with redundancy | Systems Director or SDMC with High Availability |
|-----------------------------------|-----------------------------------------------------------|-----------------------------------------------------------|--------------------------------------------------------|
| Type of environment | Redundant. | Redundant. | Replication. |
| High availability topology | Active/Active: Both consoles are active at the same time. | Active/Active: Both consoles are active at the same time. | Active/Passive: Only one console is active at a time. |
| Data | Data is not identical. | Data is not identical. | All data is identical on the two nodes. |
| Management Console | HMC. | Systems Director. | Systems Director. |
| Console versions | Can be different. | Can be different. | Must be the same. |

In a redundant setup, it is also possible to have one SDMC point to another SDMC's agent manager, which would allow both SDMCs to manage the agents at the same time. However, because the agent manager is running on only one of the SDMCs, this is a single point of failure. If this SDMC goes down, the other SDMC now loses contact with the agents.

For this setup, configure an SDMC (A) to point to the active agent manager running on another SDMC (B). From the GUI on SDMC A, go to the Settings category in the left pane and click **Agent Manager Configuration**. Click **Add** on the Agent Manager Configuration page, which opens and configures the agent manager using the IP address and agent manager user ID and password for SDMC B (Figure 12-2).

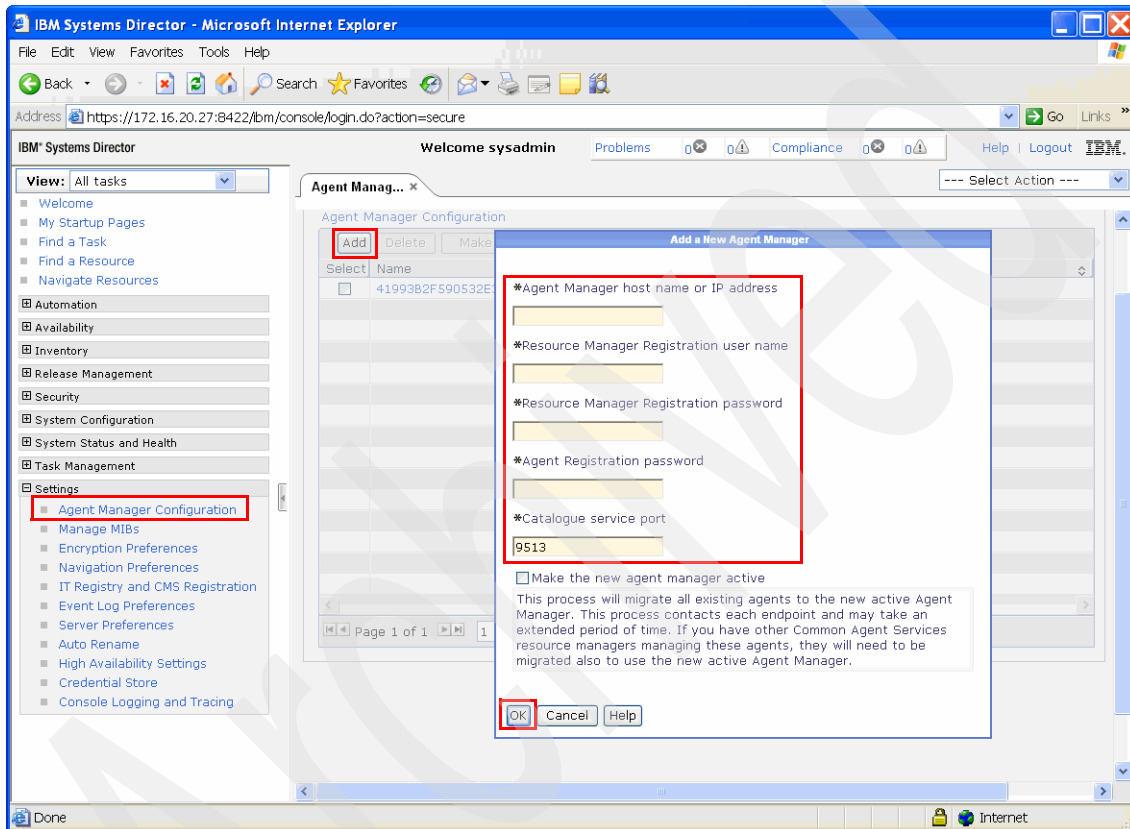


Figure 12-2 Add an New Agent Manager

12.2 Active/Passive High Availability overview

In a high availability environment, there are two SDMCs operating as synchronized nodes in an active/passive cluster. One node in the environment is kept active at all times, with a second passive node kept in close synchronization. If your active node fails, the passive node (on standby, waiting for a failure of the active node) takes over in about 10 minutes.

Figure 12-3 shows both the software and hardware stack that of an SDMC High Availability environment. These internal software components that make up SDMC High Availability are transparent to the user and do not need to be directly configured. IBM Tivoli System Automation for Multiplatform (TSA) is used to monitor the hardware and software stack. It also provides failover and quorum capability. Data is mirrored using Distributed Replicated Block Device (DRBD). Apache MQ performs operating system synchronization, and also contains the firewall rules, NTP configuration, network and user settings. Floating IP addresses used to connect to the active SDMC can be moved between the nodes with the active node. The OS on the passive node is started, but the software stack is not.

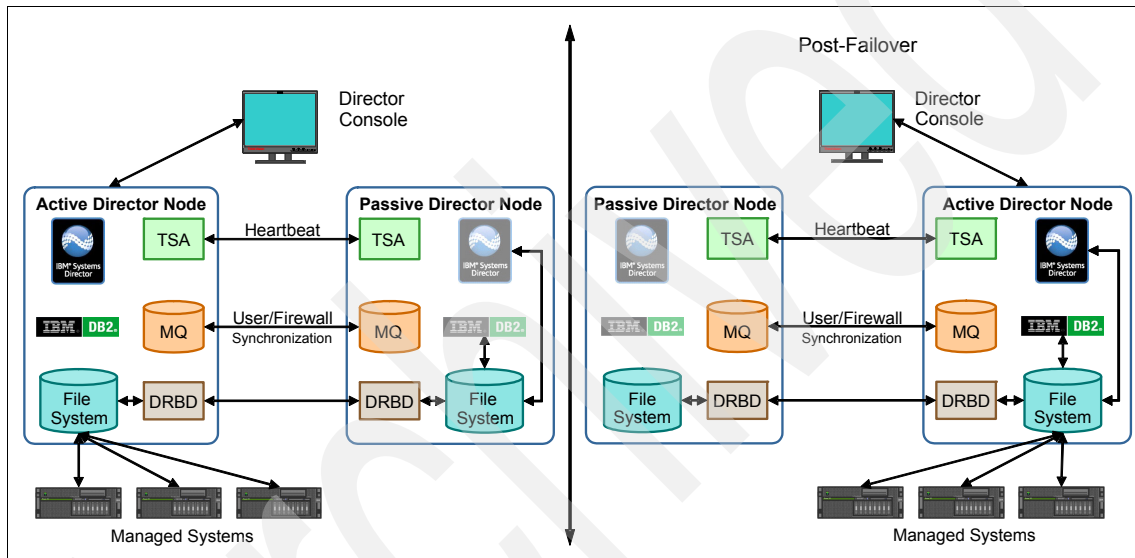


Figure 12-3 SDMC High Availability environment before and after failover

Running the setup wizard or using CLI commands on the SDMC designated to be the primary node configures the internal High Availability components on both the primary and secondary SDMCs. Figure 12-4 shows the SDMC High Availability configuration sequence that sets up the two SDMCs in an High Availability cluster.

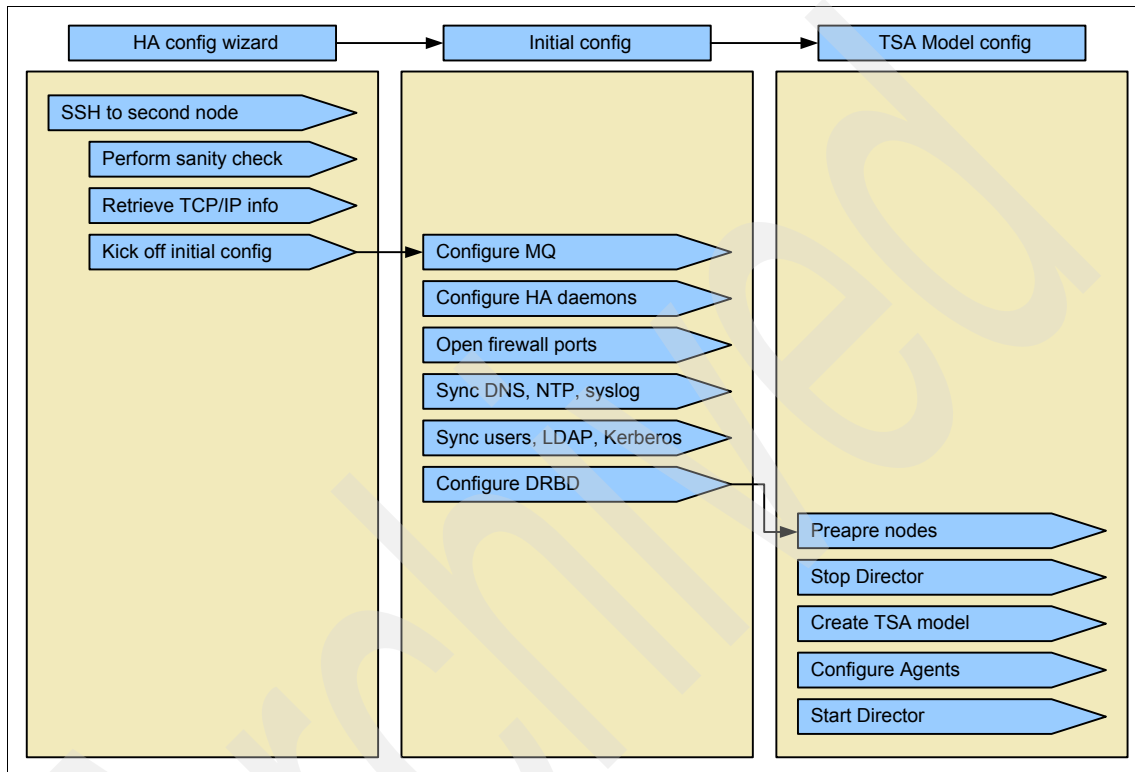


Figure 12-4 Active/Passive configuration sequence

12.2.1 High availability terminology

Refer to this list of terms to help you better understand high availability concepts:

Node

A node is an SDMC that is configured to be part of a high availability environment.

Active node

The active node manages your environment. Only one node is active at a time.

Passive node

The passive node is not currently active. Any changes you make to the active node are replicated to the passive node.

| | |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Primary node | This is the node you use to set up high availability. It is initially the active node. When you set up a high availability cluster, the IBM Systems Director data, remote authentication configuration settings, users, and firewall settings on this node are replicated to the secondary node. |
| Secondary node | This is the node that you set up to take over if the primary node fails. It is initially the passive node, but takes over as the active node if the primary node fails. |
| Network status IP address | The cluster nodes use this IP address to determine which node is connected to the network. If they cannot contact each other, the node that can connect this IP address becomes the active node. |
| Floating IP address | This address is always assigned to the active node. Users should always access this address so they do not have to know which node is active. It also enables you to use IBM Systems Director Common Agent with high availability. |

12.2.2 SDMC High Availability synchronized data

The following data changes on the active SDMC are synchronized to the standby SDMC:

- ▶ User additions
- ▶ User modifications
- ▶ User deletions
- ▶ Firewall changes
- ▶ NTP configuration
- ▶ Kerberos/LDAP configuration
- ▶ Initial High Availability configuration
 - DRBD configuration
 - Users
 - Authentication files (LDAP and Kerberos)
 - Firewall settings
 - DNS resolver
 - NTP configuration

12.2.3 SDMC High Availability processes monitored

These are the processes monitored by the SDMC High Availability for a redundant takeover:

- ▶ Director
- ▶ DB2
- ▶ DRBD
- ▶ CIM Server
- ▶ High Availability MQ Daemon (MQ server)
- ▶ High Availability Daemon (Processes MQ messages)
- ▶ NTP Server
- ▶ DHCP Server

12.2.4 Active/Passive High Availability: Log location

Here are the locations of the SDMC High Availability log files:

- ▶ `/opt/ibm/director/ha/logs/`, which contains:

| | |
|----------------------------|-------------------------------------------------------------------|
| <code>daemon0-x.log</code> | High Availability Daemon log |
| <code>mq0-x.log</code> | ActiveMQ log |
| <code>smha.log</code> | TSA monitor log |
| <code>init0-x.log</code> | Initial configuration from initiated outside the Director process |
- ▶ `/opt/ibm/director/lwi/logs`
Contains SDMC High Availability task logs captured in the Director High Availability configuration task
- ▶ The daemon log and mq log are rolling logs that contain up to five log files, where x is the log file number. Each log file can contain approximately 10 MB data.

In addition, consider the following items:

- ▶ Turn the log level to `com.ibm.isdvmi.ha.level=FINEST` if there are problems with the SDMC High Availability configuration.
- ▶ Log files are collected using the SDMC appliance log collector called `pedbg`. You must collect logs as the `pe` user. `pedbg` also collects TSA log files if high availability has been configured.

12.3 Active/Passive High Availability: Configuration planning

You need to plan the setup of SDMC High Availability, and there are several considerations and issues to be aware of in setting up and administering this environment:

- ▶ Both SDMCs must be at the same code level prior to the High Availability configuration.
- ▶ SSH must not be blocked by the firewall during the initial High Availability configuration.
- ▶ Data on the secondary node is lost during the High Availability configuration.
- ▶ Data on the primary node, where the High Availability configuration is triggered, is retained and mirrored to the secondary node.
- ▶ Both SDMCs must be turned on at all times to receive the benefits of high availability.
- ▶ Only the active SDMC console can be accessed after High Availability is configured.

Note: Prior to the High Availability configuration, backups of both SDMC images should be taken so that the SDMCs can revert back to their original non-High Availability states should there be problems during the High Availability setup or if you want to go back to a non-High Availability setup.

12.3.1 Network requirements

Because data is continually replicated between the two cluster nodes, carefully consider your networking topology. Figure 12-5 shows a diagram of a typical SDMC High Availability environment.

Note that the SDMC provides network path redundancy through two connections to each Flexible Service Processor (FSP) of a managed system. When the front and back IPs of the FSP are connected through different networks to the SDMC and one of the networks goes down, then the connection is automatically established to the FSP from the same SDMC through the other network, providing continuous availability to the user.

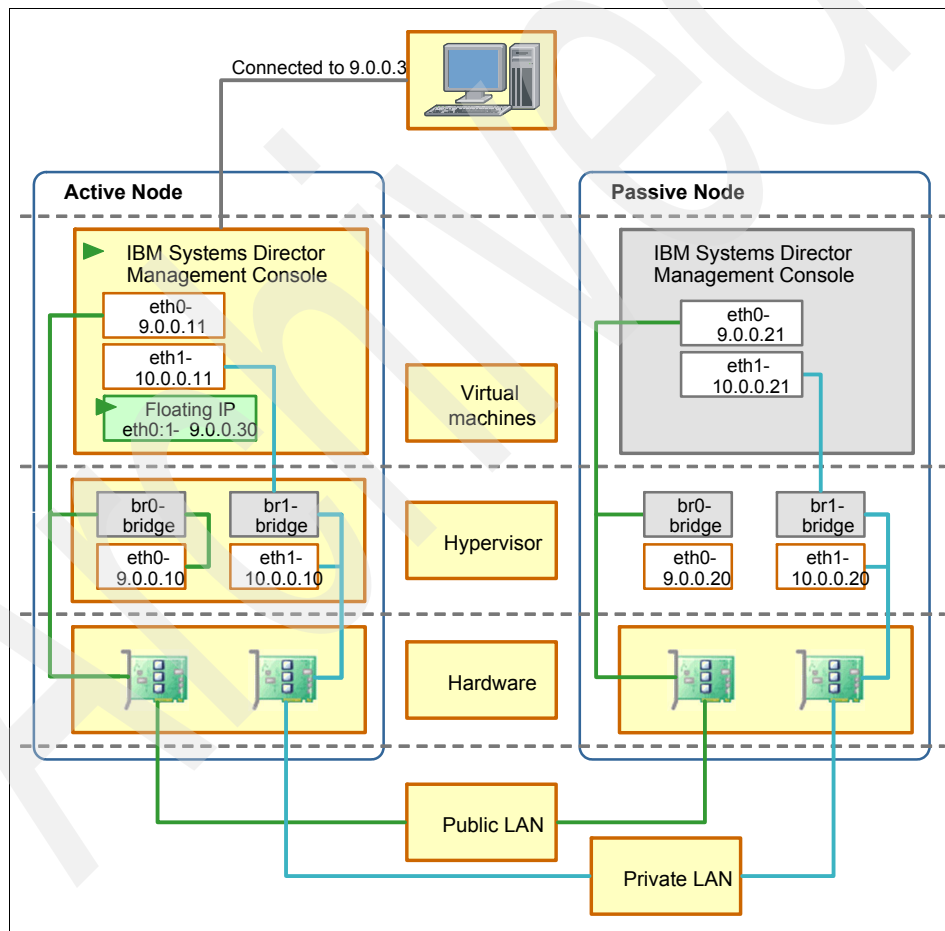


Figure 12-5 High Availability network topology

Replication IP address

Because the replication IP address on each of the two SDMC nodes in the High Availability cluster is used to constantly synchronize data, it is important that this network connection be fast as possible.

Guidelines for the replication IP address

The guidelines for the replication IP address are:

- ▶ If possible, use a separate private network for replication between the nodes for better performance and place the two SDMCs within close range.
- ▶ A high-speed Ethernet link, such as a crossover cable using gigabit Ethernet, can be used to reduce latency for the initial and ongoing synchronization between the active and passive SDMCs.

Network status IP address

Although having a network status IP address is optional, it is a best practice. The nodes use this IP address to determine which node is connected to the network. If they cannot contact each other, the node that can connect this IP address becomes the active node.

If you do not specify a network status IP address, both nodes might become active at the same time. If one node cannot connect to the other, it assumes that the other node has lost network connectivity and makes itself the active node. If both nodes have network connectivity but cannot connect to each other, both nodes might become active.

If both nodes become active, changes might be made to both nodes, but all changes made to one node are lost. When connectivity is restored, one node becomes passive and the data on the active node is copied to it. Changes that were made to the node that becomes the passive node are lost.

Guidelines for the network status IP address

The guidelines for the network status IP address are:

- ▶ This address works best in domains where all nodes are in the same subnet. Having the nodes in different subnets makes it more likely that both nodes can ping the IP address, but they cannot communicate with each other.
- ▶ Do not install a firewall rule that blocks ICMP traffic between the cluster nodes and the network status IP instance.
- ▶ Choose an address that the nodes can connect to only when they can connect to the whole network.
- ▶ Choose an address that is available most of the time.

- ▶ Choose an address that each node can reach by a single path. If there are multiple paths, it is possible that one path is down, causing the ping to fail, when the node is online.
- ▶ Do not use an address that either node uses, including the floating IP address.
- ▶ The gateway address for the SDMC is a good candidate to use as a network status IP address.

Floating IP address and agent manager IP address

The floating IP address is always initially assigned to the active node and is reassigned to the secondary node that takes over as the active node during a failure. This is the address that users should always access so that they always connect to the currently active node.

If you use Common Agent Services (CAS) agents, they use the floating IP address specified as the agent manager IP address to communicate with the nodes. For information about common agents, see the Common Agent topic in the Systems Director Information Center at:

<http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp>

The agent manager uses the agent manager IP address to identify itself to the CAS agents that it manages. If you only specify one floating IP address, it is used as the agent manager IP address. If you specify more than one floating IP addresses, you can specify which one is the agent manager IP address.

Guidelines for the floating IP address

The guidelines for the floating IP address are:

- ▶ It must not be in use.
- ▶ All systems that need to connect to the nodes must be able to access this IP address through your network.
- ▶ If your nodes are connected to multiple networks, configure multiple floating IP addresses.

All CAS agents you want to manage must be able to contact the floating IP address that you specify as the Agent Manager address.

12.3.2 DHCP considerations

The SDMC cannot be a DHCP client. If your network is set up so that one DHCP server is running at a time (you have one range of DHCP addresses), then both the SDMC network configurations must be identical and each network interface card (NIC) must be connected to the same networks on each node. For example, if eth0 is connected to the 192.168.1.0 network segment on the primary node, then eth0 on the secondary node must also be connected to the same segment.

The SDMC High Availability environment can be configured in either a non-shared or shared DHCP configuration, as shown in Figure 12-6 on page 312.

Non-shared DHCP configuration

The DHCP server is run (and monitored) on each node. Configure each node to use the same network interface (eth0 in Figure 12-6 on page 312) but to use different address ranges.

Archived

Shared DHCP configuration

The DHCP server is only run on the active node. Configure the first node as using DHCP server with a specific address range. Choose the first reserved address for the node. Configure the second node as a standard network configuration and choose the second reserved address for the node.

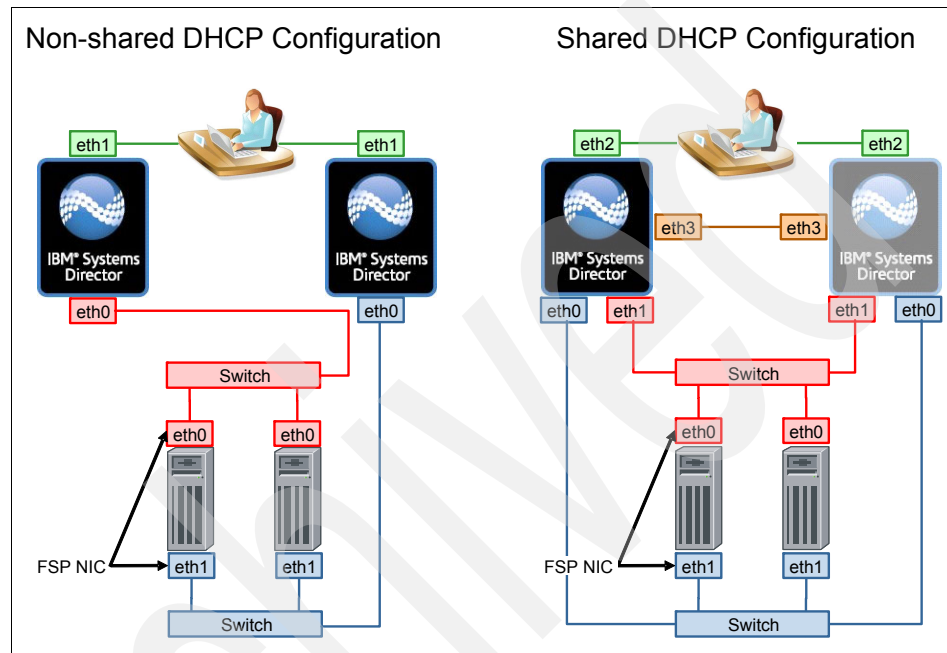


Figure 12-6 Shared and non-shared DHCP configurations

12.4 High Availability configuration

On the SDMC that is intended to be the primary node, perform the procedure in this section to configure a high availability cluster in your environment. You must have the SMAAdministrator role to configure high availability.

12.4.1 Configuration using SDMC High Availability setup wizard

Perform the following steps:

1. Open up the IBM Systems Director Management Console GUI using a web browser and log in as the sysadmin user. In the left navigation pane, expand **Settings** and click **High Availability Settings**. The High Availability Settings page opens. Click **Set Up High Availability**. Figure 12-7 shows the initial page as you start the High Availability setup process.

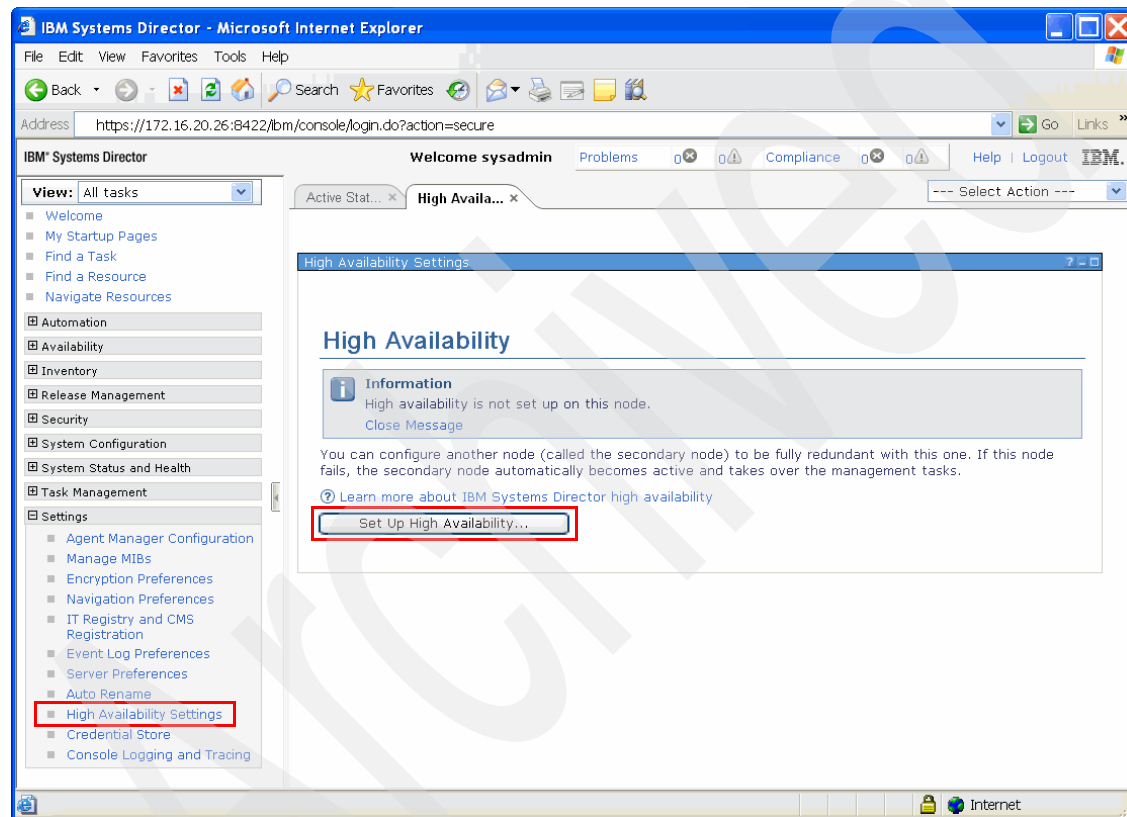


Figure 12-7 High Availability Settings page

Note: If you do not see the Set Up High Availability button, high availability is already configured.

2. The Welcome page for the High Availability setup wizard (Figure 12-8) shows the SDMC as the primary node that you are using to perform the configuration. It reminds the user of prerequisites and provides links to support documents for more information about High Availability. Click **Next** to begin setup.

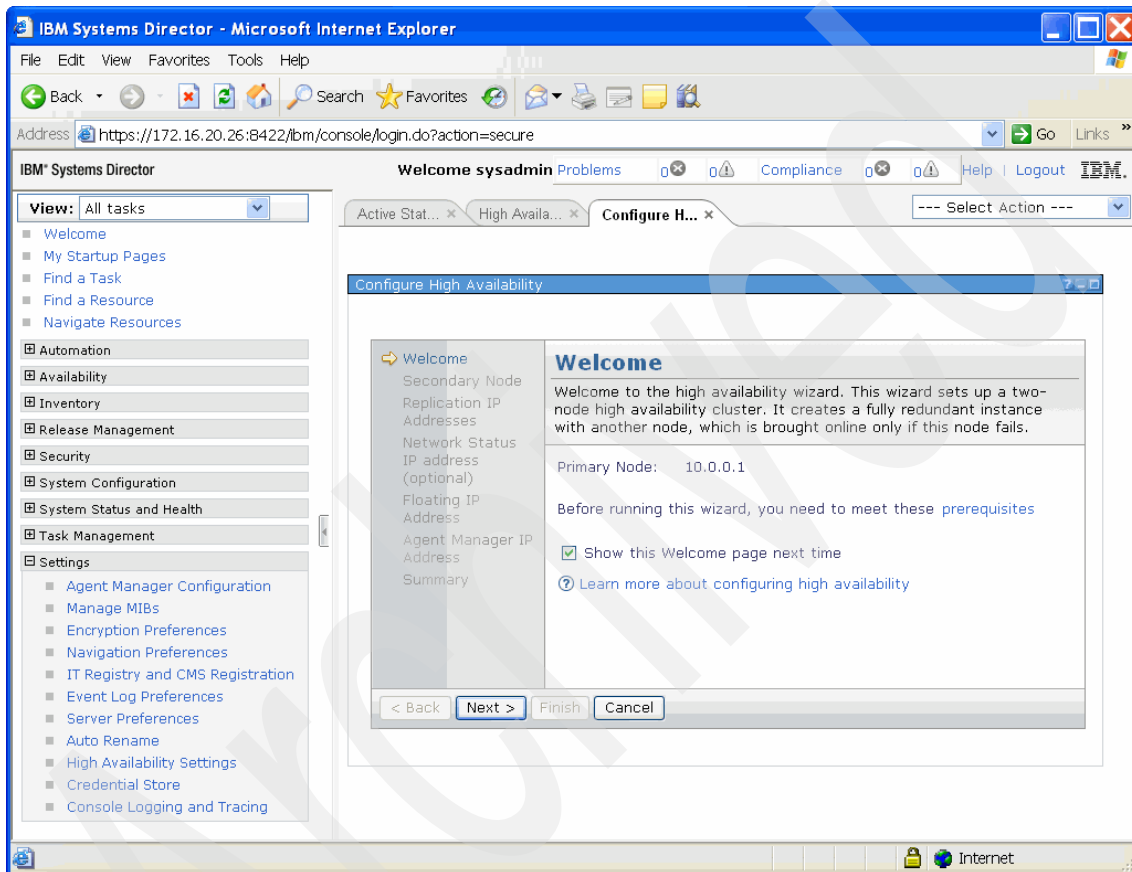


Figure 12-8 Welcome page

3. In the Secondary Node setup page (Figure 12-9), enter the IP address or host name and the password for the sysadmin user on that SDMC. Click **Next**.

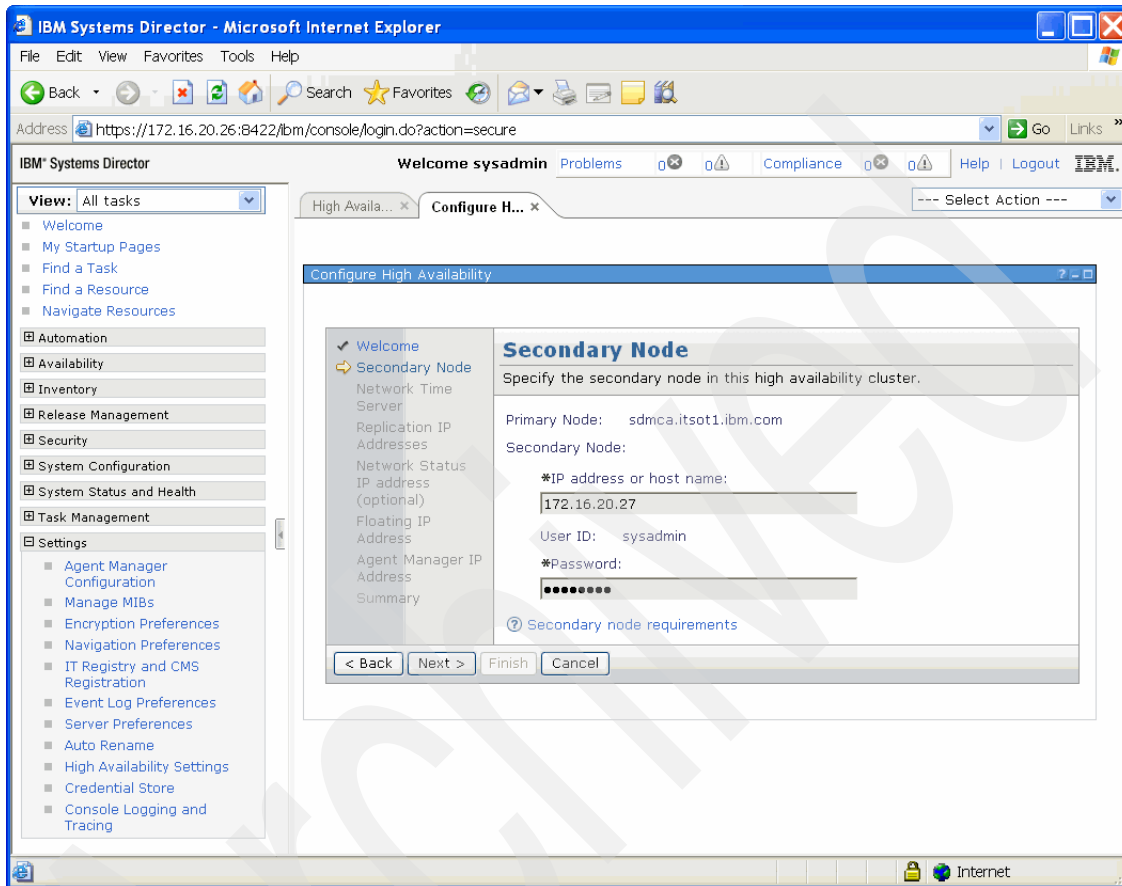


Figure 12-9 Secondary Node page

4. In the Network Time Server page (not shown), specify the IP address for a network time server or choose a primary node as the time server for both nodes. Click **Next**.

5. In the Replication IP Address page (Figure 12-10), specify the IP addresses to use for data replication between the two nodes (one on each node). Click **Next**.

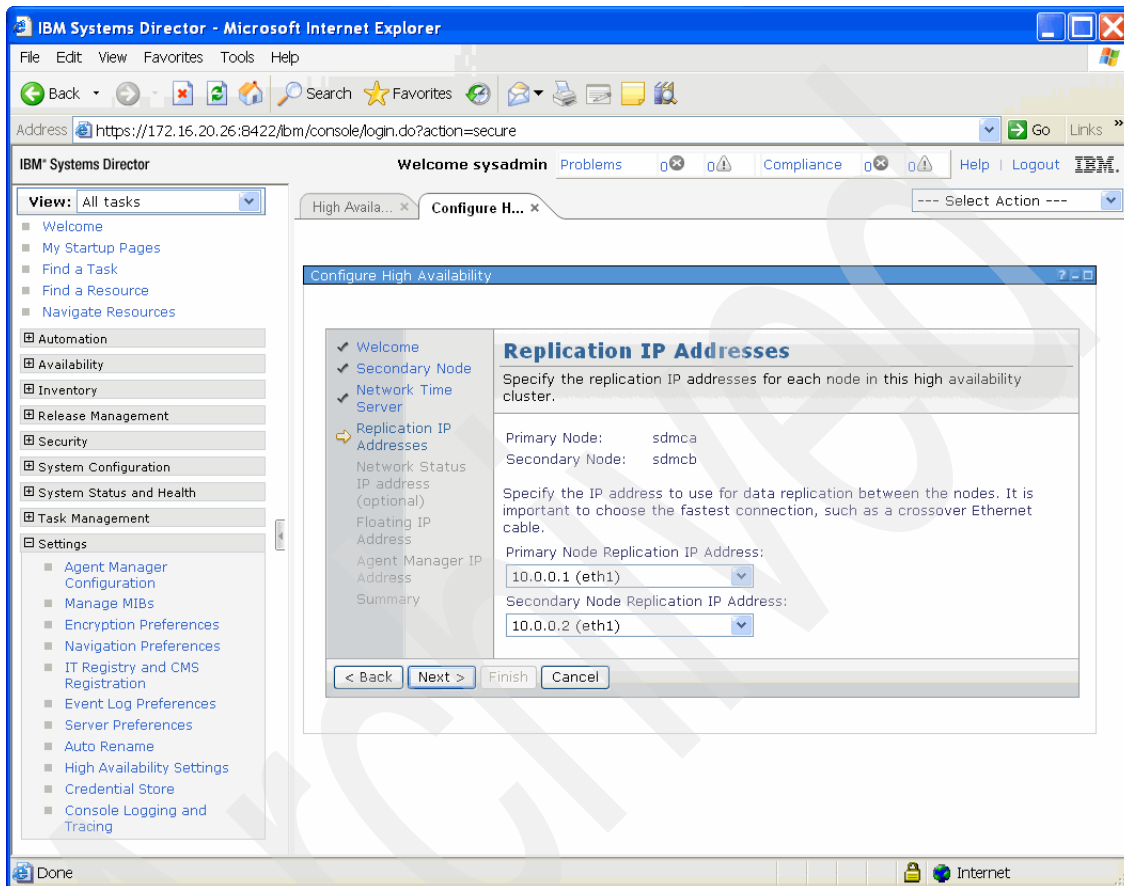


Figure 12-10 Replication IP Address settings page

6. If you want a network status IP address, determine an appropriate IP address and enter it into the Network Status IP address page (Figure 12-11). Click **Next**.

Note: A good choice for this address is the SDMCs gateway IP address.

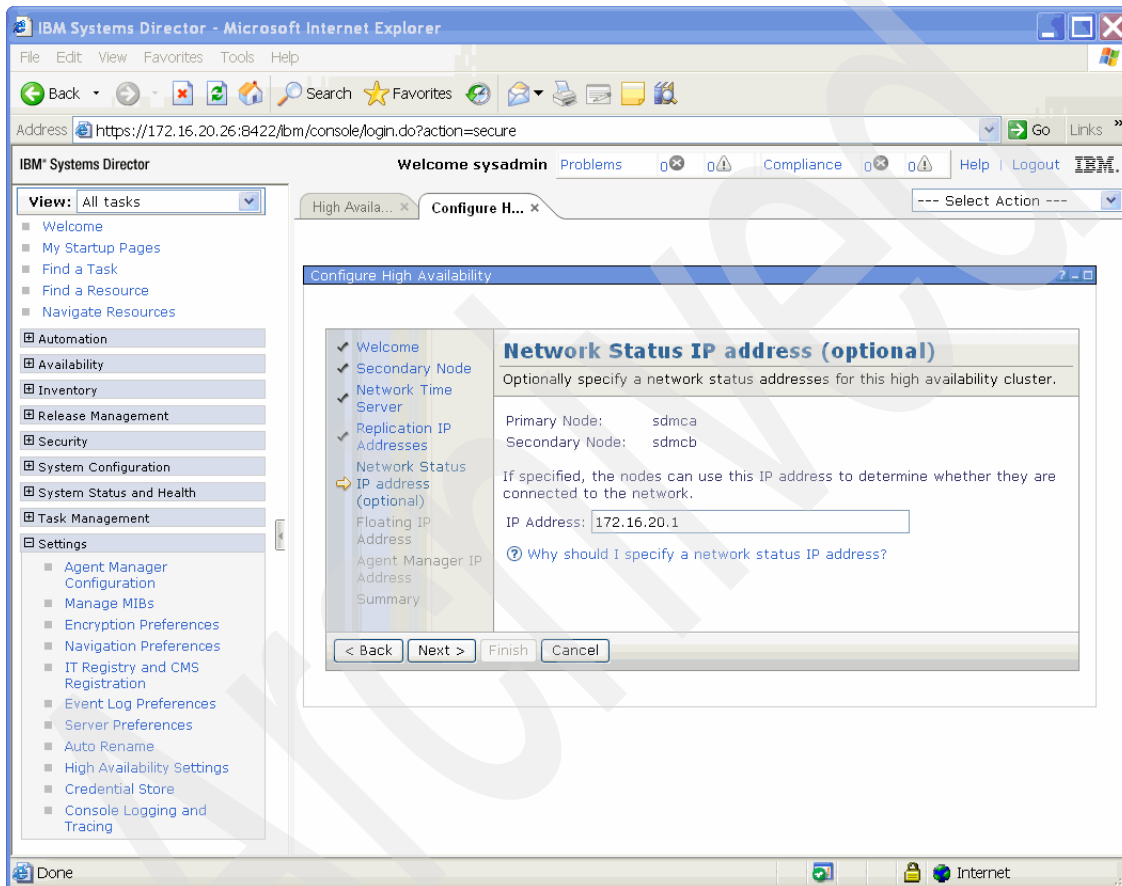


Figure 12-11 Network Status IP address

7. Determine the available IP address to be used as the floating IP address and enter this address at the Floating IP Address page (Figure 12-12). Click **Next**.

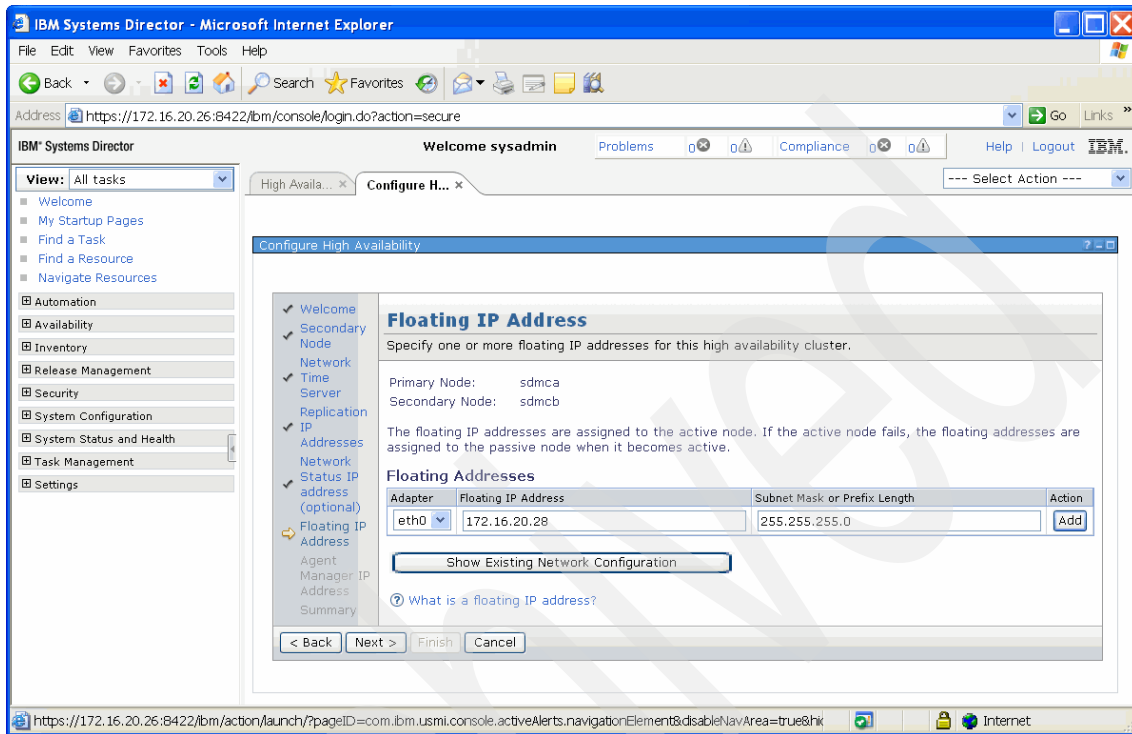


Figure 12-12 Adding floating IP addresses

8. If you use Systems Director Common Agent Services, you must specify an agent manager IP address so that the active node can manage the agents. Figure 12-13 shows the Agent Manager IP Address page in the setup wizard. Click **Next**.

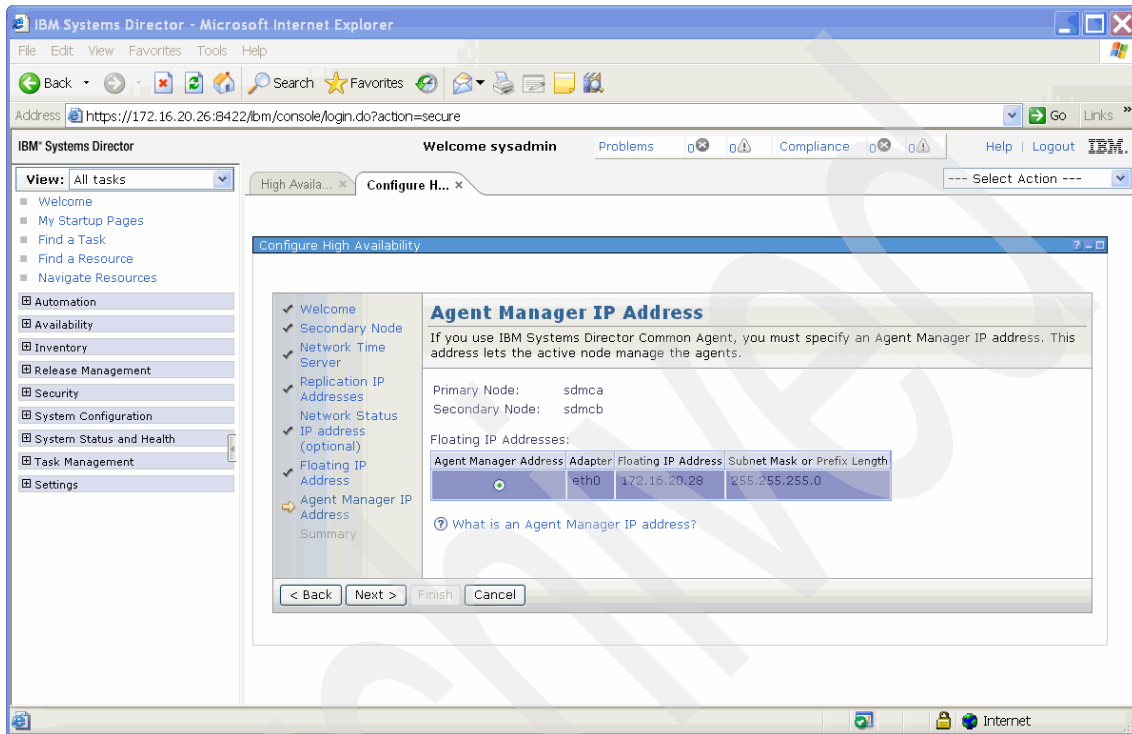


Figure 12-13 Agent Manager IP Address page

9. The final page (Figure 12-14) shows the summary of all the configuration inputs entered during the setup. Review the information and click **Finish**.

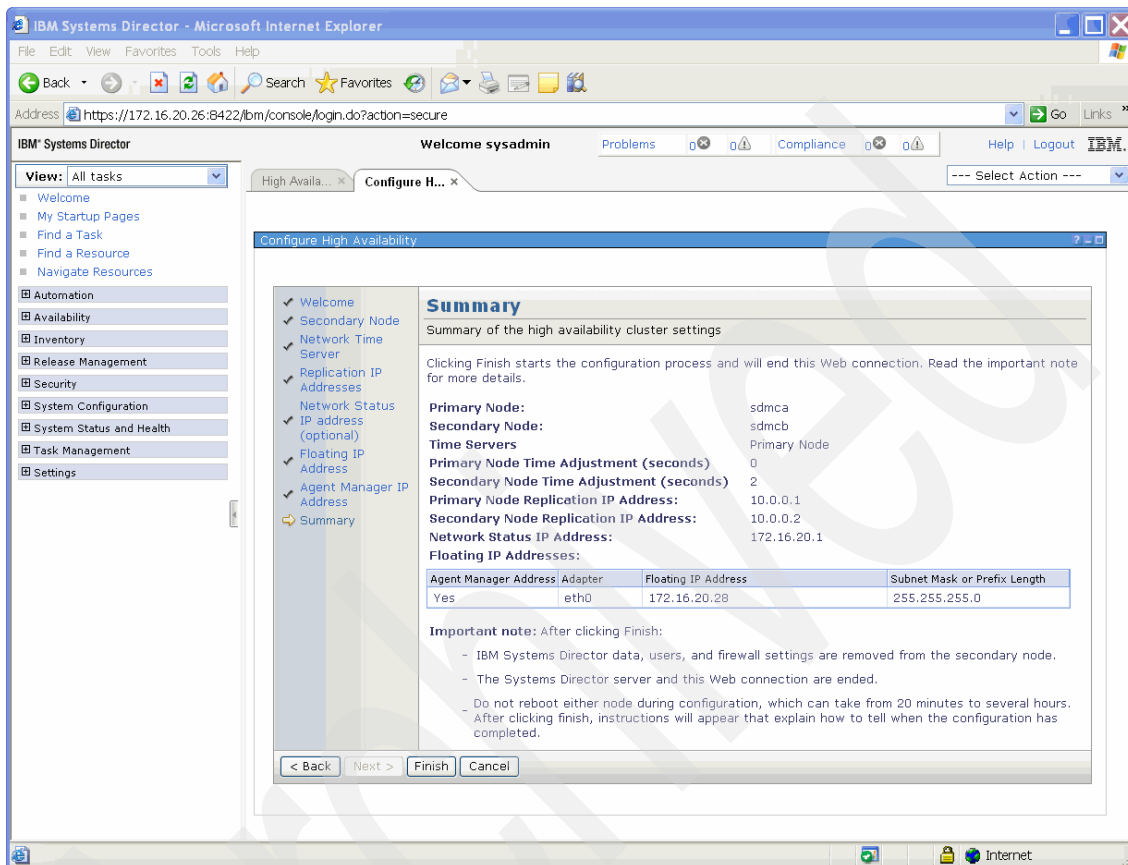


Figure 12-14 Summary page

While high availability is being configured, Systems Director is shut down on both cluster nodes. During this time, information is copied from the primary to the secondary node. The speed of your network determines how long the replication takes.

To monitor the status of the configuration, perform the following steps:

1. Start an SSH session from an SSH client to connect to either node. Log in as sysadmin.
2. Run **smhastatus -r**. This command displays the configuration status as it proceeds.
3. Press Ctrl+C to exit **smhastatus**.

After the configuration completes, you can use the floating IP address to connect to the Systems Director server on the active node.

12.4.2 Steps to install High Availability using the CLI

As an alternative to the graphical user interface, you can use the SDMC command-line interface to configure and administrate High Availability.

To configure High Availability using the CLI, connect, using an SSH session, to the SDMC that is designated to be the primary node in the High Availability cluster. Log in as sysadmin and issue the following command with the respective parameters:

```
smcli configureHA --secondary-node <second node> --password <password>
--primary-rep-addr <primary replication IP address>
--secondary-rep-addr <secondary replication IP address> --floating-addr
"<floating IP address>,<network interface>"
```

Example 12-1 shows the command with parameters that was run to create an SDMC High Availability cluster in the ITSO lab environment.

Example 12-1 Configuring High Availability using the CLI

```
smcli configureHA --secondary-node sdmcb --password passw0rd
--primary-rep-addr 10.0.0.1 --secondary-rep-addr 10.0.0.2
--floating-addr "172.16.20.29,eth0"
```

Additional options (such as the network time server or tiebreaker address) can also be specified using additional flags. Run **smcli configureHA --help** or refer to the **configureHA** man pages for information about additional options.

Additional command-line tools

Here are additional command-line tools for installing and configuring High Availability. Run **<command> --help** or use the man pages for information about additional options:

| | |
|--------------------------|-------------------------------------------------------|
| smcli configureHA | Performs the initial High Availability configuration. |
| smcli failover | Performs a manual failover. |
| smcli removeHA | Removes the High Availability configuration. |
| smhastatus | Returns a High Availability status. |
| smha | Manages High Availability. |

12.5 Active/Passive High Availability: Updates

For the initial release of the SDMC, you must update it by performing the following steps:

1. The active node must be updated.
2. A manual failover must be performed.
3. The new active node that was previously passive must now be updated.
4. Another manual failover must be performed.

Updates only need to be downloaded once, as the update repository is mirrored between the two SDMC nodes.

Both nodes should be updated in sequence in a timely fashion.

Updates will not take effect until the failover occurs.

A backup/snapshot should be taken of both nodes prior to updating the SDMC nodes.

12.6 Active/Passive High Availability: Upgrades

For the initial release of the SDMC, you must upgrade it by performing the following steps:

1. Download and select to install the upgrade on the active node (node A).
2. A manual failover must be performed after the Update Manager finishes installing the upgrade. It is not active until node A is rebooted.
3. On the new active node (node B) that was previously passive, search for updates (should be in the mirrored storage). Select to install them.
4. Reboot node A.
5. A second manual failover must be performed that will make node A active again.
6. Reboot node B.
7. Collect software inventory for both nodes again.

The upgrade need only to be downloaded once, as the update repository is mirrored between the two SDMC nodes.

Note: You should not deviate from the above procedure, or you might reload both nodes. Currently, upgrading mirrored data imposes restrictions on when you activate the new code (although this may be changed in future releases).

The Director data is at a Snapshot level that is equivalent to when you started the upgrade. Events received during the upgrade will be lost.

Note: A snapshot of each node should be taken prior to upgrading the SDMC nodes so that they can be restored should problems arise during the upgrade process.

Archived

Archived

Advanced System Management Interface

In this chapter, we describe how to log in to the Advanced System Management Interface (ASMI) using the IBM Systems Director Management Console (SDMC). The ASMI provides a terminal interface through a standard web browser to the service processor that allows you to perform general and administrator level service tasks. The ASMI allows you to perform service functions and various system management functions. For a description of the available functions, refer to Chapter 14, “Advanced System Management Interface”, in *Hardware Management Console V7 Handbook*, SG24-7491.

13.1 Connecting to ASMI using the SDMC

To connect to the ASMI using the SDMC, perform the following steps:

1. On the SDMC Resources tab, select the managed system to which you want to connect through ASMI.
2. Right-click the managed system name and select **Operations** → **Launch Advanced System Management (ASM)** (Figure 13-1).

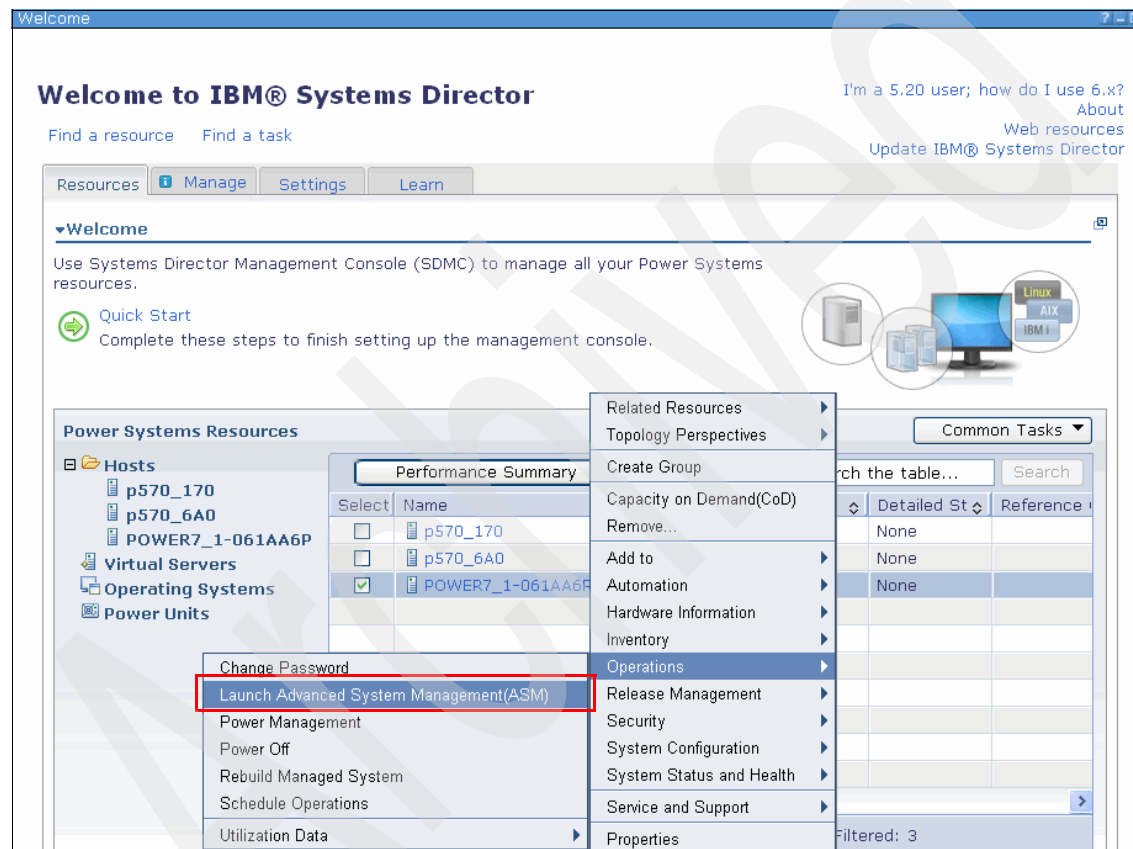


Figure 13-1 Connecting to ASMI using the SDMC

3. A page opens that has a drop-down menu for the service processor to which you want to connect (Figure 13-2).

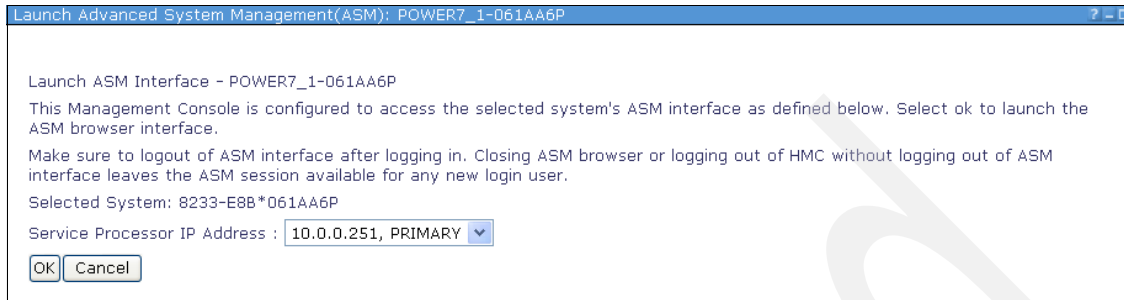


Figure 13-2 Selecting the Service Processor

4. A new browser page opens with the login page of the ASMI (Figure 13-3).

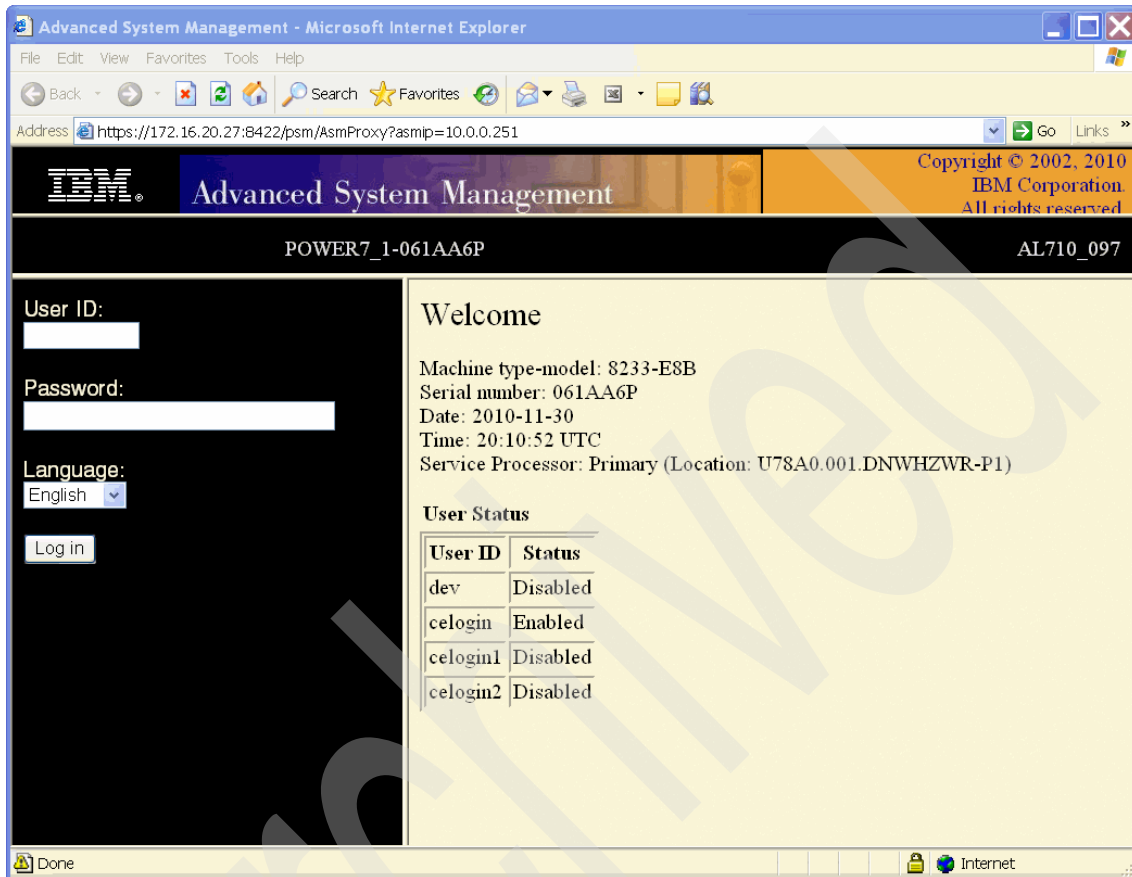


Figure 13-3 ASMI login

We only give here an overview of the ASMI menu and a brief description of the functions. For further information, refer to Chapter 14, "Advanced System Management Interface", in *Hardware Management Console V7 Handbook*, SG24-7491.

13.2 Connecting to ASMI using the CLI

To connect to the ASMI using the SDMC command-line interface, you must have an X-Server on your local machine. Connect remotely to the SDMC command line through an SSH connection and export your display. Here is an example, with the IP of your local machine, of exporting the display:

```
export DISPLAY="172.16.254.14:0"
```

Afterwards, you can start the ASMI by running the following command using the IP address of the service processor to which you want to connect:

```
asmmenu --ip 10.0.0.251
```

Note: For the `asmmenu` command, you do not have to use the `smcli` prefix.

An ASMI page will open (you will be prompted to first accept an HTTPS certificate).

13.3 Using ASMI

We provide an overview of the ASMI menu and a brief description of the functions. For further information, refer to Chapter 14, “Advanced System Management Interface”, in *Hardware Management Console V7 Handbook*, SG24-7491.

- ▶ **Power/Restart Control**
 - Power On/Off System** Powers on/off a system and sets power on options.
 - Auto Power Restart** Lets a system automatically restart after an unexpectedly power down.
 - Immediate Power Off** Shuts down a system immediately.
 - System Reboot** Reboots the system.
 - Wake On LAN** Lets you activate wake on LAN.
- ▶ **System Service Aids**
 - Error/Event Logs** Displays system error and event logs.
 - Serial Port Snoop** This function is not available when your system is connected to the SDMC.

| | |
|-----------------------------------------|--------------------------------------------------------------------------------------------------|
| System Dump | Initiates a system dump. |
| Service Processor Dump | Initiates a service processor dump. |
| Partition Dump | This function is not available when your system is connected to the SDMC. |
| Serial Port Setup | This function is not available when your system is connected to the SDMC. |
| Modem Configuration | This function is not available when your system is connected to the SDMC. |
| Call-Home/Call-In Setup | This function is not available when your system is connected to the SDMC. |
| Call-Home Test | This function is not available when your system is connected to the SDMC. |
| Reset Service Processor | Reboots the Service Processor. |
| Factory Configuration | Restores the system to the factory default settings. |
| Deconfiguration Records | This function is not available when your system is connected to the SDMC. |
| Resource Dump | Initiates a resource dump on the system server firmware. |
| USB-Enabled Service Functions | Lets you handle attached USB devices. |
| ► System Information | |
| Vital Product Data | Displays manufacturers vital product data (VPD). |
| Power Control Network Trace | Performs a system power control network (SPCN) trace and displays the results. |
| Previous Boot Progress Indicator | Displays the previous boot progress indicator. |
| Progress Indicator History | Displays the progress of codes that are displayed in the control panel during the previous boot. |
| Real-time Progress Indicator | Displays the progress and error codes that are currently displayed on the control panel. |

Memory Serial Presence Detect Data

Shows manufactures data of detected memory modules.

Firmware Maintenance History

Shows the history of service processor firmware updates.

► System Configuration

System Name

Lets you change the system name

Configure I/O Enclosures

Lets you configure I/O enclosures.

Time of Day

Lets you change the systems current data and time.

Firmware Update Policy

Lets you specify if firmware updates are allowed from the operating system when the system is managed by a SMDC.

PCI Error Injection Policy

Controls the PCI injection policy.

Interposer Plug Count

This function is not available when your system is connected to the SDMC.

HSL Opticonnect Connections

Lets you set how to handle HSL Opticonnect Connections.

I/O Adapter Enlarged Capacity

Controls the size of PCI memory space allocated to each PCI slot.

Hardware Management Consoles

Disconnects the SDMC from your system.

Virtual Ethernet Switches

Controls the number of virtual Ethernet Switches allocated by the system server firmware.

Floating Point Unit Computation Test

Lets you set the floating point unit test policy or runs the test immediately.

Power Management Mode Setup

Lets you enable or disable the power saver mode.

Selective Memory Mirroring

This function is not available when your system is connected to the SDMC.

Acoustic Mode Control

This function is not available when your system is connected to the SDMC.

– Hardware Deconfiguration

Deconfiguration Policies

Lets you set various policies to deconfigure processors and memory in certain situations.

Field Core Override

This function is not available when your system is connected to the SDMC.

Processor Deconfiguration

Lets you deconfigure a single processor.

Memory Deconfiguration

Lets you deconfigure memory banks manually.

Processing Unit Deconfiguration

Lets you deconfigure a processing unit.

– Program Vital Product Data

System Brand

Lets you set the system brand name.

System Keywords

Displays the system key words (for example, machine type-model, serial number, and unique ID).

System Enclosures

Displays system enclosure details.

– Service Indicators

System Information Indicator

Lets you disable the system attention indicator.

Enclosure Indicator

Lets you turn on or off the identify indicators in each enclosure.

Indicators by Location code

By specifying a location code you can view or modify its current state.

Lamp Test

Performs an LED test on the control panel to determine if one of the LEDs is not functioning properly.

- ▶ Network Services
 - Network Configuration** Displays and modifies the network configuration of the service processor(s).
 - Network Access** Lets you control the access to the service processor (firewall).
- ▶ Performance Setup
 - Logical Memory Block Size** Lets you set the logical block memory size for your system.
 - System Memory Page Setup** Lets you set up the system with larger memory pages to improve system performance.
- ▶ On Demand Utilities
 - CoD Order Information** Shows the information needed to order CoD activation features.
 - CoD Activation** Lets you enter an activation code.
 - CoD Recovery** Resumes the booting process of the server firmware to cause the CoD key to become recognized and activated.
 - CoD Command** Lets you issue a CoD command.
 - CoD Processor Information** Displays the information about the CoD processors.
 - CoD Memory Information** Displays the information about the CoD memory.
 - CoD VET Information** Displays the information about available Virtualization Engine technologies.
 - CoD Capability Settings** Displays information about the CoD capabilities that are enabled/disabled.
- ▶ Concurrent Maintenance
 - Control Panel** Lets you replace the operator panel.
 - RIO/HSL Adapter Slot Reservation** Displays the RIO/HSL adapter slot reservation.

► Login Profile

Change Password

Lets you change the general user, administrator, and HMC access passwords.

Retrieve Login Audits

Lets you review the login history for the ASMI.

Change Default Languages

Lets you change the language that is displayed on the ASMI Welcome page prior to login and during your ASMI session if you do not choose an alternative language at the time of login.

Update Installed Languages

Lets you install another language on the next firmware update.

User Access Policy

Lets you grant or deny access to service and development personnel.



Service and support

This chapter provides information about the service and support features available on IBM Systems Director Management Console (SDMC) to handle serviceable hardware problems and provide call home facilities.

14.1 Introduction

Service and Support Manager (SSM) is part of IBM Systems Director and automatically detects serviceable hardware problems and collects supporting data for serviceable hardware problems that occur on your managed systems. The Electronic Service Agent tool is integrated with the Service and Support Manager and transmits serviceable hardware problems and associated support files to IBM support.

The Service and Support Manager includes the following features:

- ▶ Automatically detects serviceable hardware problems on the managed systems.
- ▶ The Electronic Service Agent tool securely transmits serviceable hardware problems, associated support files, and performance management data to IBM support.
- ▶ Collects and securely transmits scheduled system inventory and diagnostic support files to an IBM database, which is available for IBM support personnel.
- ▶ Communicates with IBM support using a secure connection using encryption and authentication.
- ▶ Includes the option to send email notifications when a serviceable problem is detected and a service request is opened.

SDMC extends the capabilities of the Service and Support Manager to provide service and support functions on Power Systems. SDMC works in conjunction with the Service and Support Manager and takes responsibility for performing tasks that are related to the serviceability of Power Systems. SDMC makes use of the Service and Support Manager to perform functions such as transmission of serviceable events and support files to IBM support.

14.2 Setup wizard

To set up the Service and Support Manager to report serviceable problems to IBM, you have to run the Service and Support Manager Getting Started Wizard. You can find the wizard on the Welcome to IBM Systems Director page below Serviceability tasks (Figure 14-1).



Figure 14-1 Service and Support Manager Getting Started Wizard

Perform the following steps:

1. Click the **Service and Support Manager Getting Started Wizard** link and the wizard opens (Figure 14-2). Click **Next**.

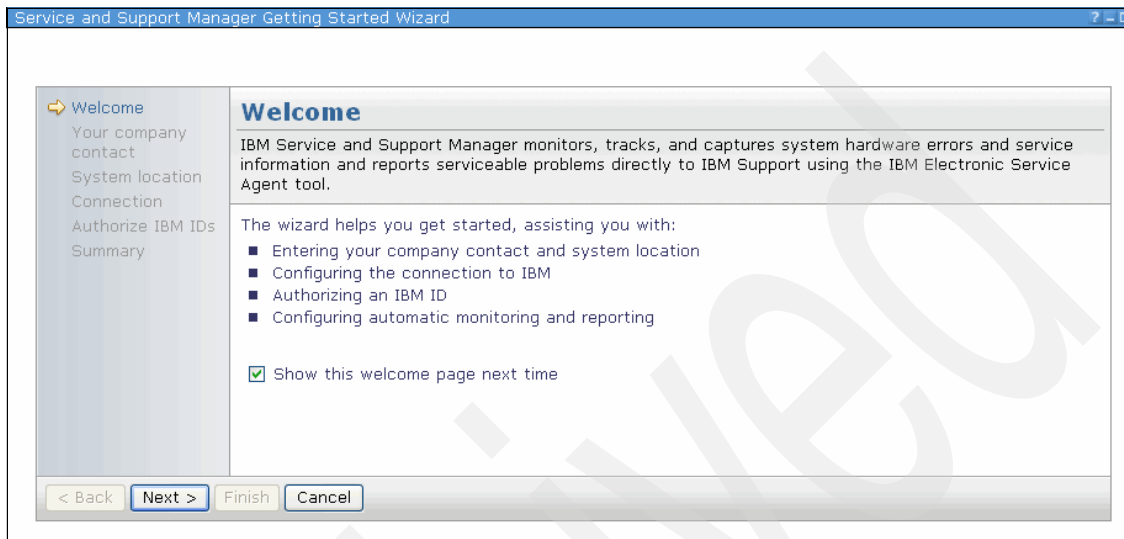


Figure 14-2 Welcome page of the SSM Getting Started Wizard

2. On the next page, enter your company's contact data (Figure 14-3).

Service and Support Manager Getting Started Wizard

Your company contact

Provide information about the person that IBM Support may contact about a problem reported by Electronic Service Agent.

Navigation:

- ✓ Welcome
- ➔ Your company contact
- System location
- Connection
- Authorize IBM IDs
- Summary

Form Fields:

- *Contact name:
- *Company name:
- *Telephone number:
- Fax number:
- Alternate fax number:
- *E-mail:
- Alternate e-mail:
- Help desk number:
- Pager number:
- Street address Line 1:
- Line 2:
- Line 3:
- City:
- State or province:
- *Country or region:
- Postal code:

Buttons: < Back, Next >, Finish, Cancel

Figure 14-3 Company contact page

3. The fields marked by an asterisk are mandatory and must be completed before proceeding. When you click **Next**, the System location page opens and requires information as to where your system (the SDMC) is physical located (Figure 14-4).

Service and Support Manager Getting Started Wizard

System location

Provide default information about the physical locations of your systems. Information can be overridden for specific systems by clicking Navigate Resources, selecting a system, and clicking Location under the Additional Properties heading.

*Telephone number:

*Country or region:

*Street address:

*City:

*State or province:

*Postal code:

*Building:

Floor:

Room number:

Row:

Aisle:

Displaced height (cm):

Altitude (meters):

Other information:

< Back Next > Finish Cancel

Figure 14-4 System location page

4. As on the page in Figure 14-3 on page 339, fields marked with an asterisk are mandatory. Complete the fields and click **Next**.

5. In the Connection page, you have to specify how the SDMC can connect to IBM, either through a direct Internet connection or through a proxy server (Figure 14-5).

Figure 14-5 Connection page

There is also a Test Connection, button that lets you test whether your SDMC has a connection to IBM.

Unlike the HMC, where VPN and modem are also options, on the SDMC only SSL over an Internet connection is an option to send serviceable requests to IBM.

6. When you click **Next**, the Authorize IBM IDs page opens (Figure 14-6).

Service and Support Manager Getting Started Wizard

✓ Welcome
✓ Your company contact
✓ System location
✓ Connection
➔ Authorize IBM IDs
Summary

Authorize IBM IDs

Provide an IBM ID to be associated with information sent by Electronic Service Agent.

Providing your IBM ID enables you to access the service information transmitted to IBM by Electronic Service Agent. If you do not have an IBM ID, you can obtain one at <http://www.ibm.com/registration>. Secure access to the service information is available via the IBM Electronic Services Web site (<http://www.ibm.com/support/electronic>), at any time, regardless of your system status. The My Systems link provides several functions aimed at saving you time and helping you solve problems more quickly.

If you choose not to enter your IBM ID now, you can enter it later using the Service and Support Manager Summary page.

Primary IBM ID:

Secondary IBM ID:

< Back Next > Finish Cancel

Figure 14-6 Authorize IBM IDs

Here you can provide the IBM IDs that can later access the service information transmitted to IBM by the Electronic Service Agent. This step can also be done at a later point.

7. When you click **Next**, the Summary page opens (Figure 14-7).

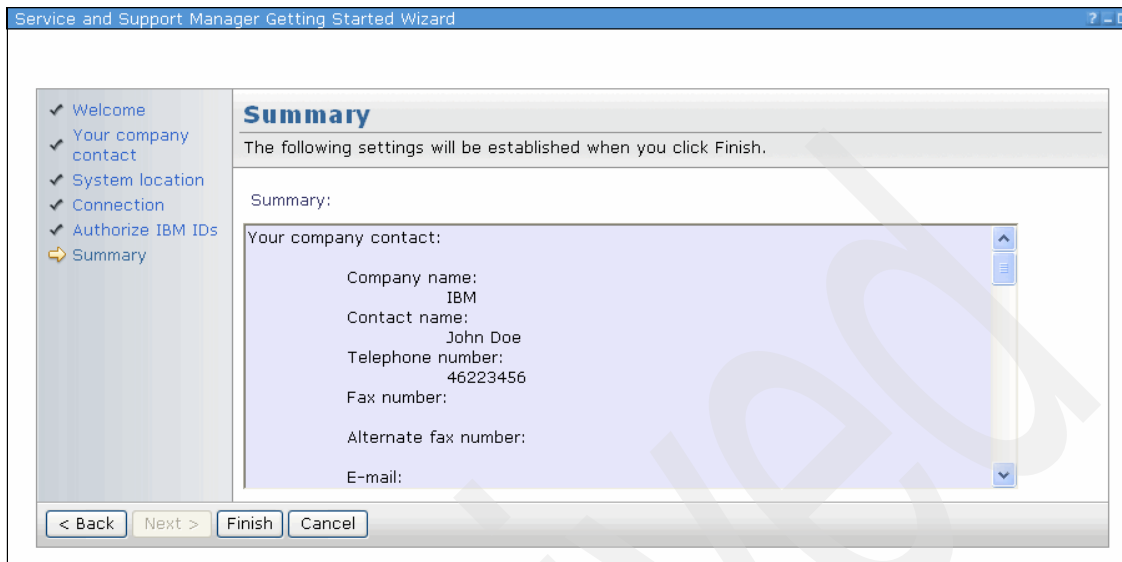


Figure 14-7 Summary page

8. You can always go back from here if the displayed data is not as expected. If you are satisfied with the data provided, click **Finish**. You can always go back to the Welcome page and start the Service and Support Manager Getting Started Wizard again.

14.3 Call Home

Call Home is the utility IBM uses to automatically capture data and report errors in the SDMC. This feature minimizes the need for human intervention in gathering and offloading data to IBM support. The Service and Support Manager Getting Started Wizard configures the Call Home feature in SDMC, enabling it to automatically contact IBM if a problem occurs.

Verify that SDMC is monitoring the managed systems from the Navigate Resources page. If there are any problems with the monitoring, SDMC is not able to send error information to IBM support. Go to the **Navigate Resources** page and click **Service and Support Groups**. Click **Monitored Systems** and verify that the Power Systems that you are managing are listed there.

The tasks related to the Call Home feature are available on the context menu of the monitored systems. Right-click any of the monitored systems and you can see the context menu (Figure 14-8).

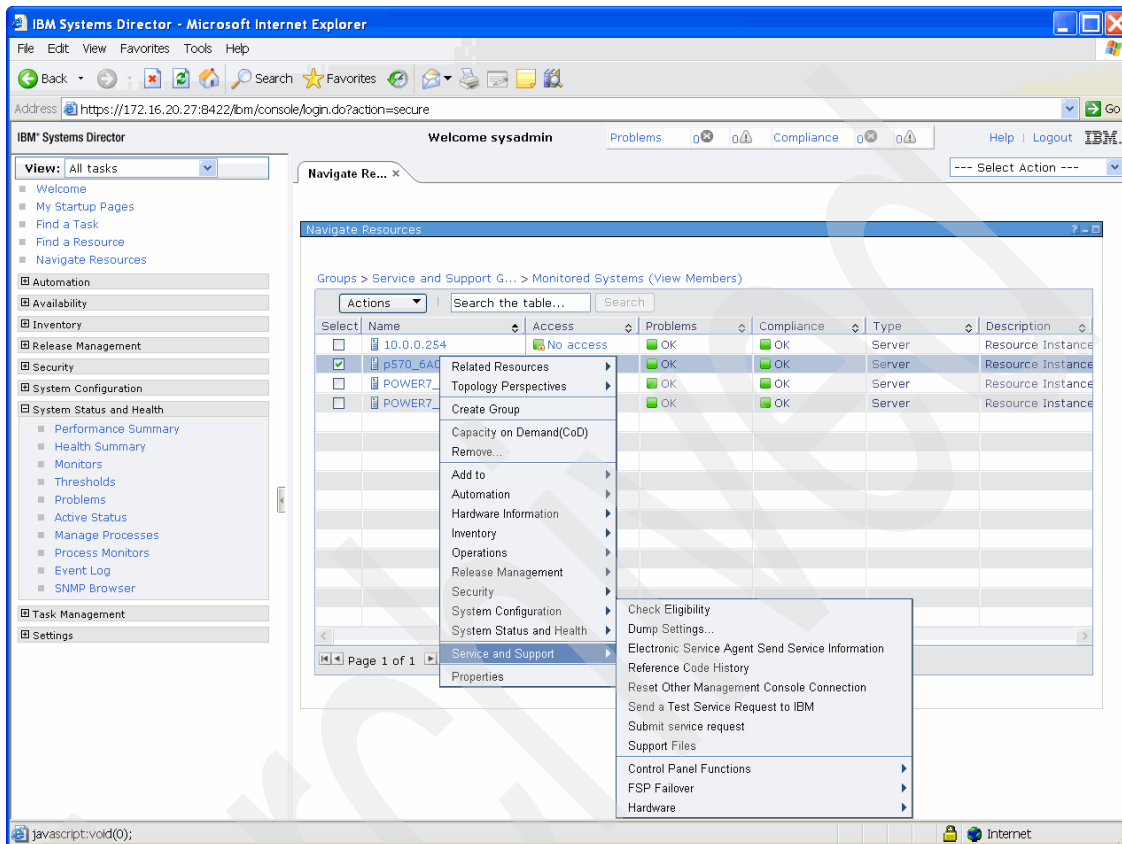


Figure 14-8 Service and Support context menu

You can perform the following Call Home tasks from this context menu:

Electronic Service Agent Send Service Information

You can send the service information manually from the SDMC to IBM Support. This task can be scheduled and made to run immediately or at a later time and also at regular intervals.

Send a Test Service Request to IBM

This task sends a test service request to IBM and verifies whether the Call Home feature is working properly in the SDMC. This task can also be scheduled at a later time and at regular intervals.

Support Files

You can use this task to collect the support files for the monitored system. The support files can be Resource dump, System dump, Node controller dump, Power dump, or a System controller dump. You can send these support files to IBM using this task.

Submit Service Request

You can send a service request to IBM by briefly describing your problem and also providing details regarding the problem.

You can also verify the Call Home configuration in your SDMC from the Service and Support Manager page (Figure 14-9). You can launch it from the Manage tab of the Welcome page.

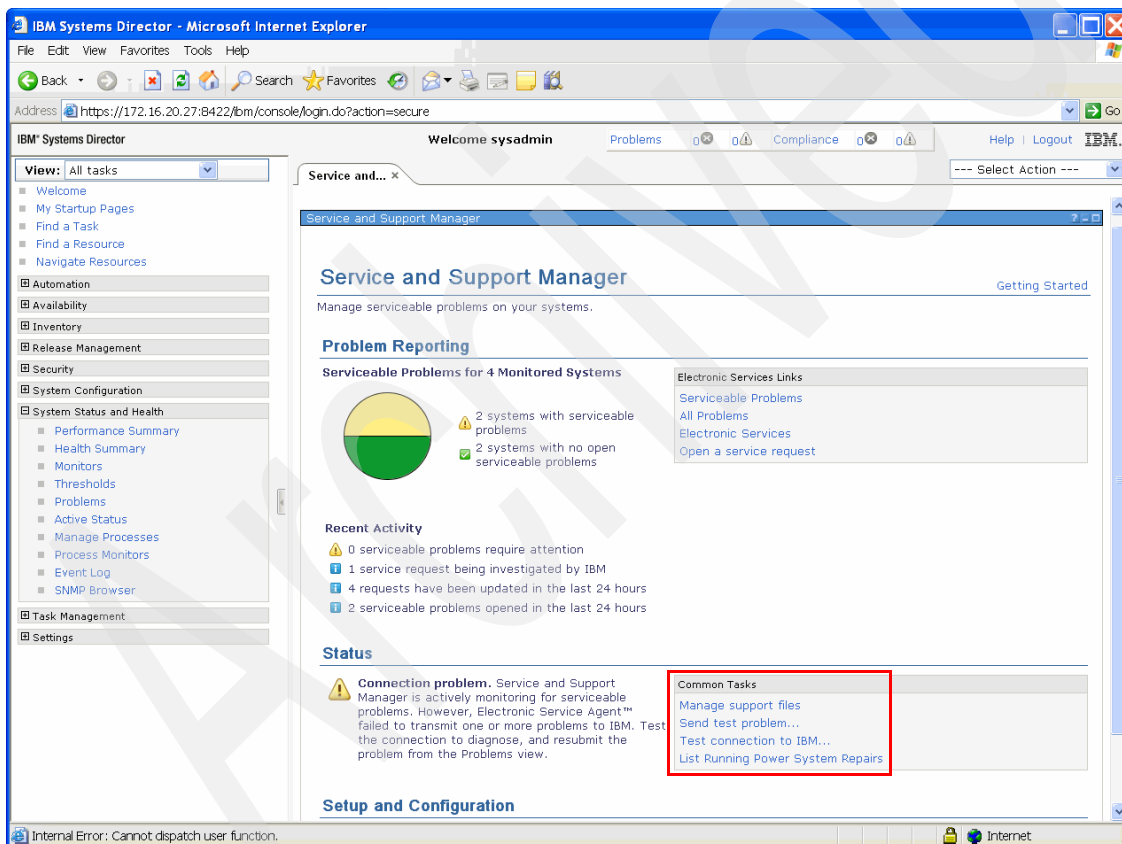


Figure 14-9 Service and Support Manager page

A list of common tasks are provided in the Status area. You can manage the support files, send a test problem, and test the connection to IBM from your SDMC from this page.

14.4 Serviceable event processing

The Service and Support Manager automatically detects error conditions and reports any hardware problem that requires service to repair it. These problems are reported to you as *serviceable events*. The Service and Support Manager provides the management of serviceable events on the managed system and the transmission of service requests for hardware problems to IBM support. These include:

- ▶ Detection of serviceable events
- ▶ Persistent storage and management of serviceable event data
- ▶ Transmission of service requests and extended error data to IBM
- ▶ Processing of duplicate serviceable events
- ▶ Supporting user actions on serviceable events
- ▶ Closure of serviceable events

14.4.1 Detection of serviceable events

The Problem Analysis component of SDMC handles the detection and analysis of serviceable events. The Problem Analysis component resides within the Service and Support Manager available in SDMC. It receives the errors directly from the FSP of the managed system and its Virtual Servers. SDMC uses the same communication methods as Remote Monitoring and Control (RMC) was used in HMC to receive OS related errors.

SDMC analyses the error indications received from the managed system and the Virtual Servers and determines whether they warrant the creation of a new serviceable event. It creates a IBM Systems Director event and provides all the information for identifying the error conditions and the resources involved. The event also specifies the failing Power System. The Service and Support Manager listens for the creation of this event and will create an entry in its database. This triggers the creation of the IBM Systems Director Status Set. After the IBM Systems Director Status Set is created, the serviceable event is displayed on the Problems page.

14.4.2 Persistent storage and management of serviceable event data

Service and Support Manager persists all the information that is available with the event in its database tables. SDMC provides the information for the event. This event also provides information about the location of the Extended Error Data (EED) files that have been collected on behalf of the serviceable event. SDMC also maintains a cache of information about the serviceable events.

During the life cycle of the serviceable event, The Service and Support Manager also creates events so that the subsequent functions within the Service and Support Manager can process the original event.

14.4.3 Transmission of service requests and EED to IBM Support

The original event created by the Problem Analysis component contains the information necessary to send a service request to IBM Support using the ECC protocol. The Service and Support Manager provides the ability to control whether the service requests are transmitted automatically or manually. By default, the service requests are transmitted automatically. The service requests transmitted on SDMC are equivalent to the service requests sent by an HMC when using the ECC protocol.

IBM Support creates a problem management record hardware (PMH) in RETAIN® upon receiving the service request from the Electronic Service Agent. RETAIN is a database system used internally within IBM for providing service support to IBM field personnel and customers. Once the PMH is created, the Electronic Service Agent starts transmitting the EED files that were previously collected by the Problem Analysis component. These EED files have a primary and secondary designation. Only the primary EED files are transmitted automatically when the service request is transmitted.

14.4.4 Processing of duplicate events

SDMC handles the detection of duplicate serviceable events. It determines whether a given condition is a duplicate serviceable event or not. If it detects a duplicate serviceable event, SDMC initiates a request to the Service and Support Manager to update the duplicate event information in its database tables, which also appears in the Problems page on the GUI.

14.4.5 User actions

You can see a problems dashboard on top of the web interface that displays the number of Problems and Compliances. This dashboard shows the number of Problems and Compliance issues with the managed system.

The details of the problems are listed in the Problems page. Select **System Status and Health** → **Problems** to open the Problems page (Figure 14-10).

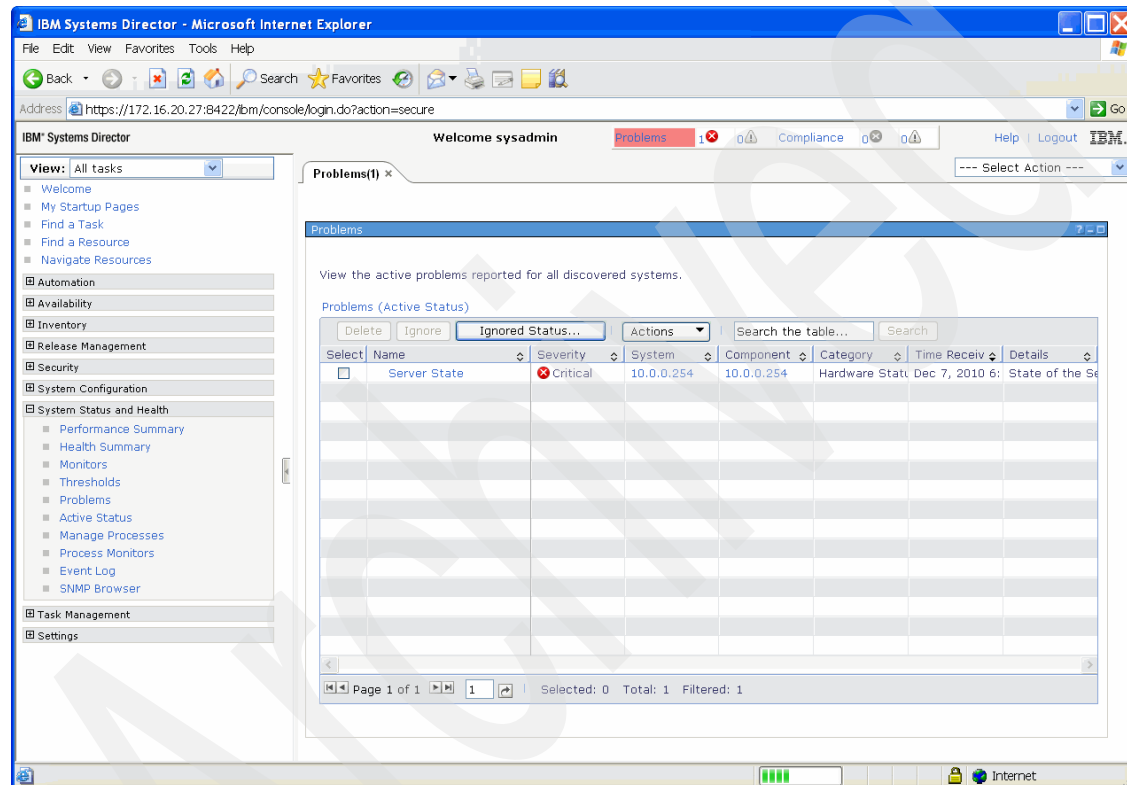


Figure 14-10 Problems page

This page shows all the active problems reported for all discovered systems. Click any of the problems and you should see the properties page of the selected problem (Figure 14-11).

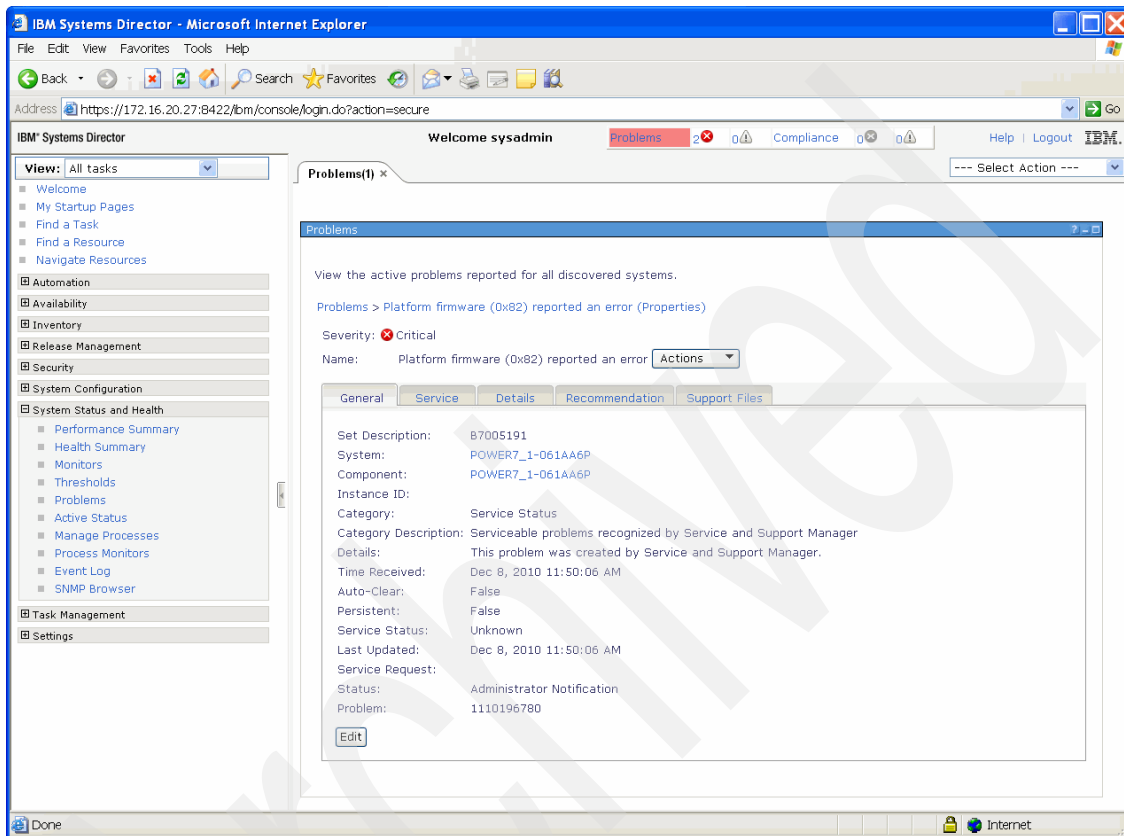


Figure 14-11 Problems: General properties

The General tab provides information from the Director Status Set of the event. The Service tab provides information about the state of the service request and maintains the information shown in the service log associated with the problem. The Recommendation tab contains a Reference link that, when clicked, opens another browser page. This page (Figure 14-12) has the Problem Explanation and Determination information along with the reference code. The Support Files tab contains the list of EED files that you can submit to IBM.

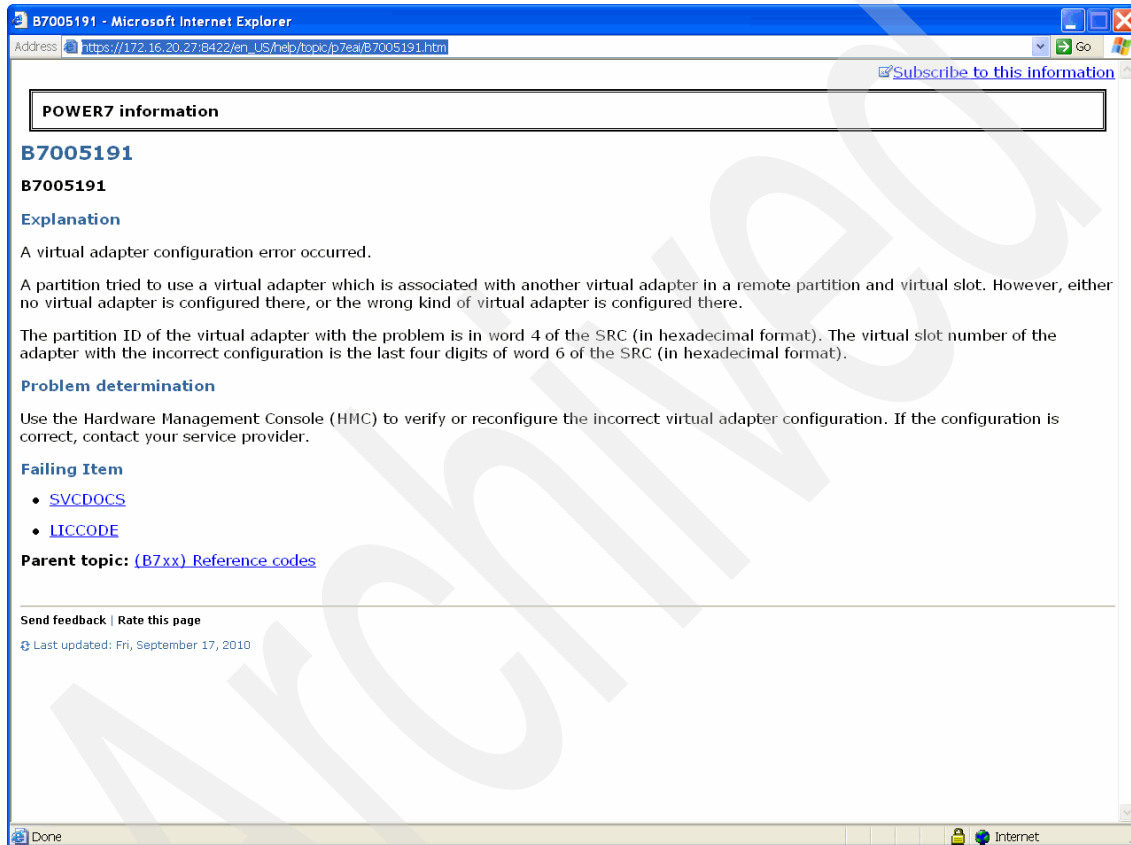


Figure 14-12 Problem Explanation page

14.4.6 Closure of serviceable events

When a Software Service Representative (SSR) completes the Guided Repair procedure for a given serviceable event, they can force the closure of the service request at IBM Support. In that case, the Service and Support Manager sends an update to IBM Support to indicate that the service request should be closed. The serviceable events goes into a closed state.

You can also close a serviceable event by selecting **Request Closure** of a given service request, which causes the Service and Support Manager to update the service request and indicate that you have requested closure of the service request. The serviceable event then goes into a closed state. Serviceable events, including problems, are displayed on the Problems page until you delete the problem from the Problems page.

14.5 Support File Management (dump)

The Service and Support Manager (SSM) provides the management of support files (including extended error data collected with serviceable events, and dump files collected via other means). The Service and Support Manager provides the following capabilities in the area of support file management:

- ▶ Supports the file user interface.
- ▶ Collection of support files.
- ▶ Transmission of support files to IBM.
- ▶ Copying support files to removable media devices (USB drives).
- ▶ Removal of support files from the SDMC appliance.
- ▶ Support file space management.

14.5.1 Support Files view

There are three different support file views provided by the Service and Support Manager:

System wide support files view

Shows all support files on the SDMC appliance for all the systems being monitored by the Service and Support Manager.

Monitored system support files view

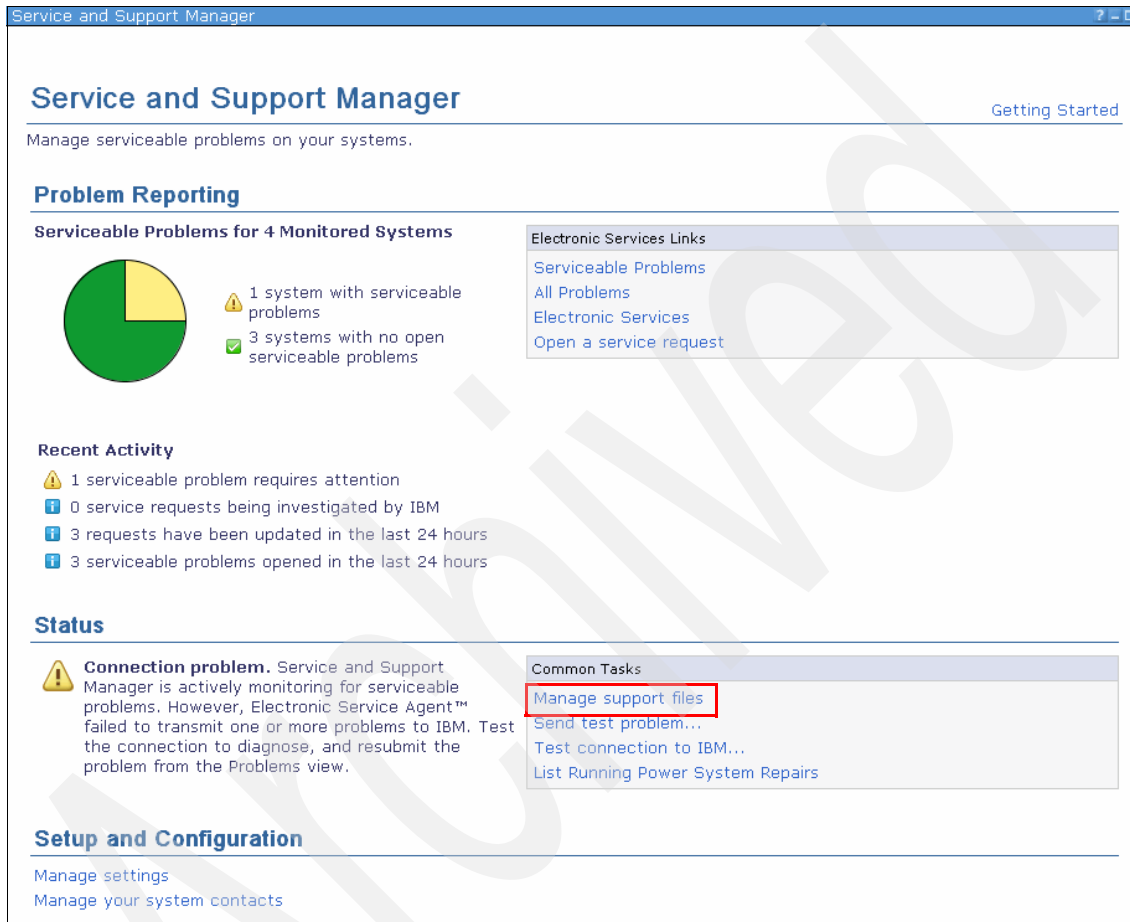
Shows all of the support files on the SDMC appliance on behalf of a given monitored system.

Serviceable problem support files view

Shows all of the support files on the SDMC appliance on behalf of a given serviceable problem.

System wide support files view

The system wide support files view can be reached by opening the **Service and Support Manager** page and clicking **Manage support files** under **Common Tasks** (Figure 14-13).



Service and Support Manager


Service and Support Manager

Getting Started

Manage serviceable problems on your systems.

Problem Reporting

Serviceable Problems for 4 Monitored Systems



- 1 system with serviceable problems
- 3 systems with no open serviceable problems


Electronic Services Links

- [Serviceable Problems](#)
- [All Problems](#)
- [Electronic Services](#)
- [Open a service request](#)

Recent Activity

- 1 serviceable problem requires attention
- 0 service requests being investigated by IBM
- 3 requests have been updated in the last 24 hours
- 3 serviceable problems opened in the last 24 hours

Status

 **Connection problem.** Service and Support Manager is actively monitoring for serviceable problems. However, Electronic Service Agent™ failed to transmit one or more problems to IBM. Test the connection to diagnose, and resubmit the problem from the Problems view.

Common Tasks

- Manage support files**
- [Send test problem...](#)
- [Test connection to IBM...](#)
- [List Running Power System Repairs](#)

Setup and Configuration

- [Manage settings](#)
- [Manage your system contacts](#)

Figure 14-13 Service and Support Manager

After you click the link, the Manage Support Files system wide view opens (Figure 14-14).

Manage Support Files

This view displays all support files on this system that have been collected by Service and Support Manager. Support files can contain detailed system information used to help diagnose a serviceable hardware problem, dump files collected from an endpoint system, event logs, and more. Use this view to see more details about collected support files, to manually collect additional support files, and to submit collected files to the IBM service provider for analysis.

Note: Support files associated with a problem cannot be submitted unless the problem itself has been submitted to IBM support and is currently in a submitted state. Click on Problems to view the current status of the problem and ensure that the status is submitted before attempting to submit any associated support files.

Support Files

Collect Support Files... Submit to IBM... Delete Support Files... Actions Search the table... Search

| Select | File | Type | System | Problem ID | St | Status | Collection Time | St | File Size | Location |
|--------------------------|------------------|-----------------------|------------------|------------|----|-----------------------|-------------------------|----|-----------|-----------|
| <input type="checkbox"/> | 57.zip | Unknown | 8233-E8B*061AA6P | 2057337504 | | Collection successful | Dec 8, 2010 11:59:19 AM | | 1.93 mb | /dump/57/ |
| <input type="checkbox"/> | additional55.zip | Compressed Error Data | 8233-E8B*061AA6P | 1110196780 | | Collection successful | Dec 8, 2010 11:50:06 AM | | 1.90 mb | /dump/55/ |
| <input type="checkbox"/> | additional57.zip | Compressed Error Data | 8233-E8B*061AA6P | 2057337504 | | Collection successful | Dec 8, 2010 11:59:19 AM | | 1.93 mb | /dump/57/ |
| <input type="checkbox"/> | additional41.zip | Compressed Error Data | 8233-E8B*061AA6P | 1011760206 | | Collection successful | Dec 8, 2010 8:56:38 AM | | 0.61 mb | /dump/41/ |
| <input type="checkbox"/> | 41.zip | Unknown | 8233-E8B*061AA6P | 1011760206 | | Collection successful | Dec 8, 2010 8:56:38 AM | | 0.61 mb | /dump/41/ |
| <input type="checkbox"/> | 40.zip | Unknown | 8233-E8B*061AA6P | 1915318825 | | Collection successful | Dec 8, 2010 8:56:32 AM | | 0.59 mb | /dump/40/ |
| <input type="checkbox"/> | additional42.zip | Compressed Error Data | 8233-E8B*061AA6P | 709438025 | | Collection successful | Dec 8, 2010 8:56:40 AM | | 0.65 mb | /dump/42/ |
| <input type="checkbox"/> | SYSDUMP_061AB2P | SYSDUMP | 8233-E8B*061AB2P | | | Collection successful | Dec 8, 2010 8:45:56 PM | | 45.56 mb | /dump/ |
| <input type="checkbox"/> | additional56.zip | Compressed Error Data | 8233-E8B*061AA6P | 273027142 | | Collection successful | Dec 8, 2010 11:58:23 AM | | 1.91 mb | /dump/56/ |
| <input type="checkbox"/> | 55.zip | Unknown | 8233-E8B*061AA6P | 1110196780 | | Collection successful | Dec 8, 2010 11:50:06 AM | | 1.91 mb | /dump/55/ |
| <input type="checkbox"/> | 56.zip | Unknown | 8233-E8B*061AA6P | 273027142 | | Collection successful | Dec 8, 2010 11:58:23 AM | | 1.92 mb | /dump/56/ |
| <input type="checkbox"/> | additional40.zip | Compressed Error Data | 8233-E8B*061AA6P | 1915318825 | | Collection successful | Dec 8, 2010 8:56:32 AM | | 0.58 mb | /dump/40/ |
| <input type="checkbox"/> | 42.zip | Unknown | 8233-E8B*061AA6P | 709438025 | | Collection successful | Dec 8, 2010 8:56:40 AM | | 0.64 mb | /dump/42/ |

Page 1 of 1 1 Selected: 0 Total: 13 Filtered: 13

Using 0.04% of total cache (46.04 of 120948 mb)
Last Updated: December 9, 2010 11:09:21 AM EST
[Support Files settings](#)

Refresh

Figure 14-14 Manage Support Files system wide view

Monitored system support files view

The monitored system support files view can be reached by going to the Welcome page, clicking the **Resources** tab, right-clicking a selected host, and selecting **Service and Support** → **Support files** (Figure 14-15).

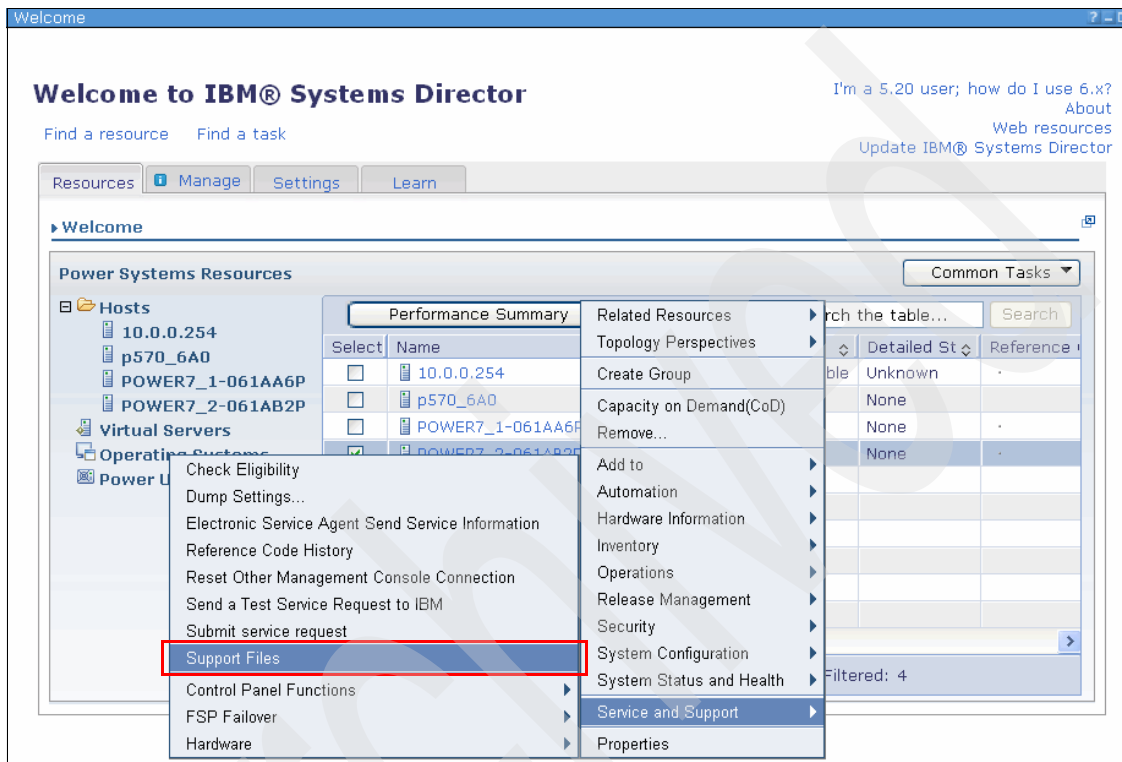


Figure 14-15 Support Files in the context menu of a host

The Manage Support Files page opens. This page shows only the support files of the selected host; otherwise, it is identical to the Manage Support Files system wide view (Figure 14-14 on page 353).

Serviceable problem support files view

The serviceable problem support files view can be reached over an active serviceable problem. If you select the Properties of a serviceable problem, you can find, on the Support Files tab, the serviceable problem support files view, which shows only the support files available for this problem (Figure 14-16).

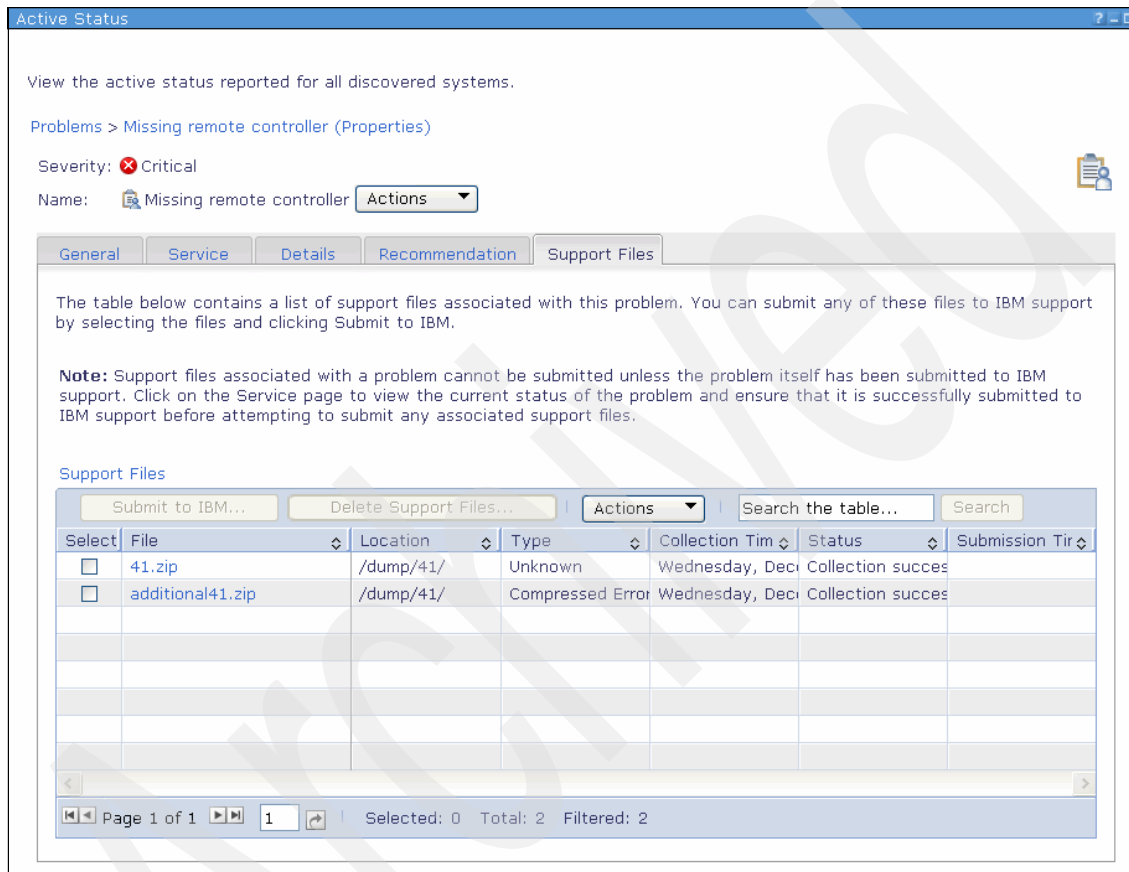


Figure 14-16 Serviceable Problem Support Files view

14.5.2 Support Files Management

On the Managed Support Files page (Figure 14-14 on page 353), you have the following options:

- ▶ Collecting new support files by clicking the **Collect Support Files...** button (not available on the serviceable problem support files view).

- ▶ Submit support files to IBM by clicking the **Submit to IBM...** button, or by using the **Action** drop-down menu.
- ▶ Delete support files by clicking the **Delete Support Files...** button, or by using the **Action** drop-down menu.
- ▶ Copy support files to media (USB) by using the **Action** drop-down menu.
- ▶ Show the properties of a support file by using the **Action** drop-down menu, or by clicking the support file itself.
- ▶ Specify general support files settings by clicking **Support Files settings** (not available on the serviceable problem support files view).

Collecting new support files (dump)

The collecting of new support files is a two step process:

1. You have to specify from which monitored system you want to collect the support files by selecting the system on the System tab of the Collect Support Files... page and adding it to the Selected site (Figure 14-17 on page 357).

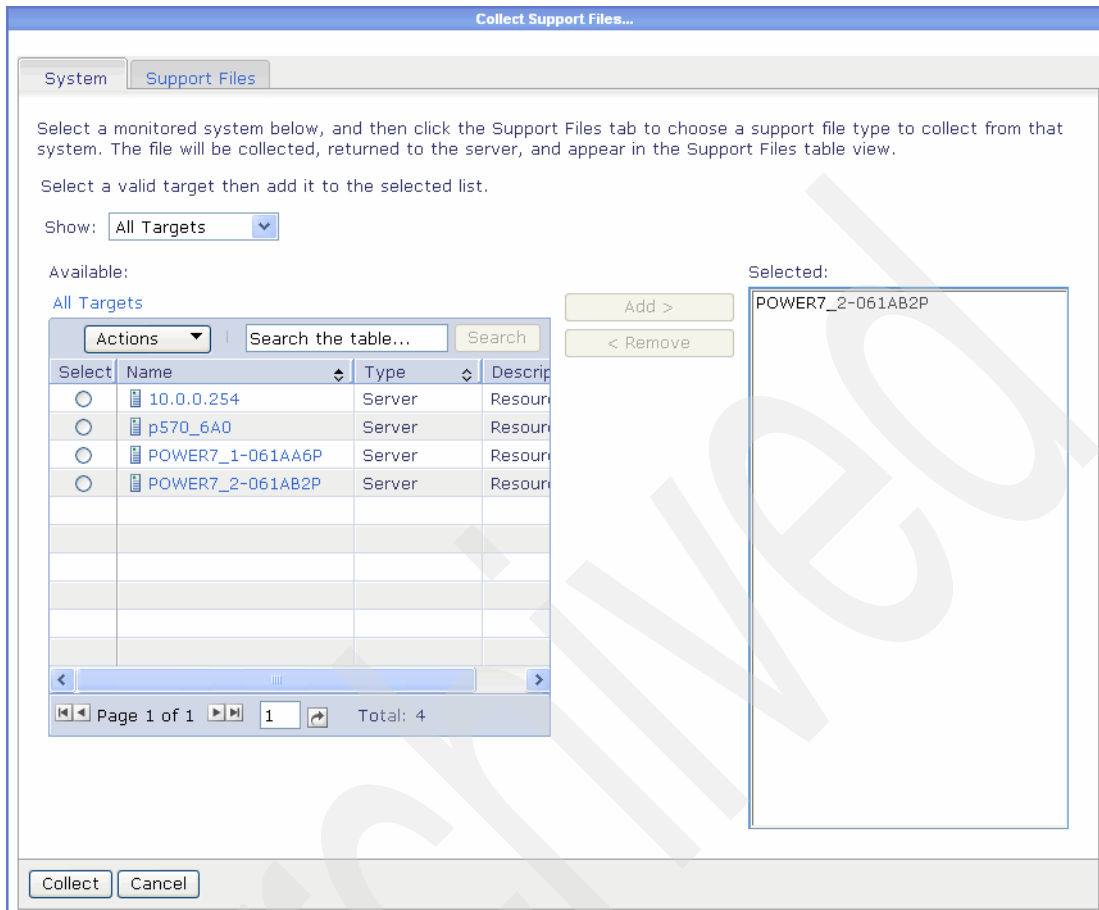


Figure 14-17 Collect Support Files page

You can only get support files from one system at a time. Specify the type of support file you want to collect on the Support Files tab of the Collect Support Files... page. Depending on the system selected, you have five kinds of support file types:

Resource dump

A resource dump is a nondisruptive dump that you can use to capture server firmware diagnostic data. You can perform a resource dump without needing to shut down the managed system or any of its Virtual Servers, and without needing to open a special service connection to the system to recover this data.

| | |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| System dump | A system dump is a dump of the hardware and server firmware content (platform) for the managed system. This task abnormally ends the managed system and all its Virtual Servers. |
| System controller dump | A system controller dump is a dump of the service processor. It should not cause any disruption to the managed system unless an unexpected error occurs. |
| Node controller dump | A node controller dump is a dump of the node controller. It should not cause any disruption to the managed system unless an unexpected error occurs. |
| Power dump | A power dump is a dump of the Power Unit (formerly bulk power controller) service processor. This task is available only for certain models of managed systems and should not cause any disruption to the managed system unless an unexpected error occurs. |

For some of the dumps, you can specify further option(s) to reduce the amount of dump data that will be collected.

- When you are finished with your selection, click the **Collect** button. The collection of the specified dump starts in the background and you return to the Manage Support Files page. The collection of the dump takes some time and you can refresh the Manage Support Files page by clicking the **Refresh** button to see the dump when the collection is finished.

Submitting support files to IBM

Extended error data files and other dump files that are shown on the Manage Support Files page can be transmitted to IBM, provided the required Service and Support Manager setup information has been entered using the Service and Support Manager setup wizard or by running the `smcli ssmimport` command.

The EED files collected automatically during serviceable event processing are transmitted to IBM as an attachment to the service request. For dump files that are not collected as part of the serviceable event processing (manually collected dump files), you can choose to send them either as an attachment to an existing service request or you can send them using the ecc StatusReport service provider.

Deleting support files

By manually deleting a support file, you are prompted if you really want to delete it; if you do, click **OK**.

There are two other tasks that can be used to remove support files

- ▶ The Service and Support Manager Support File Cleanup task. Support files that are transmitted successfully to IBM are deleted after a set time period (the default is 7 days).
- ▶ The support file space management task, which is invoked every time a dump is copied from the managed system onto the SDMC appliance. Support files are removed by the following algorithm when the new dump will cause the free space to be exceeded:
 - First, any support files associated with service requests that have been closed (oldest to newest) are removed.
 - Next, support files already transmitted to IBM (oldest to newest) are removed.
 - If additional space is still needed, any support files not yet transmitted (oldest to newest) are removed.

Copying support files to media

One or more support files can be copied to a USB device that exists on the SDMC appliance. If multiple USB devices are available on the SDMC appliance, you can select the USB device to use. A support file has to be less than 4 GB to be copied to a USB device.

Properties of support files

On the General tab of the properties page of a support file, you can view some information about a support file (Figure 14-18), such as:

- Location of the support file.
- Type of the support file.
- System from which the support file originated.
- Time the support file was collected.
- Time the support file was submitted to IBM.
- Size of the support file.

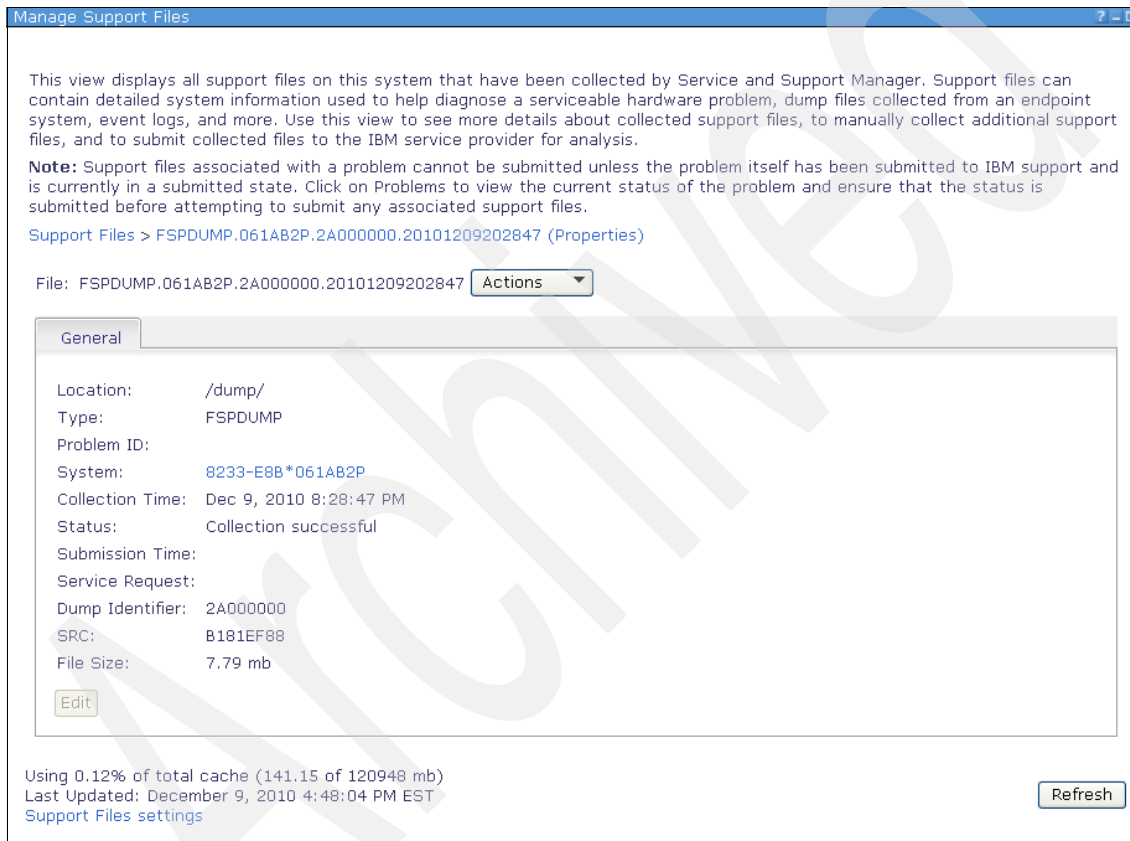


Figure 14-18 Properties of a support file

General support files settings

On the Support Files tab, you can view and set some general global settings for the support files:

- You can see the maximum size of the space for support files. You can modify this size only when the space does not occupy a whole partition.

- ▶ You can see the location where the support files are saved locally.
- ▶ You can see the free space left for the support files.
- ▶ You can see and modify the time period for when the submitted support files are automatically removed by the Service and Support Manager Support File Cleanup task. The time period can be set to:
 - Delete immediately
 - 1 Day
 - 7 Days (default)
 - 14 Days
 - 21 Days
 - 28 Days
- ▶ You can choose what happens with the deployed support file collectors on the system:
 - You can leave them on all systems (this is the default, and reduces bandwidth, but consumes space).
 - You can remove them on all systems.
 - You can customize on which systems they will be left and on which they will be removed.

Dump settings

For each host, you can specify individual dump policies by opening the **Welcome** page, clicking **Resource** tab, selecting the host, and selecting **Service and Support** → **Dump Settings...** On the Dump Settings page, you can set the following policies:

- ▶ Dump as needed
 - Enabled (by default)
- ▶ Hardware content
 - Automatic (by default)
 - Maximum
- ▶ Firmware content
 - Automatic (by default)
 - Maximum
 - Physical I/O
 - Virtual I/O
 - HPS Cluster
 - HCS I/O

14.6 Service and Support Manager command-line interface

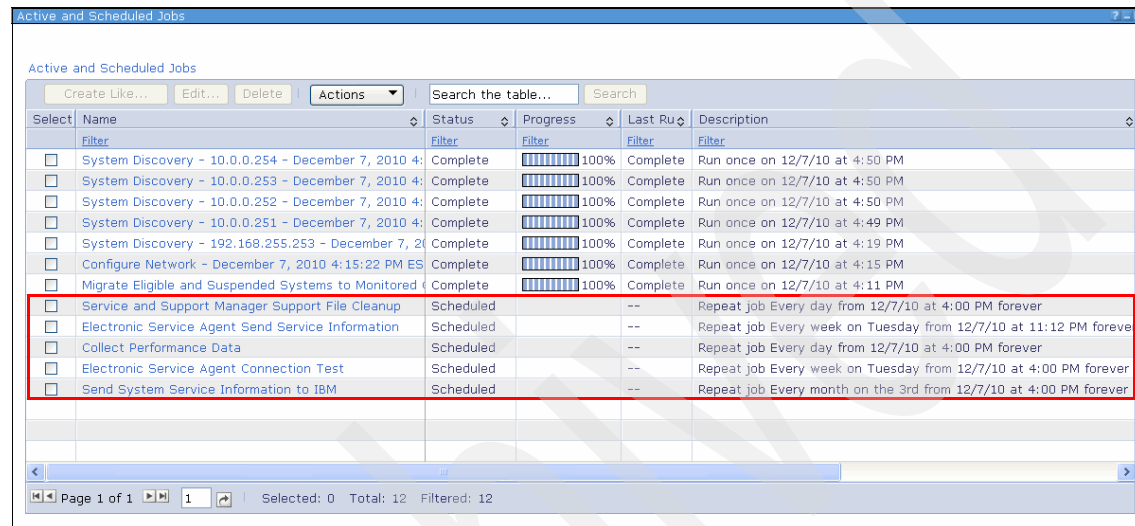
The Service and Support Manager (SSM) provides the following SDMC commands:

| | |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ssmimport | Used to provide the configuration information required by the Electronic Service Agent (ESA) to allow electronic service transactions to flow between the SDMC appliance and IBM. Provides the functional equivalence of running the Service and Support Manager Setup wizard. |
| lssvcproblem | Provides a listing of and detailed information about serviceable problems that are on the SDMC appliance. Provides the functional equivalence of the Director Problems view and setting the output to only show problems with a category of Service Status. |
| lssptfile | Provides a listing and detailed information about support files that are on the SDMC appliance. Provides the functional equivalence of selecting the support files view. |
| collectsptfile | Provides the ability to collect a support file from a managed system. Provides the functional equivalence of using the Collect Support Files option from the support files view. |
| submitsptfile | Provides the ability to transmit a support file to IBM. Provides the functional equivalence to using the Submit to IBM option in the support files view. |
| cpsptfile | Provides the ability to copy a support file to a removable media device (USB). Provides the functional equivalence of using the Copy to Media option in the support files view. |
| rmsptfile | Provides the ability to remove a support file from the support files view and delete the support file from the file system. Provides the functional equivalence to using the Delete Support Files option in the support files view. |

For additional options for the commands and examples of how to use them, refer to the man page for each command, or refer to “SSM commands” on page 375.

14.7 Service and Support Manager tasks

The Service and Support Manager (SSM) defines a number of tasks (scheduled jobs) that are performed on a periodic basis. That period depends on the specific task. You can see these task in the Active and Scheduled Jobs page (Figure 14-19).



| Select | Name | Status | Progress | Last Run | Description |
|--------------------------|----------------------------------------------------------|-----------|----------|----------|-------------------------------------------------------------------|
| <input type="checkbox"/> | System Discovery - 10.0.0.254 - December 7, 2010 4: | Complete | 100% | Complete | Run once on 12/7/10 at 4:50 PM |
| <input type="checkbox"/> | System Discovery - 10.0.0.253 - December 7, 2010 4: | Complete | 100% | Complete | Run once on 12/7/10 at 4:50 PM |
| <input type="checkbox"/> | System Discovery - 10.0.0.252 - December 7, 2010 4: | Complete | 100% | Complete | Run once on 12/7/10 at 4:50 PM |
| <input type="checkbox"/> | System Discovery - 10.0.0.251 - December 7, 2010 4: | Complete | 100% | Complete | Run once on 12/7/10 at 4:49 PM |
| <input type="checkbox"/> | System Discovery - 192.168.255.253 - December 7, 2010 4: | Complete | 100% | Complete | Run once on 12/7/10 at 4:19 PM |
| <input type="checkbox"/> | Configure Network - December 7, 2010 4:15:22 PM ES | Complete | 100% | Complete | Run once on 12/7/10 at 4:15 PM |
| <input type="checkbox"/> | Migrate Eligible and Suspended Systems to Monitored | Complete | 100% | Complete | Run once on 12/7/10 at 4:11 PM |
| <input type="checkbox"/> | Service and Support Manager Support File Cleanup | Scheduled | -- | -- | Repeat job Every day from 12/7/10 at 4:00 PM forever |
| <input type="checkbox"/> | Electronic Service Agent Send Service Information | Scheduled | -- | -- | Repeat job Every week on Tuesday from 12/7/10 at 11:12 PM forever |
| <input type="checkbox"/> | Collect Performance Data | Scheduled | -- | -- | Repeat job Every day from 12/7/10 at 4:00 PM forever |
| <input type="checkbox"/> | Electronic Service Agent Connection Test | Scheduled | -- | -- | Repeat job Every week on Tuesday from 12/7/10 at 4:00 PM forever |
| <input type="checkbox"/> | Send System Service Information to IBM | Scheduled | -- | -- | Repeat job Every month on the 3rd from 12/7/10 at 4:00 PM forever |

Figure 14-19 Tasks in Active and Schedule Jobs page

You cannot edit the tasks, but you can change the run times.

The tasks are:

- Service and Support Manager Support file cleanup

This task runs every day. It cleans up the support files. By default, all reports transmitted successfully to IBM are deleted after 7 days. Furthermore, if disk space falls below a certain percentage, the support files are deleted by this task.

- Electronic Agent Send Service information

This task runs once a week. It is called an *Inventory* task. The task harvests the appropriate inventory data from the Director database (hardware, software, and Capacity Upgrade on Demand data) on behalf of the Power Systems and Virtual Servers that it monitors (AIX and Linux). The actual collection of inventory is performed by IBM Systems Director Inventory component. On the first run, a complete inventory is sent. On all subsequent runs, only an incremental inventory (only things that have changed) is sent. The inventory data is stored in the eService database at IBM.

- ▶ Collect Performance Data

This task runs on a daily basis. It is performed for AIX partitions that have been configured and set up to collect performance measurements. The Service and Support Manager attempts to collect performance measurements data after a partition is discovered and unlocked. Performance measurement data is stored in the eService database at IBM.

- ▶ Electronic Service Agent Connection test

This task runs once a week. It is called a *Heartbeat* task. It generates an ECC report using the ECC status report service provider in which it conveys to IBM whether a given Power System is *online* or *offline*. It sends this information on behalf of the SDMC appliance itself and the monitored Power Systems. It does not send a heartbeat on behalf of other partitions or Power Units. The heartbeat information is stored in the eService database at IBM.

- ▶ Send System Service Information to IBM

This task runs once a month.

14.8 First Failure Data Capture

SDMC supports First Failure Data Capture (FFDC), which provides persistent records of failures and significant software incidents that occur during run time in SDMC. The FFDC feature runs in the background and collects events and errors that occur at run time. The feature provides a means for associating failures to one another, allowing software to link the effects of a failure to their causes, and thereby facilitate the quick location of the root cause of a failure. The data that is captured can be used to identify exception processing that occurred at the time of the failure.

On the HMC, the method for transmitting the FFDC information to IBM was to send a hardware service request on behalf of the machine type, model, and serial number of the HMC that would result in a PMH being created.

On the SDMC, the FFDC feature generates an event for each unique FFDC condition that occurs. The Service and Support Manager listens for these events and transmits the FFDC data created by the SDMC component generating the FFDC condition. The FFDC data is transmitted to IBM using the ECC Status Report Service Provider. The events are routed to ecurep and it triggers an email notification to the SDMC component owner. The transmission of FFDC event files are disabled by default. You can enable it from the Service and Support Manager Service Agent settings.

14.9 Guided Repair

You can perform Guided Repair procedures from the context menu of a managed system. Right-click a server and select **Service and Support**. The Guided Repair tasks are listed under two menus: Hardware and FSP Failover. Guided Repair is also referred to as Repair and Verify (R&V).

Here are the common Repair and Verify procedures:

Add or Remove FRU

Displays a list of Field Replaceable Units (FRUs) that can be added or removed from the managed system. Select the FRU that you want to add or remove and Guided Repair guides you through the procedure.

Add or Remove Enclosure

Displays a list of FRUs that can be added or removed from the managed system. Select the FRU that you want to add or remove and Guided Repair guides you through the procedure.

Open or Close MES

Displays a list of MES numbers. You can create a new MES number entry in the Order MES page. You can close or end a MES number by selecting and clicking **Next** in the Close MES page.

Exchange FRU

Displays a list of FRUs that can be exchanged with replacement FRUs. Select the FRUs to exchange and Guided Repair guides you through the procedure.

Setup FSP Failover

Enable or disable FSP failover on managed systems with more than one FSP.

Initiate FSP Failover

Fails over FSP control from the primary to secondary FSP.

Power On/Off Unit

You can power on or power off the unit or PCI slot from the displayed tree of I/O drawers.

Prepare for Hot Repair/Upgrade

Select the component using the location code of the system to be repaired. After selecting the component, SDMC provides a summary of required actions to be performed to isolate a particular hardware component as part of a service procedure.

Problem Repair

You can execute a repair from the Problem Information page, which guides you through the procedure to replace the FRUs. You can do some of the repairs concurrently.

List Running Power System Repairs (Resume Repair)

Displays a list of Guided Repair processes that are currently running on the SDMC. Click a process to continue it. Currently running processes are removed if the SDMC is restarted.

Identify LED

Displays a list of enclosures and FRUs. You can then activate/deactivate the LED on supporting FRUs and enclosures.

LED Lamp Test

Enables all LEDs on the managed system for a few minutes.

System Attention LED

Deactivates the System Attention LED.

14.9.1 Differences from HMC

SDMC does not have the ability to disconnect and resumes user sessions like HMC does. You can resume a Guided Repair function using the List Running Power System Repairs task. Click any one of the listed processes to resume that process.

You can also initiate a R&V process from the Recommendations tab of the Problem properties window. Click the **Problems** link at the top of the web interface and you should see a list of problems. Click any of the problems and you should see the Problem properties window. Click the **Recommendation** tab, and click the **Repair** button. The R&V process starts and exchanges FRUs to fix the problem.

Command-line reference

In this appendix, we list the IBM Systems Director Management Console (SDMC) commands with their options, new ones and old ones, that are not covered by the already existing documentation.

IBM Power Systems management commands

This section lists the Power Systems management commands (the ones in the psm-path) not covered by the IBM HMC Command-Line specification at the time of writing. The actual HMC Command-Line specification can be found at the following address:

<http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/resources.html>

For a full explanation of the command options, please see the man pages or use the `?`, `-h`, or `--help` options.

Table A-1 shows information about the **chtunecfg** command.

Table A-1 *chtunecfg* command

| Command | chtunecfg |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Definition | Performs operations on an SRIOV tuning buffer on a managed system. |
| Syntax | <pre>smcli chtunecfg -m <managed system> -r sriov --id <tuning buffer id> -o a l c [-f <file> -i <data>] [--help]</pre> |

Table A-2 shows information about the **impdata** command.

Table A-2 *impdata* command

| Command | impdata |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Definition | This command imports the HMC configuration into the SDMC. It is used in the HMC to SDMC transition. |
| Syntax | <pre>smcli impdata { -f <file> { -h <HMC hostnamelipaddress> -u <HMC user ID> [--passwd <HMC user password>]}}</pre> |
| Example | <pre>Importing the data from file: smcli impdata -f /tmp/hmcddata Importing the data from an HMC: smcli impdata -h hmcl.itso.ibm.com -u hscroot</pre> |

Table A-3 shows information about the **mk5250** command.

Table A-3 *mk5250 command*

| | |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command | mk5250 |
| Definition | Launches a 5250 console for an IBM i partition. This command launches an X Window System application, so it needs to be run locally or using an exported display. |
| Syntax | <pre>smcli mk5250 -m <managed system> -p <partition name> --id <partition ID> [--mode shared ded] [--env "<environment variables>"] [--help]</pre> |
| Example | <p>Launching a 5250 console:</p> <pre>smcli mk5250 -m p570_170 -p "IBM i"</pre> |

Table A-4 shows information about the **refdev** command.

Table A-4 *refdev command*

| | |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command | refdev |
| Definition | Refreshes the partition and profile data, which is used for remote restart of the partition, on the reserved storage device for the partition. |
| Syntax | <pre>smcli refdev [-m <managed system>] [-p <partition name> --id <partition ID>] [-w <wait time>] [-d <detail level>] [-v] [--help]</pre> |

Table A-5 shows information about the **rmdump** command.

Table A-5 *rmdump command*

| | |
|-------------------|-----------------------------------------------------------|
| Command | rmdump |
| Definition | Removes the specified dump file. |
| Syntax | <pre>smcli rmdump -f <dump filename> [--help]</pre> |

| | |
|----------------|-------------------------------------------------------------------------------------|
| Command | rmdump |
| Example | Removing a dump file: smcli rmdump -f FSPDUMP.100072A.01000019.20040629205455 |

IBM Systems Director application commands

This section lists the IBM Systems Director application commands (psm-path excluded) not covered by the IBM Systems Director Command-Line specification at the time of the writing of this book. The actual IBM Systems Director Command-Line specification can be found in the **IBM Systems Director V6.2.1 → Reference → Commands → smcli** section at the following address:

<http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp/>

For a full explanation of the command options, please see the man pages or use the `-?`, `-h`, or `--help` options.

Table A-6 is a list of the old IBM Systems Director commands that were replaced by newer IBM Systems Director application commands.

Table A-6 IBM Systems Director commands replaced

| Command | Replacement |
|------------|-------------|
| accessmo | accesssys |
| chmo | chsys |
| deploytmp1 | runtask |
| exporttmp1 | lscfgtmp1 |
| importtmp1 | mkcfgtmp1 |
| lsmo | lssys |
| lstmp1 | lscfgtmp1 |
| mkmo | discover |
| mktmp1 | mkcfgtmp1 |
| pingmo | pingsys |
| rmmo | rmsys |
| rmtmp1 | rmcfgtmp1 |

Event commands

This section lists the commands for event handling. To see the options of the commands in the event path, run the **list** command:

```
smcli event list
```

Table A-7 shows information about the **appleventactionplan** command.

Table A-7 *appleventactionplan* command

| | |
|-------------------|--------------------------------------------------------------------------------------------------------------------|
| Command | appleventactionplan |
| Definition | Assigns targets to an event action plan. |
| Syntax | smcli applyeventactionplan <PlanName> [-s system-oid(1)...system-oid(N)] [-g group-oid(1)...group-oid(N)] |

Table A-8 shows information about the **createeventactionplan** command.

Table A-8 *createeventactionplan* command

| | |
|-------------------|-----------------------------------------------------------------------------------------------|
| Command | createeventactionplan |
| Definition | Creates an event action plan. |
| Syntax | smcli createeventactionplan <PlanName> [-e filterName(1) ActionName(1)...ActionName(N)] |

Table A-9 shows information about the **listeventactionplans** command.

Table A-9 *listeventactionplans* commands

| | |
|-------------------|--------------------------------------------------------------------|
| Command | listeventactionplans |
| Definition | Lists the event action plans. |
| Syntax | smcli listeventactionsplans [-rl-reportl-tl-terse] |
| Example | To list the event action plans, run: smcli listeventactionplans |

Table A-10 shows information about the **listeventactions** command.

Table A-10 listeventactions command

| | |
|-------------------|-----------------------------------------------------------------------------------------|
| Command | listeventactions |
| Definition | Lists the event actions and the corresponding number. |
| Syntax | smcli listeventactions [-rl-reportl-tl-terse] |
| Example | To list the event actions and the corresponding numbers, run: smcli listeventactions |

Table A-11 shows information about the **listevents** command.

Table A-11 listevents command

| | |
|-------------------|----------------------------------------------------------------------------------------------------------------|
| Command | listevents |
| Definition | Lists events. |
| Syntax | smcli listevents [-rl-reportl-tl-terse] [-e filterName] [-h hours] [system-oid(1)...system-oid(N)] |
| Example | To get a listing of all events, run: smcli listevents |

Table A-12 shows information about the **listeventtypes** command.

Table A-12 listeventtypes command

| | |
|-------------------|-------------------------------------------------------------------|
| Command | listeventtypes |
| Definition | Lists all the event types. |
| Syntax | smcli listeventtypes |
| Example | To get a listing of all event types, run: smcli listeventtypes |

Table A-13 shows information about the **listfilters** command.

Table A-13 *listfilters* command

| | |
|-------------------|---------------------------------------------------------|
| Command | listfilters |
| Definition | Lists all event filters. |
| Syntax | smcli listfilters [-rl-report -tl-terse] |
| Example | To get a list of all filters, run: smcli listfilters |

Scheduler commands

In this section, we list the commands for the scheduler handling. To see the options of the commands in the scheduler path, run the **list** command:

```
smcli scheduler list
```

Table A-14 shows information about the **canceljobactivation** command.

Table A-14 *canceljobactivation* command

| | |
|-------------------|--------------------------------------------------------|
| Command | canceljobactivation |
| Definition | Cancels a scheduled job. |
| Syntax | smcli canceljobactivation <JobID> <ActivationID> |

Table A-15 shows information about the **getjobactivationlog** command.

Table A-15 *getjobactivationlog* command

| | |
|-------------------|-------------------------------------------------------------------------------------------------------|
| Command | getjobactivationlog |
| Definition | Lists the job activation logs. |
| Syntax | smcli getjobactivationlog <JobID> <ActivationID> [Managed-Object ID] |
| Example | To get the first page of the activation log for job number 70, run: smcli getjobactivationlog 70 1 |

Table A-16 shows information about the **getjobstatus** command.

Table A-16 *getjobstatus* command

| | |
|-------------------|-------------------------------------------------------------------|
| Command | getjobstatus |
| Definition | Lists the status of a specified job. |
| Syntax | smcli getjobstatus <JobID> |
| Example | To get the status of job number 70, run: smcli getjobstatus 70 |

Table A-17 shows information about the **listjobactivations** command.

Table A-17 *listjobactivations* command

| | |
|-------------------|----------------------------------------------------------------------------------|
| Command | listjobactivations |
| Definition | List the times a specific job was executed. |
| Syntax | smcli listjobactivations <JobID> [Managed-Object ID] |
| Example | To list the times job number 70 was executed, run: smcli listjobactivation 70 |

Table A-18 shows information about the **listjobactivationssystem** command.

Table A-18 *listjobactivationssystem* command

| | |
|-------------------|-----------------------------------------------------------|
| Command | listjobactivationssystem |
| Definition | List the times jobs where executed for a specific system. |
| Syntax | smcli listjobactivationssystem <Managed-Object ID> |

Table A-19 shows information about the **listjobs** command.

Table A-19 *listjobs* command

| | |
|-------------------|-----------------------------------|
| Command | listjobs |
| Definition | Lists all jobs and their numbers. |
| Syntax | smcli listjobs |

| | |
|----------------|------------------------------------------------------|
| Command | listjobs |
| Example | To get a listing of all jobs, run: smcli listjobs |

SSM commands

In this section, we list the commands for the Service and Support Manager (SSM).

Table A-20 shows information about the **chkssmconfig** command.

Table A-20 *chkssmconfig* command

| | |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Command | chkssmconfig |
| Definition | Verifies whether the Service and Support Manager is configured. |
| Syntax | smcli chkssmconfig {-h -? -- help} [-L <i>language</i>] |
| Example | To verify whether Service and Support Manager is already configured with the required information, run: smcli chkssmconfig |

Table A-21 shows information about the **collectsptfile** command.

Table A-21 *collectsptfile* command

| | |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command | collectsptfile |
| Definition | Collects support files from a specified system and copies them to the management server. |
| Syntax | smcli collectsptfile {-h -? -- help} [-L <i>language</i>] [-v] {-t <i>support_file_type</i> } [-s <i>specifier</i>] [-C] {-i <i>ip_address_hostname</i> -n <i>managed_system</i> -m <i>machineserial_model_type</i> } |

| | |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command | collectsptfile |
| Example | <p>This example illustrates how to collect a DSA support file from a system with an IP address of 8.10.115.37:</p> <pre>smcli collectsptfile -i 8.10.115.37 -t dsa</pre> <p>This example illustrates how to collect IBM Power Systems subsystem support files from a side A of a system with a machine type of 9406, a model number of 570, and a serial number of 1234567:</p> <pre>smcli collectsptfile -m 9406-570*1234567 -t psd -s a</pre> |

Table A-22 shows information about the **cpsptfile** command.

Table A-22 *cpsptfile* command

| | |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command | cpsptfile |
| Definition | Copies one or more support files to a media device on the management server. |
| Syntax | <pre>smcli cpsptfile {-h -? -- help} [-L language] [-v] {-F file_list} {-t target_location}</pre> |
| Example | <p>This example illustrates how to copy a single support file to the USB flash drive. In this case, the specified support file is a flexible service processor dump.</p> <pre>smcli cpsptfile -F /dump/9119.FHA.02FD881.problem.NOPROB.pmh.NOPMH.FS PDUMP.opt.ccfw.da-ta.p.sa.FSPDUMP.02FD881.18000000 .20090602065452.gz -t /dev/sda</pre> |

Table A-23 shows information about the **lssptfile** command.

Table A-23 *lssptfile* command

| Command | lssptfile |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Definition | Displays a list of support files located on the management server. |
| Syntax | <pre>smcli lssptfile {-h -? -- help} [-L <i>language</i>] [-v] [-p <i>serviceable_problem_number</i> -r <i>service_request</i>] {-i <i>ip_address_hostname</i> -n <i>managed_system</i> -m <i>machineserial_model_type</i> [-A <i>attribute_list</i>]}</pre> |
| Example | <p>This example illustrates how to list all the support files on the management server:</p> <pre>smcli lssptfile</pre> <p>This example illustrates how to display a list of all support files on the management server for the managed system with a machine type of 9406, a model number of 570, and a serial number of 12345678:</p> <pre>smcli lssptfile -m 9406-570*12345678</pre> <p>This example illustrates how to display a list of support files on the management server associated with the local serviceable problem number 1498:</p> <pre>smcli lssptfile -p 1498</pre> <p>This example illustrates how to display a list of support files on the management server associated with service request number 61999,933,000:</p> <pre>smcli lssptfile -r 61999,933,000</pre> |

Table A-24 shows information about the **lssvcproblem** command.

Table A-24 *lssvcproblem* command

| Command | lssvcproblem |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Definition | Displays a list of serviceable problems on the management server. |
| Syntax | <pre>smcli lssvcproblem {-h -? -- help} [-L <i>language</i>] [-v] [-P <i>query</i>] [-i <i>ip_address_hostname</i> -n <i>managed_system</i> -m <i>machineserial_model_type</i>] [-d <i>symbol</i>] [-A <i>attribute_list</i>]</pre> |
| Example | <p>This example illustrates how to display a list of all serviceable problems on the management server:</p> <pre>smcli lssvcproblem</pre> <p>This example illustrates how to display a list of all of the serviceable problems on the management server for the managed system with a machine type of 9406, model number of 570, and serial number of 12345678:</p> <pre>smcli lssvcproblem -m 9406-570*12345678</pre> <p>This example illustrates how to display a list of serviceable problems that have service requests in an open state:</p> <pre>smcli lssvcproblem -P "ServiceRequestStatusEnum=1"</pre> |

Table A-25 shows information about the **rmsptfile** command.

Table A-25 *rmsptfile* command

| Command | rmsptfile |
|-------------------|------------------------------------------------------------------------------------------------|
| Definition | Removes one or more support files from the managed server. |
| Syntax | <pre>smcli rmsptfile {-h -? -- help} [-L <i>language</i>] [-v] {-F <i>file_list</i>}</pre> |

| | |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command | rmsptfile |
| Example | <p>This example illustrates how to remove a single support file from the management server. In this case, the specified support file is a flexible service processor dump:</p> <pre>smcli rmsptfile -F /dump/9119.FHA.02FD881.problem.NOPROB.pmh.NOPMH.FS PDUMP.opt.ccfw.da-ta.p.sa.FSPDUMP.02FD881.18000000 .20090602065452.gz</pre> <p>This example illustrates how to remove two support files from the management server. In this case, the specified files are Dynamic Systems Analysis (DSA) support files:</p> <pre>smcli rmsptfile -F /dump/7979AC1_23D0600_20090320-191612.xml.gz, /dump/7976AC2_9170300_20090427-181459.xml.gz</pre> |

Table A-26 shows information about the **ssmimport** command.

Table A-26 *ssmimport* command

| | |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command | ssmimport |
| Definition | Imports initial configuration data into the Service and Support Manager. |
| Syntax | <pre>smcli ssmimport {-h -? -- help} [-L <i>language</i>] -f "<i>filename</i>" [-c] [-v]</pre> |
| Example | <p>This example illustrates how to import the configuration file:</p> <pre>smcli ssmimport -f "C:/home/config.properties"</pre> <p>This example illustrates how to validate the configuration parameters to ensure that everything is ready to import, but it will not actually import the configuration file:</p> <pre>smcli ssmimport -f "C:/home/config.properties" -v</pre> |

Table A-27 shows information about the **submitsptfile** command.

Table A-27 *submitsptfile* command

| | |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command | submitsptfile |
| Definition | Sends a support file on the management server to the service provider. |
| Syntax | smcli submitsptfile {-h -? -- help} [-L <i>language</i>] [-v] {-F <i>file_name</i> } [-r <i>service_request</i>] |
| Example | <p>This example illustrates how to send a service processor support file to the service provider. In this case, the specified support file is a flexible service processor dump. The support file is not associated with a service request.</p> <pre>smcli submitsptfile -F /dump/9119.FHA.02FD881.problem.NOPROB.pmh.NOPMH.FS PDUMP.opt.ccfw.da-ta.p.sa.FSPDUMP.02FD881.18000000 .20090602065452.gz</pre> <p>This example illustrates how to send a Dynamic Systems Analysis (DSA) support file to the service provider and associate it with a service request. In this case, the service request is identified as USEOCSUTWUL.</p> <pre>smcli submitsptfile -F 7979AC1_23D0600_20090320-191612.xml.gz -r USEOCSUTWUL</pre> |

High availability commands

In this section, we list the commands for high availability handling. Be aware that there are more high availability commands in the IBM Director appliance section (see Table 10-1 on page 277).

Table A-28 shows information about the **configureHA** command.

Table A-28 *configureHA* command

| | |
|------------|----------------------------------------------|
| Command | configureHA |
| Definition | Configures nodes for high availability (HA). |

| Command | configureHA |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Syntax | <pre>smcli configureHA --secondary-node <i>secNode</i> --password <i>thePassword</i> --primary-rep-addr <i>primRepAddr</i> --secondary-rep-addr <i>secRepAddr</i> --floating-addr "<i>addr1,subnet1,netlfc1 [...</i> <i>addrN,subnetN,netlfcN</i>]" [--time-server <i>timeServer</i> --use-primary-as-time-server] [--force-time-sync] [--agent-mgr-addr <i>agtMgrAddr</i>] [-v] [--tiebreaker-addr <i>tieAddr</i>]</pre> |

| Command | configureHA |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Example | <p>This example illustrates how to configure high availability using only the required options. In this example, the primary node already has a time server configured.</p> <pre>smcli configureHA --secondary-node node2 --password abcdefgh --primary-rep-addr 10.6.6.100 --secondary-rep-addr 10.6.6.101 --floating-addr "10.6.6.200,255.255.0.0,eth0"</pre> <p>This example illustrates how to configure high availability with two floating IP addresses and other options:</p> <pre>smcli configureHA --secondary-node node2 --password abcdefgh --primary-rep-addr 10.6.6.100 --secondary-rep-addr 10.6.6.101 --floating-addr "10.6.6.200,255.255.0.0,eth0 192.168.6.200,255.255.255.0,eth1" --agent-mgr-addr 10.6.6.200 --use-primary-as-time-server --force-time-sync</pre> <p>This example illustrates how to configure high availability with all other options:</p> <pre>smcli configureHA --secondary-node node2 --password abcdefgh --primary-rep-addr 10.6.6.100 --secondary-rep-addr 10.6.6.101 --tiebreaker-addr 10.6.6.1 --floating-addr "10.6.6.200,255.255.0.0,eth0 192.168.6.200,255.255.255.0,eth1" --agent-mgr-addr 10.6.6.200 --time-server time.yourcompany.com --force-time-sync</pre> |

Table A-29 shows information about the **failover** command.

Table A-29 failover command

| Command | failover |
|------------|-------------------------------------------------------------------------------|
| Definition | Starts a failover to the passive node in a high available (HA) configuration. |

| | |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command | failover |
| Syntax | smcli failover [-v -r] |
| Example | <p>This example illustrates how to start a failover to the passive node:</p> <pre>smcli failover</pre> <p>This example illustrates how to start a failover to the passive node and return from the command as soon as the failover task is created:</p> <pre>smcli failover -r</pre> |

Table A-30 shows information about the **removeHA** command.

Table A-30 *removeHA* command

| | |
|-------------------|-----------------------------------------------------------------------------------------------------------|
| Command | removeHA |
| Definition | Removes the high availability (HA) configuration from the active node and the corresponding passive node. |
| Syntax | smcli removeHA |
| Example | To remove high availability from both nodes, run: smcli removeHA |

User commands

In this section, we list the commands for user handling.

Table A-31 shows information about the **mkuser** command.

Table A-31 *mkuser* command

| | |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command | mkuser |
| Definition | Creates a user. |
| Syntax | smcli mkuser -u name [-p <i>password</i>] [-g <i>groups</i>] [-d " <i>description</i> "] [-x <i>key=value[,key=value...]</i>] [-h] |

| | |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Command | mkuser |
| Example | <p>This example illustrates how to create a user named "user1". In this example, the user password must be entered when you are prompted.</p> <pre>smcli mkuser -u user1</pre> <p>This example illustrates how to create a user named "user2" with the provided password. The expiration is set to 90 days, and the SSH timeout to 10 minutes. The new user will belong to the IBM Systems Director group smadmin.</p> <pre>smcli mkuser -u user2 -g smadmin -p password -d "User 2" -x expire=90,timeout=600</pre> <p>This example illustrates how to create a remotely authenticated LDAP user named "user3":</p> <pre>smcli mkuser -u user3 -x usertype=ldap</pre> <p>This example illustrates how to create a remotely authenticated Kerberos user named "user4". The new user will belong to the IBM Systems Director group smadmin.</p> <pre>smcli mkuser -u user4 -g smadmin -d "User 4" -x usertype=kerberos</pre> |

Table A-32 shows information about the **rmuser** command.

Table A-32 *rmuser* command

| | |
|-------------------|----------------------------------------------------------------------------------------------------|
| Command | rmuser |
| Definition | Deletes a user. |
| Syntax | <pre>smcli rmuser -u name [-h]</pre> |
| Example | <p>This example illustrates how to delete user named "user1":</p> <pre>smcli rmuser -u user1</pre> |

Other commands

In this section, we list commands not listed in the previous sections.

Table A-33 shows information about the **enablehierachicalmgmt** command.

Table A-33 *enablehierachicalmgmt* command

| | |
|-------------------|-----------------------------------------------------------------------------------------------|
| Command | enablehierachicalmgmt |
| Definition | Enables IBM Director for hierachical management. |
| Syntax | smcli enablehierachicalmgmt [-h -? --help] [-L <i>language</i>] |
| Example | To enable hierarchical management on the Director Server, run: smcli enablehierachicalmgmt |

Table A-34 shows information about the **isglobalserver** command.

Table A-34 *isglobalserver* command

| | |
|-------------------|---------------------------------------------------------------------------------------------|
| Command | isglobalserver |
| Definition | Shows whether the IBM Director Server can act as a global server. |
| Syntax | smcli isglobalserver [-h -? --help] [-L <i>language</i>] |
| Example | To verify if the IBM Director Server can act as global server, run: smcli isglobalserver |

Table A-35 shows information about the **licensestatus** command.

Table A-35 *licensestatus* command

| | |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Command | licensestatus |
| Definition | Displays the license status. |
| Syntax | smcli licensestatus [-v] {-p --product <i>productid</i> } {-s --feature <i>feature</i> } {-c --component <i>component</i> } |
| Example | To get the license status of all registered products, run: smcli licensestatus |

Table A-36 shows information about the **printInformation** command.

Table A-36 *printInformation* command

| | |
|-------------------|-------------------------|
| Command | printInformation |
| Definition | N/A |

Table A-37 shows information about the **simffdc** command.

Table A-37 *simffdc* command

| | |
|-------------------|----------------|
| Command | simffdc |
| Definition | N/A |

Table A-38 shows information about the **ssh_for_dsh** command.

Table A-38 *ssh_for_dsh* command

| | |
|-------------------|--------------------|
| Command | ssh_for_dsh |
| Definition | N/A |

Table A-39 shows information about the **startdiscovery** command.

Table A-39 *startdiscovery* command

| | |
|------------|----------------------------------------|
| Command | startdiscovery |
| Definition | Starts a discovery of SNMP devices. |
| Syntax | smcli startdiscovery [network mask] |

Table A-40 shows information about the **updatelicense** command.

Table A-40 *updatelicense* command

| | |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Command | updatelicense |
| Definition | Updates the licenses. |
| Syntax | smcli updatelicense [-v] {-p --product <i>productid</i> } {-s --feature <i>feature</i> } {-c --component <i>component</i> } |

Archived



IBM Systems Director base functions

In this appendix, we discuss the IBM Systems Director base functions.

Base functions

Base functions (plug-ins) in IBM Systems Director provide core functions to manage the full life cycle of IBM servers, storage, network, and Virtual Servers. Plug-ins that provide advanced functions or functions tailored to a particular environment can be downloaded and installed on top of IBM Systems Director.

The base functions include:

- ▶ Finding and viewing resources and resource information, including relationships and properties.
- ▶ Organizing logical sets of resources into groups.
- ▶ Starting, stopping, and scheduling tasks.
- ▶ Integrating third-party management software and other programs into the IBM Systems Director web interface.
- ▶ Managing auditing.
- ▶ Encrypting interprocess communication.
- ▶ Managing Common Agent registration and authentication.
- ▶ Authenticating users through a configured user registry available from the operating system, Lightweight Directory Access Protocol (LDAP), or domain controller.
- ▶ Creating roles and authorizing users and user groups to access certain systems, groups, and tasks.
- ▶ Managing credentials to support single sign-on authentication, even when services span different systems.

Here are some of the managers that are part of the IBM Systems Director that are available in the IBM Systems Director Management Console (SDMC):

Discovery Manager

The Discovery Manager performs physical and virtual system discovery and inventory of related resources on the network.

Status Manager

The Status Manager provides an at-a-glance view of the health of your managed resources (including systems, operating systems, applications, and security) and processes.

Configuration Manager

The Configuration Manager is used to integrate new hardware into your environment, configure systems after installation, or do one-off configurations for problem resolution. The configuration manager uses a set of well defined templates that can be applied to servers, storage, and network resources even if the resources are composed of very different technologies.

Automation Manager

The Automation Manager provides tools to notify an administrator or run a predefined tasks automatically when a certain event occurs.

Update Manager

The Update Manager provides tools for maintaining current versions of operating systems, device drivers, firmware and BIOS, and IBM Systems Director agent and server code on managed systems without an upgrade or migration of the installed product.

Remote Access Manager

The Remote Access Manager provides tools that support running and monitoring applications and services running on remote systems.

Virtualization Manager

The Virtualization Manager provides tools for managing the life cycle of virtual resources.

Network Management

Network Management provides management functions for network devices, including discovery, inventory, health and status monitoring, and configuration.

IBM BladeCenter and System x management

IBM BladeCenter and System x management provides life cycle management of your modular IBM System x and BladeCenter systems and related resources, including discovery, health and status monitoring, configuration, updates, and virtualization. It also provides platform-specific functions.

IBM System z® management

IBM System z management provides the capability to discover System z hosted Virtual Servers, and to access status information about them.

IBM Power Systems management

IBM Power Systems management provides life cycle management of your IBM Power Systems, and platform managers, such as Hardware Management Console (HMC) and Integrated Virtualization Manager (IVM) platform managers, including discovery, health and status monitoring, configuration, updates, and virtualization. It also provides platform-specific functions.

IBM System Storage management

IBM System Storage management provides life cycle management of your physical and virtual storage systems, including discovery, health and status monitoring, configuration, updates, and virtualization. It also provides platform-specific functions.

Additional IBM Systems Director plug-ins

Additional IBM Systems Director plug-ins can be downloaded and installed on top of IBM Systems Director to provide advanced functions or functions tailored to a particular environment.

IBM Systems Director Management Console distribution details

In this appendix, we give detailed information about the IBM Systems Director Management Console (SDMC) disk images.

IBM Systems Director Management Console virtual disk images

Table C-1 shows the virtual image used for SDMC. It is composed of seven virtual disks.

Table C-1 Seven virtual disk images for SDMC

| Location on RHEV-H Blue | Virtual disk name | Size | Guest device file | Description |
|-------------------------|-------------------|--------|-------------------|-------------------------|
| HostVGData | dvmdisk1.img | 50 MB | /dev/hda | Boot disk |
| HostVGData | dmvdisk2.img | 60 GB | /dev/vda | OS/Application disk |
| HostVGData | dvmdisk3.img | 80 GB | /dev/vdb | Database disk |
| AppVGData | dmvdisk4.img | 40 GB | /dev/vdc | Update repository |
| AppVGData | dmvdisk5.img | 120 GB | /dev/vdd | Dump space |
| AppVGData | dvmdisk6.img | 60 GB | /dev/vde | Spare disk for OS/App |
| AppVGData | dvmdisk7.img | 80 GB | /dev/vdf | Spare disk for Database |

Abbreviations and acronyms

| | | | |
|--------------|---------------------------------------------|-------------|----------------------------------------------|
| AME | Active Memory Expansion | ITSO | International Technical Support Organization |
| AMM | Advanced Management Module | IVM | Integrated Virtualization Manager |
| AMS | Active Memory Sharing | KVM | keyboard/video/mouse |
| ASM | Advanced System Management | LDAP | Lightweight Directory Access Protocol |
| ASMI | Advanced System Management Interface | LIC | Licensed Internal Code |
| BPA | Bulk Power Assembly | LPAR | Logical Partition |
| BPC | Bulk Power Controllers | LV | Logical Volume |
| CAS | Common Agent Service | LVM | Logical Volume Manager |
| CCFW | Common Console Framework | NIC | Network Interface Card |
| CIM | Common Information Model | NTP | Network Time Protocol |
| CLI | Command-Line Interface | OVA | Open Virtualization Archive |
| CoD | Capacity on Demand | OVF | Open Virtualization File |
| DHCP | Dynamic Host Configuration Protocol | PE | Product Engineer |
| DLPAR | Dynamic Logical Partitioning | PMH | Problem Management Record Hardware |
| DNS | Domain Name Services | PSM | Power Systems Manager |
| DRBD | Distributed Replicated Block Device | RBAC | Role-Based Access Control |
| DSA | Dynamic Systems Analysis | REST | Representational State Transfer |
| ESA | Electronic Service Agent | RHEL | Red Hat Enterprise Linux |
| FFDC | First Failure Data Capture | RIO | Remote I/O |
| FRU | Field Replaceable Unit | RMC | Remote Monitoring and Control |
| FSP | Flexible Service Processor | RSAP | Remote Service Access Points |
| FTP | File Transfer Protocol | SAN | Storage Area Network |
| GUI | Graphical User Interface | SDMC | IBM Systems Director Management Console |
| HA | High Availability | SFTP | Secure FTP |
| HMC | Hardware Management Console | SLP | Service Location Protocol |
| IBM | International Business Machines Corporation | | |
| IPL | Initial Program Load | | |

| | |
|-------------|---------------------------------|
| SMS | Systems Management Services |
| SPCN | System Power Control Network |
| SSH | Secure Shell |
| SSM | Service and Support Manager |
| SWMA | Software Maintenance |
| VLAN | Virtual LAN |
| VMC | Virtual Management Channel |
| VPD | Vital Product Data |
| VPN | Virtual Private Network |

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

The following IBM Redbooks publications provide additional information about the topic in this document. Note that some publications referenced in this list might be available in softcopy only.

- ▶ *Advanced POWER Virtualization on IBM System p Virtual I/O Server Deployment Examples*, REDP-4224
- ▶ *Hardware Management Console V7 Handbook*, SG24-7491
- ▶ *IBM PowerVM Live Partition Mobility*, SG24-7460
- ▶ *IBM PowerVM Virtualization Managing and Monitoring*, SG24-7590
- ▶ *IBM System p Advanced POWER Virtualization (PowerVM) Best Practices*, REDP-4194
- ▶ *Implementing IBM Systems Director 6.1*, SG24-7694
- ▶ *Integrated Virtualization Manager on IBM System p5*, REDP-4061
- ▶ *PowerVM Virtualization Active Memory Sharing*, REDP-4470
- ▶ *PowerVM Virtualization on IBM System p: Introduction and Configuration Fourth Edition*, SG24-7940

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks publications, at this website:

ibm.com/support

Online resources

These websites are also relevant as further information sources:

- ▶ HMC Commandline
<http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/resources.html>

- ▶ IBM Fix Central
<http://www.ibm.com/support/fixcentral/>
- ▶ IBM Systems Director 6.2 Information Center
<http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp/>
- ▶ IBM Systems Director home page
<http://www.ibm.com/systems/management/director/>
- ▶ KVM Installation Document
<http://publib.boulder.ibm.com/infocenter/lxinfo/v3r0m0/index.jsp?topic=/lxaai/kvminstall/lxaaikvminstallstart.htm>
- ▶ Linux-KVM
<http://www.linux-kvm.org/>
- ▶ Network bridging for the virtualization API libvirt
http://wiki.libvirt.org/page/Networking#Creating_network_initscripts
- ▶ Red Hat
<http://www.redhat.com/>
- ▶ VMWare OVF Tool
<http://communities.vmware.com/community/vmtn/vsphere/automationtools/ovf>

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

Numerics

7042-CR6 16–17

A

accesssys command 82
activate Virtual Server 152
Active and Schedule Jobs task 294
Active Energy Manager 91
Active Memory Expansion (AME) 165
Active Memory Sharing (AMS) 45
active/passive 300
Add Fibre Channel menu 174
Add or Remove Enclosure 365
Add or Remove FRU 365
advanced functions, CoD 96
Advanced Management Module (AMM) 81
Advanced System Management Interface (ASMI)
43
 accessing through command line 329
 accessing through SDMC 326
 menu 329
Advanced Virtual Ethernet Configuration 168
Agent Manager 34
agent manager 300
Agent Manager Configuration menu 302
Agent Manager IP Address page 319
AME See *Active Memory Expansion*
AMM See *Advanced Management Module*
AMS See *Active Memory Sharing*
Apache MQ 303
ASMI See *Advanced System Management Interface*
Assign Role wizard 220
assigning a role to a user 218
audit logs 269
auto discovery 82
Automation Manager 297, 391

B

backup and restore 12, 253
 KVM 261
 VMware 256
Blade Servers 2

BladeCenter 81, 391
BPA See *Bulk Power Assembly*
Bulk Power Assembly (BPA) 10, 99
 status 46, 102

C

Call Home 343
call home 343
capacity on demand 43
Capacity on Demand (CoD) 43, 94
 operations 97
cfgkrb command 232
cfgldap command 227
chnetcfg command 83, 252
chsyscfg command 171
chsysstate command 156
chuser command 239
CIM RSAP 80
CLI See *command-line interface*
Close MES 365
closure of serviceable events 350
CoD Capable 94
CoD See *Capacity on Demand*
collect utilization data 44
collectsptfile command 362
command
 pedbg 269
 pesh 270
command-line interface (CLI) 11
commands
 accesssys 82
 cfgkrb 232
 cfgldap 227
 chnetcfg 83, 252
 chsyscfg 171
 chsysstate 156
 chuser 239
 collectsptfile 362
 confighms 92
 configureHA 321
 cpsptfile 362
 discover 82
 expdata 68, 71

- failover 321
- impdata 68, 282
- lsbundle 278
- lsldap 228
- lsled 59
- lsnetcfg 252
- lsperm 209
- lsrole 205, 210
- lssptfile 362
- lssvcproblem 362
- lssys 85
- lssyscfg 59
- lsuser 201, 226
- lsusergp 203
- mk5250 282
- mksyscfg 152
- mkuser 226, 231, 236
- rediscover 83
- removeHA 321
- rmrole 210
- rmsptfile 362
- rmuser 240
- smha 321
- smhastatus 320–321
- ssmimport 362
- submitsptfile 362
- common agent 34
- Common Agent Services 300, 310, 319
- confighms command 92
- Configuration Manager 391
- Configure Access page 80
- Configure Single Sign On 93
- configureHA command 321
- content area 51
- context menu for Virtual Server 55
- context menu of server 53
- cpsptfile command 362
- create a role 206
- Create Adapter 141
- Create Group 212
- Create Role 206
- Create Server Profile 189
- Create Virtual Disk 145
- creating a group 212
- creating a user 223
- creating a Virtual Server 44, 132
- Current Configuration 182

D

- date and time 46
- DefaultProfile 154
- deleting a role 210
- deleting a user 240
- DHCP 240, 311
 - configuration 244
- Director
 - appliance commands 276
 - application commands 278
 - states 10
- discover command 82
- Discovered Manageable Systems table 77
- Discovery Manager 390
- Distributed Replicated Block Device 303
- DNS, setting 249
- domain server 91
- domain.xml 25
- dump 48, 351
 - dump settings 360–361
 - node controller dump 358
 - power dump 358
 - resource dump 357
 - system controller dump 358
 - system dump 358
- duplicate events 347

E

- edit host 43, 86
- EED See *Extended Error Data*
- Electronic Service Agent 336
- enhanced virtualization management 11
- Enter Activation Code 96
- Enter CoD Code 96
- event commands 371
- exchange FRU 365
- expdata command 68, 71
- Extended Error Data (EED) 347
- Extended Management 84

F

- failover command 321
- FFDC See *First Failure Data Capture*
- Fibre Channel 172
 - disks 144
- Field Replaceable Unit (FRU) 365
- file management 48
- firewall 240

- configuration 246
- First Failure Data Capture (FFDC) 364
- Flexible Service Processor (FSP) 308
 - failover 365
- floating IP address 303, 305, 310, 318
- frame 10, 99
- FRU See *Field Replaceable Unit*
- functional differences 49

G

- gateway, setting 248
- global server 91
- group 211–212
 - creating 212
 - smadmin 202
 - smmgr 202
 - smmon 202
 - smservicerep 202
 - smuser 202
- Group Editor wizard 213
- GroupRead role 205
- Guided Repair 365

H

- HA See *high availability*
- hardware appliance 7
- Hardware Management Console (HMC) 1, 3, 301
 - as DHCP server 73
 - commands
 - not supported 287
 - overview 280
 - supported 282
- hierarchical management 48, 91
- high availability (HA) 299
 - commands 380
 - configuration 312
 - configuration planning 307
 - logs 306
 - network 307–308
 - overview 302
 - terminology 304
 - updates 322
 - upgrades 322
- HMC See *Hardware Management Console*
- HMC to SDMC transition 65
- hmcoperator user role 199
- hmcpe user role 199
- hmcservicerep user role 199

- hmcsuperadmin user role 199
- hmcviewer user role 199
- Host Ethernet Adapter 140
- host name, setting 248
- Hot Repair/Upgrade 365
- hscpe user 198
- hscroot user 198

I

- IBM System Storage management 392
- IBM System x management 391
- IBM System z management 391
- IBM Systems Director 3
- IBM Tivoli 42
- IBM Tivoli System Automation for Multiplatform 303
- identify LED 366
- IEvent 346
- impdata command 68, 282
- initiate FSP failover 365
- Integrated Virtualization Manager (IVM) 1, 3, 7
- interactive transition 65, 68
- inventory 77
- IP address configuration 245
- IP forwarding 240
- IPv4 76, 83
- IPv6 76, 83
- IVM See *Integrated Virtualization Manager*
- IVM to SDMC transition 62

K

- Kerberos 232
- Kerberos client, configuring 233
- KVM 7

L

- launching a task 52
- LDAP 226
 - client, configure 229
- LED Lamp Test 366
- Linux 7, 16
- listing roles 210
- local authentication 224
- log files
 - high availability 306
 - SDMC 264
- log files, System Director 267
- logical partition (LPAR) 10

- states 10
- LPAR See *logical partition*
- lsbundle command 278
- lsldap command 228
- lsled command 59
- lsnetcfg command 252
- lsperm command 209
- lsrole command 205, 210
- lssptfile command 362
- lssvcproblem command 362
- lssys command 85
- lssyscfg command 59
- lsuser command 201, 226
- lsusergp command 203

M

- manage Virtual Server 44, 159
- managed endpoint (MEP) 10
- managed system 10
 - capabilities 94
 - edit host 86
 - power on 87
 - rebuild 43
 - remove 80
- media devices 175
- memory settings 96
- mk5250 command 282
- mksyscfg command 152
- mksysconn command 83
- mkuser command 226, 231, 236
- modem 341
- modifying a user 237
- monitored systems 343

N

- navigation area 51
- NETC RSAP 80
- network
 - boot (PXE) 18
 - configuration 240
 - connectivity, testing 253
 - settings 241
 - status IP address 305, 309, 317
 - time server 315
- Network Management 391
- node 304
- NTP service, enabling 252

O

- offline transition 71
- On Demand Type 95
- open network 18, 240
- Open or Close MES 365
- OVF/OVA 19

P

- Partial Access state 80
- partition mobility 10, 44, 195
- Password Updates Required state 88
- PE 269
- pe user 32
- pedbg commands 269
- pesh command 270
- physical disks 144
- physical volumes 172
- PlatformManagerType 85
- POWER 5 5
- POWER 575 8
- POWER 6
 - supported models 9
- POWER 7 6
 - supported models 9
- POWER code matrix 7
- power management 43
- POWER processor-based blades 2
- POWER processor-based blades, discovery 81
- Power Systems management commands 280
- Power Unit 10, 99
 - change password 102
 - initialize 45, 103
 - managment 100
 - power off 104
 - rebuild 46
 - rebuild information 104
- PowerHA 192
- private network 18, 240
- Problem Repair 366
- processor settings 96
- product engineer 269
- profile 185
- Properties view 57
- public network 240

R

- Readiness Check page 110
- Red Hat 7

- rediscover command 83
- redundancy 12, 299–301
- relocation 10
- Remote Access Manager 391
- Remote Command Execution 276
- Remote Monitoring and Control (RMC) 186, 346
- Remote Service Access Points (RSAP) 80
- Remote Virtual Terminal 276
- Remove Enclosure 365
- Remove FRU 365
- remove managed system 80
- removeHA command 321
- Repair and Verify 365
- replaced IBM Systems Director application commands 370
- replication IP address 309, 316
- Representational State Transfer (REST) 93
- Request Access page 79
- Request Management Access 93
- reserved storage device pool 45
- Resource Manager 34
- resource views 55
- REST See *Representational State Transfer*
- resume 192
- resume partitions 45
- Revoke Access page 80
- RMC See *Remote Monitoring and Control*
- rmrole command 210
- rmsptfile command 362
- rmuser command 240
- role 205–206
 - assigning 218
 - creating 206
 - defined
 - GroupRead 205
 - SMAAdministrator 10, 205, 312
 - SMMManager 10, 205
 - SMMonitor 205
 - SMUser 10, 205
 - deletion 210
 - listing 210
- role, HMC
 - hmcoperator 10, 199
 - hmcpe 199
 - hmcservicerep 199
 - hmcsuperadmin 10, 199
 - hmcuser 10
 - hmcviewer 199
- role, SDMC

- SMAAdministrator 199
- SMMManager 199
- SMMonitor 199
- SMUser 199
- root user 32
- RSAP See *Remote Service Access Points*

S

- Save Current Configuration 184
- schedule operations 43
 - creating 290
 - editing, deleting, or copying 294
 - overview 295
- scheduler commands 373
- SDMC appliance update 271
- SDMC as DHCP server 73
- SDMC hardware appliance 16
 - installation 17
 - requirements 16
- SDMC software appliance 16
 - installation 19
 - Red Hat KVM 24
 - VMware 19
 - requirements 16
- Secure Shell (SSH) 276
- Server Preferences 92
- Server Profiles 188
- servicable event processing 346
- service and support management 47
- Service and Support Manager (SSM) 336
 - command line 362
 - commands 375
 - setup 337
 - tasks 48
 - standard tasks 363
- serviceable event data 347
- serviceable events 47, 346
 - closure 350
- setup FSP failover 365
- setup wizard, installation 28
- Shared Ethernet Adapter 139
- shared processor pools 45
- shut down Virtual Server 157
- smadmin group 202
- SMAAdministrator role 10, 199, 205, 312
- smcli discover command 82
- smcli prefix command 278
- smha command 321

- smhastatus command 320–321
- SMMManager role 10, 199, 205
- smmgr group 202
- smmon group 202
- SMMonitor role 199, 205
- SMS See *Systems Management Services*
- smservicep group 202
- smuser group 202
- SMUser role 10, 199, 205
- software appliance 7
- SSH See *Secure Shell*
- SSL 341
- ssmimport command 362
- state mappings 90
- Status Manager 390
- submitsptfile command 362
- Support File Management 351
- support files
 - collecting 356
 - copying 359
 - deleting 358
 - general settings 360
 - properties 360
 - submitting to IBM 358
- Support Files task 345
- suspend 192
 - capable 134
 - operations 193
 - partitions 45
- sysadmin user 32
- System Attention LED 366
- system discovery 76
- Systems Management Services (SMS) 186

T

- table view 56
- Topology Perspectives 58
- topology view 58
- trace logs 266
- transition 61
 - in a private network 72
 - workflow 72

U

- update management 48
- Update Manager 108, 271, 391
- updates
 - auto-update 114

- getting 114
- installation 112, 119
- management 119, 126
- manual download 115
- SDMC appliance 271
- user
 - pe 10, 32, 201
 - root 32, 200
 - sysadmin 10, 32, 201
- user authentication 222
- user authorization 222
- user commands 383
- user management 223
 - creating 223
 - deleting 240
 - modifying 237
- user, HMC
 - hscpe 10, 198
 - hscroot 10, 198
 - root 198
- utilization data 44

V

- Verify Connection page 78
- View Code Information task 96
- View History Log task 96
- virtual disk images 394
- virtual disks 144, 172
- Virtual I/O Server 3
- virtual networks 45
- virtual private network (VPN) 46, 341
- Virtual Server 132
 - activation 152
 - creation 132
 - management 159
 - profiles 185
 - shutdown 157
- virtual storage 45
- Virtualization Manager 391
- VMControl 91
- VMware 7
- VPN See *virtual private network*

W

- waiting for input 88
- Welcome page 50
- World Wide Port Names 171

X
x86 hardware 16–17

Archived

Archived



IBM Systems Director Management Console: Introduction and Overview

(0.5" spine)
0.475" <-> 0.875"
250 <-> 459 pages



IBM Systems Director Management Console

Introduction and Overview



Documents the SDMC appliance, which uses the Systems Director user interface

Discusses the differences between the HMC and SDMC

Provides a practical guide to the SDMC

This IBM® RedpaperRedbooks® publication positions the IBM Systems Director Management Console (SDMC) against the IBM Hardware Management Console (HMC). The IBM Systems Director Management Console provides system administrators the ability to manage IBM Power System® servers as well as IBM Power Blade servers. It is based on IBM Systems Director.

This Redpaperpublication is designed for system administrators to use as a desktide reference when managing Virtual Servers (formerly partitions) using the SDMC.

The major functions that the SDMC provides are server hardware management and virtualization management.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks