Implementing IBM Director 5.20

- Describes how to plan and implement an IBM Director solution
- Includes many advanced scenarios of use
- Companion to IBM Director product publications

David Watts
Robert J Brenneman
David Feisthammel
Tim Sutherland

ibm.com/redbooks
Note: Before using this information and the product it supports, read the information in “Notices” on page xv.

Fourth Edition (April 2007)

This edition applies to Version 5.20 of IBM Director.

© Copyright International Business Machines Corporation 2001, 2003, 2006, 2007. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP
6.4 Mass Configuration .................................................. 368
  6.4.1 Asset ID Profile Builder ....................................... 369
  6.4.2 Configure SNMP Agent Profile Builder ...................... 373
  6.4.3 Network configuration ........................................ 375
6.5 Install-time extension tasks ........................................... 378
  6.5.1 BladeCenter Management ...................................... 378
  6.5.2 Rack Manager .................................................. 383
6.6 Free extension tasks .................................................. 386
  6.6.1 APC PowerChute Extensions for IBM Director .............. 386
  6.6.2 Electronic Service Agent ...................................... 392
  6.6.3 PowerExecutive ............................................... 393
  6.6.4 ServeRAID Manager ............................................ 393
  6.6.5 System Availability .......................................... 395
  6.6.6 Virtualization Manager ...................................... 400
6.7 Fee-based extension tasks ............................................ 400
  6.7.1 Capacity Manager .............................................. 401
  6.7.2 Remote Deployment Manager .................................. 402
  6.7.3 Software Distribution Premium Edition ..................... 407
  6.7.4 IBM z/VM Center .............................................. 411

Chapter 7. Update Manager ............................................. 413
7.1 Update Manager overview ............................................. 414
  7.1.1 Update Manager profiles ...................................... 415
  7.1.2 UpdateXpress System Packs .................................. 415
7.2 Updating IBM systems using Update Manager ..................... 416
7.3 Updating the management server ................................... 435
7.4 Update Manager and software distribution ....................... 441
  7.4.1 Software health check ....................................... 442
7.5 Important considerations ............................................ 444
  7.5.1 Update Manager needs supervision ......................... 445
  7.5.2 It is called Update Manager for a reason .................. 446
  7.5.3 Static groups have a short half-life ....................... 446
  7.5.4 Package categories should be cleaned up ................... 447
  7.5.5 Rules for success with Update Manager ..................... 447
7.6 Adding undiscovered machine types ................................ 447
7.7 Update Manager events .............................................. 450
7.8 DIRCLI commands for Update Manager ............................ 452
  7.8.1 CLEANLIB command .......................................... 452
  7.8.2 IMPORTUP command ......................................... 458
  7.8.3 The exportprof command ..................................... 459

Chapter 8. IBM Electronic Service Agent .............................. 461
8.1 Overview .......................................................... 462
8.1.1 How Electronic Service Agent works ........................................ 462
8.1.2 Implementing Electronic Service Agent .................................... 463
8.1.3 Obtaining Electronic Service Agent ........................................... 464
8.2 Installation .................................................................................. 464
  8.2.1 Installing on Windows Systems .................................................. 464
  8.2.2 Installing on Linux systems ...................................................... 465
8.3 Configuration .............................................................................. 467
8.4 Enroll systems ............................................................................ 479
  8.4.1 Event filters ........................................................................... 486

Chapter 9. IBM PowerExecutive ....................................................... 487
  9.1 Overview .................................................................................. 488
    9.1.1 PowerExecutive communication ........................................... 489
  9.2 Installation ................................................................................ 491
    9.2.1 Obtaining PowerExecutive .................................................... 491
    9.2.2 Installing on Windows Systems .............................................. 491
    9.2.3 Installing on Linux systems ................................................... 492
  9.3 Using PowerExecutive .............................................................. 493
    9.3.1 PowerExecutive Console ...................................................... 495
    9.3.2 PowerExecutive data descriptions ........................................ 500
    9.3.3 Manage trend data ............................................................... 501
    9.3.4 Manage power .................................................................... 502
    9.3.5 Derate power ........................................................................ 507
    9.3.6 Show trend data ................................................................. 508
    9.3.7 PowerExecutive console tasks .............................................. 512

Chapter 10. IBM Virtualization Manager ......................................... 515
  10.1 Overview ............................................................................... 516
    10.1.1 Features ............................................................................ 516
  10.2 Components ............................................................................ 517
    10.2.1 Components required for supported environments ............... 518
  10.3 Installation and configuration .................................................. 521
  10.4 One tool, two interfaces .......................................................... 531
    10.4.1 IBM Director Console ....................................................... 532
    10.4.2 Virtualization Manager Web interface ................................ 538
  10.5 Event filters ............................................................................ 561
  10.6 Event actions .......................................................................... 561
    10.6.1 Customizable event actions ................................................ 562
    10.6.2 Migration tasks as event actions ....................................... 564
  10.7 DIRCLI commands ................................................................ 567
    10.7.1 Virtualization Manager commands ................................... 567
    10.7.2 Noninteractive Virtualization Manager tasks ...................... 568

Chapter 11. IBM z/VM Center ......................................................... 571
## Chapter 11. Implementing IBM Director 5.20

11.1 Overview .................................................. 572
   11.1.1 z/VM Management Access Point ...................... 573
   11.1.2 z/VM Center server extension ......................... 573
   11.1.3 z/VM Center Console extension ....................... 574
   11.1.4 How it all works ..................................... 575
11.2 Planning and preparation ............................... 578
   11.2.1 Questions to answer .................................. 578
   11.2.2 The initial configuration ............................. 579
11.3 z/VM customization ....................................... 580
   11.3.1 DirMaint customization ............................... 580
   11.3.2 Define a custom user class ........................... 590
   11.3.3 Create IDs for MAPSERVE and MAPAUTH ............. 591
   11.3.4 VSMSERVE enablement ................................ 594
   11.3.5 VMRM enablement .................................... 601
11.4 Installing the Management Access Point ............... 603
11.5 Installing the z/VM Center extension ................. 614
11.6 Verifying the installation and initial setup .......... 617
11.7 General usage ........................................... 625
   11.7.1 Virtual Server Deployment ........................... 626
   11.7.2 Server complexes ................................... 654

## Chapter 12. Event management

12.1 Introduction .............................................. 678
12.2 The Event Action Plan Wizard ......................... 679
12.3 The Event Action Plan Builder ......................... 686
   12.3.1 Event action plans .................................. 687
12.4 Event filters ............................................. 689
   12.4.1 Event filter types .................................. 690
   12.4.2 Event Type tab ...................................... 698
   12.4.3 Severity tab ........................................ 722
   12.4.4 Day/Time tab ........................................ 723
   12.4.5 Category tab ........................................ 725
   12.4.6 Sender Name tab .................................... 725
   12.4.7 Event Text tab ...................................... 727
   12.4.8 Extended Attributes tab ............................. 729
   12.4.9 System Variables tab ................................ 729
12.5 Event actions ............................................ 731
12.6 Example: creating an event action plan ............... 742
12.7 Event flow ................................................ 746
   12.7.1 Event queuing ....................................... 747
12.8 Recommended EAPs ....................................... 749
   12.8.1 Event filters ........................................ 750
   12.8.2 Log all events ...................................... 750
12.8.3 Hardware events for client systems and OEM hardware .... 754
12.8.4 Hardware events for System x servers ....................... 755
12.8.5 Online and offline events .................................. 757
12.8.6 Example of an application EAP ............................ 757
12.9 Exporting and importing EAPs ................................ 760
12.9.1 Export ......................................................... 761
12.9.2 Import ......................................................... 761

Chapter 13. Scenarios .................................................. 765
13.1 IBM Director Agent on a cloned Windows system .......... 766
  13.1.1 The problem .................................................. 770
  13.1.2 The solution .................................................. 771
  13.1.3 Extending this scenario .................................... 778
13.2 Automated IBM Director Agent promotion .................. 778
  13.2.1 The problem .................................................. 779
  13.2.2 The solution .................................................. 779
13.3 Creating status reports with DIRCLI ........................ 795
  13.3.1 The problem .................................................. 795
  13.3.2 The solution .................................................. 796
  13.3.3 Extending this scenario .................................... 811
13.4 Quick-start implementation of IBM Director ................ 812
  13.4.1 The task ...................................................... 814
  13.4.2 The solution .................................................. 814
  13.4.3 Extending this scenario .................................... 842
13.5 Comparing system lists using a spreadsheet ............... 842
  13.5.1 The problem .................................................. 843
  13.5.2 The solution .................................................. 843
  13.5.3 Extending this scenario .................................... 847
13.6 Monitoring for prohibited applications ...................... 848
  13.6.1 The problem .................................................. 848
  13.6.2 The solution .................................................. 849
  13.6.3 Extending this scenario .................................... 853
13.7 Monitoring for inventory changes .............................. 860
  13.7.1 The problem .................................................. 860
  13.7.2 The solution .................................................. 860
  13.7.3 Extending this scenario .................................... 869
13.8 Data center planning using PowerExecutive ................ 869
  13.8.1 The problem .................................................. 869
  13.8.2 The solution .................................................. 869
13.9 Provisioning test systems with z/VM complexes .......... 877
  13.9.1 The problem .................................................. 877
  13.9.2 The solution .................................................. 877
  13.9.3 Extending this scenario .................................... 891
Appendix A. Event actions ................................. 893
Event Action Plan Builder actions ......................... 894
Add/Remove event system to static group .................. 896
  Parameters ........................................ 896
Add/remove source group members to target static group .... 898
  Parameters ........................................ 898
Add a message to the console ticker tape .................. 898
  Parameters ........................................ 899
Add to the Event Log .................................... 899
Define a Timed Alarm to Generate an Event ................. 900
  Parameters ........................................ 900
Define a Timed Alarm to Start a Program on the Server .... 901
  Parameters ........................................ 902
Log to a Textual Log File ................................ 902
  Parameters ........................................ 903
Post to a News Group (NNTP) ............................... 903
  Parameters ........................................ 904
Resend Modified Event ................................... 904
  Parameters ........................................ 904
Send an Alphanumeric Page (via TAP) ....................... 906
  Parameters ........................................ 906
Send an Event Message to a Console User .................. 907
  Parameters ........................................ 907
Send an Internet (SMTP) E-mail ............................ 908
  Parameters ........................................ 909
Send an SNMP Inform to an IP Host ....................... 909
Send an SNMP Trap to a NetView Host ...................... 910
  Parameters ........................................ 910
Send an SNMP Trap to an IP Host .......................... 911
  Parameters ........................................ 911
Send a Numeric Page .................................... 912
  Parameters ........................................ 912
Send a TEC Event to a TEC Server ....................... 913
  Parameters ........................................ 913
Set an Event System Variable .............................. 914
  Parameters ........................................ 915
Start a Program on a System .............................. 916
  Parameters ........................................ 916
  Examples ......................................... 916
Start a program on the event system ...................... 917
  Parameters ........................................ 917
Start a Program on the Server ............................ 918
  Parameters ........................................ 918
Start a Task on the “event” System .......................................................... 919
Parameters ........................................................................................................ 919
Update the Status of the “event” System ....................................................... 920
Parameters ........................................................................................................ 920
Virtualization Manager event actions ............................................................... 922
Add a Host to a Virtual Farm ........................................................................... 923
Parameters ........................................................................................................ 923
Add a Host to VirtualCenter ............................................................................ 924
Parameters ........................................................................................................ 924
Manage a Host ................................................................................................... 925
Parameters ........................................................................................................ 925
Manage a Virtual Server ................................................................................. 926
Parameters ........................................................................................................ 926
Remove a Host from a Virtual Farm ................................................................. 927
Parameters ........................................................................................................ 927
Migration tasks ................................................................................................. 928

Appendix B. CIM subscriptions ........................................................................ 931
Predefined CIM handlers ................................................................................... 932
Predefined CIM filters ....................................................................................... 932
Predefined CIM subscriptions ......................................................................... 937

Abbreviations and acronyms ............................................................................ 943

Related publications ......................................................................................... 947
IBM Redbooks ................................................................................................... 947
Other publications ............................................................................................. 947
Online resources ................................................................................................ 949
IBM Web sites ................................................................................................... 949
Non-IBM Web sites .......................................................................................... 950
How to get IBM Redbooks ............................................................................... 951
Help from IBM .................................................................................................. 951

Index .................................................................................................................. 953
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.

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

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

- Redbooks (logo) ®
- eServer™
- iSeries™
- i5/OS®
- pSeries®
- xSeries®
- z/VM®
- Asset ID™
- AIX 5L™
- AIX®
- BladeCenter®
- DirMaint™
- Domino®
- DB2 Universal Database™
- DB2®
- Electronic Service Agent™
- FlashCopy®
- HelpCenter®
- IntelliStation®
- IBM®
- Lotus Notes®
- Lotus®
- Netfinity®
- Notes®
- OpenPower™
- PowerExecutive™
- Predictive Failure Analysis®
- POWER™
- Redbooks®
- Sametime®
- ServeRAID™
- ServicePac®
- System i™
- System p™
- System x™
- System z™
- Tivoli Enterprise™
- Tivoli Enterprise Console®
- Tivoli Management Environment®
- Tivoli®
- TotalStorage®
- TME®
- Virtualization Engine™
- Wake on LAN®
- WebSphere®

The following terms are trademarks of other companies:

- Oracle, JD Edwards, PeopleSoft, Siebel, and TopLink are registered trademarks of Oracle Corporation and/or its affiliates.

- Adobe Reader, Adobe, and Portable Document Format (PDF) are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

- IPX, Java, JumpStart, JDBC, JRE, JVM, Power Management, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

- Active Directory, Excel, Microsoft, MSN, Visual Basic, Windows NT, Windows Server, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

- i386, 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, other countries, or both.

- 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

IBM® Director is a comprehensive systems manager designed for use across the full IBM Systems product family. An integrated, easy-to-use suite of tools, IBM Director provides clients with flexible systems-management abilities to help maximize system availability and lower IT costs. With IBM Director, IT administrators can view and track the hardware configuration of remote systems and monitor the component performance of processors, disks, and memory.

This IBM Redbooks® publication describes how to implement systems management with IBM Director 5.20, discussing IBM Director architecture, its adherence to industry standards, and the planning required for a solution.

This book covers how IBM Director integrates with the IBM System x™ service processors and the options available to deploy agents. Tasks include configuring events and alerting subsystems. The book also describes several real-life scenarios employing IBM Director.

This book helps you tailor and configure IBM Director while showing you how best to maximize your investment in IBM technology. This book is a companion to the IBM Director online publications and the product CD-ROM.

The team that wrote this book

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

David Watts is a Consulting IT Specialist at the IBM ITSO Center in Raleigh. He manages residencies and produces Redbooks on hardware and software topics related to IBM System x and BladeCenter® servers and associated client platforms. He has authored over 80 books, papers, and technotes. He holds a Bachelor of Engineering degree from the University of Queensland (Australia) and has worked for IBM for over 15 years. He is an IBM Certified IT Specialist.

Robert J Brenneman is a Software Engineer at the Test and Integration Center for Linux® in Poughkeepsie, NY. He works in Systems and Technology Group testing software for Linux on System z™. He has a Bachelor of Engineering degree from Auburn University and has worked for IBM since 2000.
David Feisthammel works in the Executive Briefing Center at the IBM Center for Microsoft® Technologies in Kirkland, Washington. He is the System x and BladeCenter Systems Management Specialist there and regularly presents and demonstrates IBM management products and solutions to customers. He has over 15 years of experience in the IT field, including four years as an IBM client. He worked in Raleigh for two years as a Program Manager and Worldwide Product Manager for IBM Director, Netfinity® Director, and related products. He holds a degree in Biological Sciences from Northwestern University. His area of expertise is systems management, including IBM Director, Microsoft SMS, and IBM Advanced System Management hardware. He was a co-author of the previous two versions of this book.

Tim Sutherland works in the Systems and Technology Group at IBM in Sydney, Australia. He is an IBM System x IT Advisory specialist and regularly presents to customers and provides workshops for x86 and systems management solutions. He has over 11 years of experience with IBM, working in New Zealand and Australia. He holds Business Computing (CBC), Microsoft Certified Systems Engineer (MCSE), and IBM eServer™ Certified Systems Expert xSeries® (CSEx) certifications. His areas of expertise are IBM System x servers, IBM BladeCenter, and IBM systems management solutions.

The team (l–r): Jay, Tim, David F., David W.
Thanks to the authors of the previous editions of this book:

- The third edition:
  - David Watts
  - David Feisthammel
  - Torben Jungsberg
  - Keith Olsen

- The second edition:
  - David Watts
  - Eddy Ciliendo
  - David Feisthammel
  - Martin Gudmundsen

- The first edition:
  - David Watts
  - Lesley Bell
  - Daniel DeBusschere
  - Yoko Fujiwara
  - Olaf Menke

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

- ITSO:
  - David Bennin, Networking Support, Poughkeepsie
  - Roy Costa, z/VM® Support, Poughkeepsie
  - Linda Robinson, Graphics Support, Raleigh
  - Margaret Ticknor, IT Support, Raleigh
  - Erica Wazewski, Business Controls, Poughkeepsie
  - Debbie Willmschen, Lead Editor, Raleigh
  - Julie Czubik, Editor, Poughkeepsie

- IBM Product Management:
  - Lauren Bragg, Raleigh
  - David Hardman, Raleigh
  - Ted Mazanec, Raleigh
  - Claudia Prawirakusumah, Boeblingen
  - Brian Sanders, Raleigh
  - Don Smith, Poughkeepsie
  - Chuck Weber, Raleigh

- IBM Director Development:
  - Julie Biselski, Raleigh
  - Jin Kim, Kirkland
  - Sandy Kipp, Raleigh
  - Karen Mobley, Raleigh
Become a published author

Join us for a two- to six-week residency program! Help write an IBM Redbooks publication dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You'll team with IBM technical professionals, Business Partners, or customers.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

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

► Use the online Contact us review form found at:
  ibm.com/redbooks

► Send your comments in an email to:
  redbook@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
Chapter 1. Introduction

This chapter provides an overview of the IBM systems management solution and briefly describes industry standards related to systems management. Then we look at IBM Director itself. A product overview and licensing summary is provided, along with a description of some of the main new features of the latest release. Finally, we provide a list of resources for additional information about IBM Director, including where to obtain various related pieces of software.

The topics covered in this chapter are:

- 1.1, “Overview” on page 2
- 1.2, “Other platforms” on page 2
- 1.3, “IBM Systems Director” on page 3
- 1.4, “Industry standards” on page 3
- 1.5, “IBM Director overview” on page 9
- 1.6, “IBM Director licensing” on page 20
- 1.7, “What is new in IBM Director 5.20” on page 23
- 1.8, “IBM Director resources” on page 26
- 1.9, “Features of IBM Director” on page 30
- 1.10, “This book” on page 36
1.1 Overview

Effective systems management is more important than ever as IT administrators are faced with the daunting task of managing complex, heterogeneous IT environments with fewer resources. Reducing the complexity with intuitive, automated tools that simplify critical IT tasks and require less training is key to helping customers face this challenge. The latest release of IBM Director enables IT staff to reduce the complexity and costs associated with managing IT environments as well as help them get started faster and be more productive with enhancements that improve ease of use.

End users are so dependent on their systems that they are increasingly frustrated by system outages, print problems, and anything that keeps them from being productive. They expect immediate assistance from the help desk or support center to fix a problem or even just to show them how to use an application. IT personnel are challenged to keep system availability high and to handle end-user requests quickly and efficiently. Yet today, their environments are more complex than ever, with diverse management tools that have no common characteristics and little to no integration. This means that they can spend too much time managing existing IT resources rather than working on other important problems.

1.2 Other platforms

IBM Director enables monitoring and event management across heterogeneous IT environments, including Intel® and POWER™ systems that support Windows®, Linux, AIX® 5L™, and i5/OS® from a single Java™-based user interface. From one access point, users can monitor system resources, inventory, events, task management, core corrective actions, distributed commands, and hardware control for both servers and storage.

IBM Director provides broad platform coverage, including Microsoft Windows, Intel Linux, Power Linux, AIX, i5/OS, and System z Linux environments across System p™, System i™, System x, System z, BladeCenter, and OpenPower™. This edition of our IBM Redbooks publication adds detailed discussion on the new functionality of IBM Director 5.20, as well as the z/VM Center extension that was introduced with the previous release of IBM Director.

z/VM Center is an extension to IBM Director for Linux on System z that saves time and simplifies the creation and grouping of virtual servers, and the deployment of Linux systems under z/VM. Through a drag-and-drop interface, IBM Director allows for fast, easy, and repeatable deployments of new virtual servers. See Chapter 11, “IBM z/VM Center” on page 569, for more information.
1.3 IBM Systems Director

IBM Systems Director is the family of platform management solutions designed to provide IT professionals with the tools they need to virtualize more and manage less of their IT infrastructure. Through IBM Systems Director, customers will be able to manage both physical and virtual IT resources spanning servers, storage, and networking.

IBM Systems Director family includes IBM Director 5.20 and IBM TotalStorage® Productivity Center as its base offerings and provides value-added extensions that come from IBM and a growing ecosystem of solution providers.

IBM Systems Director family unifies under one strategy, IBM server and storage management solutions, and builds on this foundation to provide new virtualization management support, with the goal of helping clients to manage physical and virtual resources together across multiple, heterogeneous systems.

IBM Systems Director family is a modular, open standards based solution that includes a base set of capabilities for businesses of all sizes, platform-specific extensions, and optional value added extensions for more advanced capabilities.

1.4 Industry standards

It has often been said that the nice thing about industry standards is that there are so many of them. This statement certainly is true regarding systems management. A key underpinning of IBM Director is the adherence to industry standards for systems management.

A critical requirement that must be met by any Intel-based, non-IBM system is that the system must implement Systems Management BIOS (SMBIOS), Version 2.2 or later. SMBIOS extends the system BIOS to support retrieval of management data in desktop, mobile, and server system hardware. As this requirement is placed on system firmware, it is applicable even for systems prior to loading an operating system. Most Intel-based hardware vendors implement SMBIOS in their systems.

IBM System x servers are instrumented to support many industry standards related to systems management. IBM Director supports these standards as well, providing comprehensive cross-platform support. Since IBM Director is based on
industry standards, it can manage both IBM and non-IBM Intel processor-based hardware. This is a huge benefit from the standpoint of simplifying systems management of a heterogeneous environment. A very brief summary of each systems management industry standard supported by IBM Director is provided here.

1.4.1 Common Information Model

The Common Information Model (CIM), adopted and evolved by the Distributed Management Task Force (DMTF), is a published systems management standard and was developed in open forum by DMTF member companies. Defined and promoted as an industry standard for managing systems, CIM was designed to be used for describing management information between differing management applications, running in many different operating environments, including Microsoft Windows and Linux. Detailed information about the CIM Specification is available from the DMTF home page:

http://www.dmtf.org

CIM provides a common definition of management information for systems, networks, applications, and services, and allows for vendor extensions. CIM's common definitions enable vendors to exchange rich management information between systems throughout the network. CIM is composed of a specification and a schema. The schema provides the actual model descriptions, while the specification defines the details for integration with other management models.

CIM is used extensively throughout IBM Director. In fact, the new capability in IBM Director 5.10 to manage Level-1 systems is based on CIM instrumentation and providers. For more about this capability see “IBM Director Core Services” on page 12.

1.4.2 Intelligent Platform Management Interface

Intelligent Platform Management Interface (IPMI) is a standardized, abstracted, message-based interface developed by Intel that defines records for describing platform management devices and their characteristics. This interface allows for standard communication between systems management software such as IBM Director and IPMI-compliant system management hardware such as IBM Baseboard Management Controllers (BMCs).
Figure 1-1 shows how various IPMI-aware technologies built into many System x servers work together to surface hardware issues into IBM Director and other leading systems management packages. Note that if an RSA or RSA II card is installed in a System x server that has a BMC, the inband path to and from the BMC is disabled. By *installed*, we mean that both the hardware and the drivers are properly installed and configured.

1.4.3 Platform Event Trap

A *platform event* is defined as an event that is originated directly from platform firmware (BIOS) or platform hardware (ASIC, chip set, or microcontroller) independent of the state of the operating system or system management hardware. The Platform Event Trap (PET) format is used for sending a platform event in an SNMP trap. The trap may be directly issued from the platform or may be indirectly issued via a proxy (local or remote) that acts on events or alternatively formatted traps from the platform.
The Platform Event Trap allows traps to be generated from various sources including:

- BIOS
- OS bootstrap loader
- NIC
- System alert ASIC
- System management micro-controller
- System management software
- Alert proxy software
- Service Location Protocol

Service processors such as the BMC issue PET-formatted events.

1.4.4 Predictive Failure Analysis

Predictive Failure Analysis® (PFA) gives key components in System x servers the ability to monitor their own health and generate an alert up to 48 hours before failure occurs. This allows the system administrator to either hot swap the component (if applicable) or schedule downtime at low-impact times for the component to be changed or refreshed.

PFA code monitors certain subsystems within the component, and if tolerances exceed a predetermined range, an alert is automatically generated. For example, in hard disks, PFA code monitors:

- Read/write errors
- Fly height changes (the height of the disk head above the platter)
- Torque amplification control (the amount of power used to keep the drive spinning at a constant speed)

IBM implements PFA on more server components than any other vendor. The System x components currently protected by PFA are:

- Hard disk drives
- Fans
- Power supply units
- Memory
- CPUs
- Voltage regulator modules

IBM is extremely confident of the PFA technology used in the System x range. If a hardware component generates an alert within the warranty period of the component they will exchange the component on the basis of that alert rather than waiting for the failure to actually occur.
1.4.5 Service Location Protocol

The Service Location Protocol (SLP) was originally an Internet Engineering Task Force (IETF) standards track protocol that provides a framework to allow networking applications to discover the existence, location, and configuration of networked services in enterprise networks. Traditionally, in order to locate services in the network, users of network applications have been required to supply the host name or network address of the machine that provides a desired service. SLP eliminates the need for a user to know the name or address of a network host supporting a service.

SLP is used to discover Level-1 IBM Director Agent systems. See “IBM Director Core Services” on page 12.

1.4.6 Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is a set of Internet standards for communicating with devices such as servers, workstations, printers, routers, switches, and hubs connected on a TCP/IP network.

A device is said to be **SNMP manageable** if it can be monitored and controlled using SNMP messages. These devices contain SNMP agent software to send, receive, and act upon SNMP messages. SNMP uses Management Information Base (MIB) files, which define the information available from any SNMP-manageable device.

SNMP is an application layer protocol that facilitates the exchange of management information between network devices and is part of the TCP/IP suite. It is perhaps the oldest and most widely implemented standard for systems management. Although SNMPv3 can be implemented in a secure manner, there are serious security issues you must consider before using SNMPv1 or SNMPv2. For more information about SNMP security see “Simple Network Management Protocol” on page 98.

1.4.7 System Management Bus

The System Management Bus (SMBus) is the default standard interface for system management communication in most electronic equipment from televisions to computers. It is based on the Inter Integrated Circuit (I²C) bus that was developed by Philips. It is a two-wired bus embedded on the system board in all System x servers and supports temperature sensors, fan sensors, power supply sensors, and other devices that might be in the server and can provide system management information.
Some servers do not have a service processor, but they still can provide some system management information. This is taken care of by the LM chip. The LM chip replaces the service processor in entry-level servers and is connected to the SMBus.

Because the LM chip is very common in computers today, most operating systems contain a device driver for it and can receive any messages sent from it. IBM Director can get system management information from the SMBus driver running non-IBM hardware that use the LM chip.

Even if the chip provides support for many different system management devices, it still comes down to the kind of components used in the server. For example, a fan must have an RPM counter, and the system board must have a temperature sensor for these parameters to be monitored and communicated. The LM chip is a one-way chip that can only send information to the operating system. It is not possible to request information from the LM chip.

For information about SMBus see:
http://www.smbus.org

For information about I²C see:
http://www.philipslogic.com/i2c

1.4.8 Storage Management Initiative Specification

The Storage Management Initiative Specification (SMI-S), driven by the Storage Networking Industry Association (SNIA), is an industry standard to access and manage storage devices. SMI-S expands on the CIM and WBEM standards, using XML over HTTP to communicate between storage management applications and the devices they manage.

1.4.9 System Management BIOS

The System Management BIOS (SMBIOS) specification, developed by Intel, addresses how motherboard and system vendors present management information about their products in a standard format by extending the BIOS interface on x86 architecture systems. The information is intended to allow generic instrumentation to deliver this information to management applications that use DMI, CIM, or direct access, eliminating the need for error-prone operations like probing system hardware for presence detection.
1.4.10 Systems Management Architecture for Server Hardware

The DMTF Systems Management Architecture for Server Hardware (SMASH) initiative is a suite of specifications that deliver architectural semantics, industry standard protocols, and profiles to unify the management of the data center. The Server Management (SM) Command Line Protocol (CLP) specification enables management of heterogeneous servers independent of machine state, operating system state, server system topology, or access method. This allows local and remote management of server hardware in both out-of-service and out-of-band management environments. SMASH also includes the SM Managed Element Addressing Specification, SM CLP-to-CIM Mapping Specification, SM CLP Discovery Specification, and Server Management Profiles.

1.5 IBM Director overview

IBM Director provides an integrated suite of software tools for a consistent, single point of management and automation. IBM Director's tools provide clients with flexible capabilities to realize maximum system availability and lower IT costs. With IBM Director, IT administrators can view and track the hardware configuration of remote systems in detail and monitor the usage and performance of critical components, such as processors, disks, and memory. IBM Director also complements and integrates with robust enterprise and workgroup management systems from vendors such as BMC Software, Computer Associates, HP, Microsoft, NetIQ, and Tivoli®.

IBM Director's open design point and support for industry standards enables heterogeneous hardware management with broad platform and operating system support, protecting clients' IT investment. IBM Director enables monitoring and event management across a heterogeneous IT environment, including Intel and POWER systems that support Windows, Linux, NetWare, ESX Server, AIX 5L and i5/OS from a single Java-based user interface. From one access point, users can monitor system resources, inventory, events, task management, core corrective actions, distributed commands, and hardware control for servers, clients, and storage.
1.5.1 IBM Director components

IBM Director is designed to manage a complex environment that contains numerous servers, desktop computers, workstations, notebook computers, storage subsystems, and various types of SNMP-based devices. Figure 1-2 shows a simple diagram of the major components you might find in an IBM Director managed environment, as well as the IBM Director software components (if any) on each type of hardware.

Figure 1-2  Typical IBM Director management environment
The hardware in an IBM Director environment can be divided into the following groups:

- **Management servers**: one or more servers on which IBM Director Server is installed
- **Managed systems**: servers, workstations, desktop computers, and notebook computers that are managed by IBM Director
- **Management consoles**: servers, workstations, desktop computers, and notebook computers from which you communicate with one or more IBM Director Servers
- **SNMP devices**: network devices, printers, or computers that have SNMP agents installed or embedded

In today’s rapidly changing and complex IT environments, it is common to find a mixture of system types, wiring structures, and network protocols used within a single corporate IT infrastructure. IBM Director supports hardware from the entire IBM Systems family, Intel-based hardware from many manufacturers, as well as multiple network connection types and protocols, enabling you to manage a heterogeneous environment.

IBM Director software has four main components:

- IBM Director Core Services (also known as Level-1 Agent)
- IBM Director Agent (also known as Level-2 Agent)
- IBM Director Console
- IBM Director Server

Each system in an IBM Director environment will have one or more of these components installed:

- IBM Director Core Services is a subset of IBM Director Agent and can be installed on managed systems where the smallest agent footprint is critical and management requirements are fairly simple. It is also called a Level-1 managed system.
- IBM Director Agent is the full-function management agent designed to provide comprehensive systems management capabilities. It is also called a Level-2 managed system.
- IBM Director Console is installed on any system from which a system administrator will remotely access the management server (called a management console).
- IBM Director Server is installed on the system that is to become the management server. Ideally, this is a single system in the environment, but this is not always possible.
IBM Director can manage some systems on which no component of IBM Director is installed. Such managed systems are referred to as *Level-0* managed systems. These systems must at a minimum support either the Secure Shell (SSH) or Distributed Component Object Model (DCOM) protocol. For additional information about determining whether to install IBM Director Core Services or IBM Agent on your managed systems, see 2.6, “Choosing the right agent” on page 51, and 6.1, “Tasks by agent level” on page 282.

In addition, you can augment the base functionality of IBM Director by installing IBM Director extensions to the various components listed above.

Here we provide a brief description of each of these components and extensions.

**IBM Director Core Services**

IBM Director Core Services provides a subset of IBM Director Agent functionality that is used to communicate with and administer a managed system. Systems that have IBM Director Core Services (but not IBM Director Agent) installed on them are referred to as *Level-1* managed systems.

IBM Director Core Services provides management entirely through standard protocols. This includes discovery, authentication, and management. The IBM Director Core Services package installs an SLP service agent, an SSL-enabled CIMOM (on Linux), or CIM mapping libraries to WMI (on Windows), an optional ssh server, and platform-specific instrumentation. You can perform the following tasks on a Level-1 managed system:

- Collect inventory.
- Promote to Level-2 management by distributing IBM Director Agent.
- Manage events using event action plans, event subscription, and event log.
- Monitor hardware status.
- Reboot or shut down the managed system.
- Run command-line programs.
- Distribute system update packages through software distribution.
- Remote session (requires ssh).

**Note:** IBM Director Core Services will not surface hardware events from non-IBM hardware, since the IBM CIM mapping libraries do not understand CIM indications from non-IBM hardware. The single exception to this rule is that SMART drive events should be surfaced, since there is an industry standard method developed specifically for this purpose.

**IBM Director Agent**

IBM Director Agent is installed on a managed system to provide enhanced functionality for IBM Director to communicate with and administer the managed
system. IBM Director Agent provides management data to the management server through various network protocols.

Systems (IBM or non-IBM servers, desktop computers, workstations, and mobile computers) that have IBM Director Agent installed on them are referred to as Level-2 managed systems.

Tip: For the latest information about supported operating systems see the current version of IBM Director Hardware and Software Support Guide:
http://www.ibm.com/systems/management/director/resources

IBM Director Agent features vary according to the operating system and platform on which it is installed. See Table 6-3 on page 286 for details.

IBM Director Console
IBM Director Console is the graphical user interface (GUI) for IBM Director Server. Using IBM Director Console, system administrators can conduct comprehensive hardware management using either a drag-and-drop action or a single click. The console has undergone significant improvements in the latest release of IBM Director. For more information about these enhancements see Chapter 1 of the IBM Director Systems Management Guide.

When you install IBM Director Console on a system, IBM Director Agent is not installed automatically. If you want to manage the system on which you have installed IBM Director Console, you must also install IBM Director Agent on that system.

Tip: For the latest information about supported operating systems see the current version of the IBM Director Hardware and Software Support Guide:
http://www.ibm.com/systems/management/director/resources

You can install IBM Director Console on as many systems as you need. The license is available at no charge.

IBM Director Server
IBM Director Server is the main component of IBM Director. IBM Director Server contains the management data, the server engine, and the application logic. It provides basic functions such as discovery of the managed systems, persistent storage of inventory data, SQL database support, presence checking, security and authentication, management console support, and administrative tasks.
In the default installation under Windows, Linux, and AIX, IBM Director Server stores management information in an embedded Apache Derby database. You can access information that is stored in this integrated, centralized, relational database even when the managed systems are not available. For large-scale IBM Director solutions, you can use a stand-alone database application, such as IBM DB2® Universal Database™, Oracle®, or Microsoft SQL Server. A complete list of supported databases can be found in 2.4, “Database considerations” on page 48.

**Tip:** For the latest information about supported operating systems see the current version of the *IBM Director Hardware and Software Support Guide*: http://www.ibm.com/systems/management/director/resources

IBM Director Server requires a license. Every server in the IBM Systems family (System x, p, i, z and BladeCenter) comes with an IBM Director Server license. If you want to install IBM Director Server on a non-IBM system, you must purchase an IBM Director Server license (part number 32R1223).

### 1.5.2 IBM Director Extensions

There are several plug-in modules available for IBM Director, collectively called IBM Director Extensions, that are available from IBM and third parties. These extensions further extend the capabilities of IBM Director in a variety of ways:

- Provided on the base IBM Director installation CD and simply selected during installation
- Available for download at no charge from IBM or third-party Web sites
- Fee-based products that require a license

**Important:** The Server Plus Pack for IBM Director 4.x has been discontinued and is no longer available. For more information about how to upgrade to IBM Director 5.x if these extensions are already installed, see 4.3, “Server Plus Pack considerations” on page 177.

We include here a list of IBM Director Extensions that were available when IBM Director 5.20 was released.
**Install-time extensions**

These extensions are provided on the IBM Director installation CD and can be selected for installation during initial installation of base IBM Director components:

- **System x Management Extension**
  
  The System x Management Extension enables System x-specific functionality, including System x power management functions, the Server Configuration Manager task, and Management Processor Command-Line Interface (MPCLI) support for the Remote Supervisor Adapter (RSA) family of service processors running on System x hardware. See 6.3.17, “Server Configuration Manager” on page 335, for more information.

- **IBM Director Remote Control Agent**
  
  Although not technically an extension, we mention IBM Director Remote Control Agent here since it is an optionally selectable component during the installation of IBM Director Server and Console, as well as the Level-2 IBM Director Agent for Windows. This task provides a software-based, remote console on the managed system running a supported version of the Microsoft Windows operating system. See 6.3.13, “Remote Control” on page 317, for more information.

- **BladeCenter Management Extension**
  
  The BladeCenter Management Extension is a pair of tools that work together and are focused on managing the IBM BladeCenter infrastructure.

  - **BladeCenter Configuration Manager** allows you to create and edit profiles that include configuration settings for the components of BladeCenter chassis, such as Ethernet and Fibre Channel switches, and management modules. You can easily and quickly apply these modules to BladeCenter chassis in your environment.

  - **Network Device Manager** starts vendor software to manage your switches or other network devices. Depending on the device, a Telnet window, Web interface, or other software interface is started.

See 6.5.1, “BladeCenter Management” on page 376, for more information.

- **Rack Manager**
  
  Rack Manager is an extension that allows you to group your equipment in rack suites. Using Rack Manager, you can create virtual racks by associating equipment, such as managed systems and devices, networking devices, power devices, and monitors, with a rack in order to visually represent an existing rack in your environment.

  You can use Rack Manager to view hardware-status alerts that occur on managed systems or devices in a rack. If a rack component has a
hardware-status alert, the rack component is outlined in red, blue, or yellow, depending on the severity level. See 6.5.2, “Rack Manager” on page 381, for more information.

**Free extensions**

These extensions are available from IBM and third parties for no additional charge. They can be downloaded and installed after IBM Director components are in place to add functionality to the base IBM Director capabilities.

- **HMC Manager**

  HMC Manager Tools is a suite of tools that integrates many Hardware Management Console (HMC) functions into IBM Director. With this extension installed, IBM Director can discover and authenticate with an HMC that is managing IBM System i, System p, or System z servers, then present all Central Electronic Complexes (CECs) and Logical Partitions (LPARs) that are running on these servers.

  In this manner, the IBM Director Console can be used as a single point of management, showing topology and hardware status, as well as providing power and basic hardware control for these advanced server solutions. If more extensive management is required, IBM Director can perform an in-context launch of the HMC directly.

- **IBM Electronic Service Agent™ for System x - Director Extension**

  IBM Electronic Service Agent (eSA) is a software service management tool that leverages IBM Director Agent to provide automatic hardware problem reporting and system inventory collection in order to reduce server downtime and other service-related costs. There are eSA extensions for both IBM Director Server and Console, which allow configuration and control of eSA function.

  IBM Director Agent gathers machine inventory and system errors from the managed system and forwards this data to IBM Director Server. If the system is under service agreement or warranty, the management server formats and sends the information to IBM, either by dial-up or the Internet. Using the eSA IBM Director extension you can configure system contact and location information, view historical details of significant system events, view systems eligible for Electronic Service, and enable eligible systems for Electronic Service. See Chapter 8, “IBM Electronic Service Agent” on page 459, for more information.

- **IBM PowerExecutive™**

  The IBM PowerExecutive extension to IBM Director is available for selected IBM BladeCenter and System x servers and allows direct power monitoring through IBM Director. This tool enables customers to trend actual power
consumption and corresponding thermal loading of supported IBM systems running in their environment with their applications.

IBM PowerExecutive provides the ability to monitor actual power draw and thermal loading information. This helps customers to properly size input power based on physical systems, as well as to more efficiently plan new datacenter construction and or modification, resulting in better utilization of existing resources. See Chapter 9, “IBM PowerExecutive” on page 485, for more information.

► IBM Virtualization Manager

With the IBM Virtualization Manager extension, IBM Director provides a single point of management for both physical and virtual systems in a consistent way across different virtualization technologies. This support includes a Web-based user interface; a dashboard health summary; and a graphical topology with which you can visualize and navigate relationships between virtual and physical resources, and perform simplified virtualization tasks such as creating, deleting, modifying, and relocating virtual servers. See Chapter 10, “IBM Virtualization Manager” on page 513, for more information.

You can download the Virtualization Manager extension to IBM Director from: http://www.ibm.com/systems/management/director/downloads.html

► ServeRAID™ Manager

ServeRAID Manager is a standalone tool developed by IBM that is also available as an IBM Director extension over the Web. This comprehensive RAID management tool provides a graphical interface that you can use while your server is running to monitor ServeRAID adapters or controllers that are installed locally or remotely on managed servers, alerting you in the event of ServeRAID configuration changes.

ServeRAID Manager can also perform configuration functions, including creation and deletion of logical drives, changing the RAID level, dynamically increasing the logical drive size, and rebuilding a logical drive. See 6.6.4, “ServeRAID Manager” on page 391, for more information.

You can download the ServeRAID Manager extension to IBM Director from: http://www.ibm.com/systems/support/supportsite.wss/docdisplay?brandind=5000016&lndocid=SERV-DIRECT

► System Availability

System Availability is an extension to IBM Director developed by IBM and available for no charge over the Web and that tracks and provides a variety of graphical views of system downtime or uptime for an individual system or group of systems, saving labor costs associated with managing and tracking server performance and availability. See 6.6.5, “System Availability” on page 393, for more information.
System Availability runs on Windows, Red Hat Linux, SUSE LINUX, and ESX Server. You can download the System Availability extension to IBM Director from:


**Free extensions from partners**

Free extensions from partners are:

- APC PowerChute Extensions for IBM Director
  
  APC PowerChute Extensions for IBM Director is a pair of extensions, one for the management server and one for the console, that allows you to manage APC uninterruptible power supplies from the IBM Director Console. For more details see 6.6.1, “APC PowerChute Extensions for IBM Director” on page 384. This free downloadable set of extensions is available from APC at:

  http://www.apc.com/tools/download/

- SteelEye LifeKeeper Protection Suite for IBM Director

  SteelEye has made available an application recovery kit built specifically to monitor and protect IBM Director Server on Windows. The LifeKeeper Protection Suite for IBM Director monitors IBM Director Server to ensure that all components are properly working and, in the event a failure is detected, will perform the necessary actions to resume management server functions on a standby IBM Director Server.

  The LifeKeeper Protection Suite for IBM Director is available to download and use for free with the default database, Apache Derby. Future versions will provide support for Oracle, DB2, and Microsoft SQL Server databases. More information is available in 4.2, “SteelEye LifeKeeper for high availability” on page 166.

  http://www.steeleye.com/partners/technology/ibm/director.html

**Fee-based extensions**

These extensions require a license, which is purchased prior to installation of the software. These extensions add significant additional functionality to the base IBM Director environment. See 1.6, “IBM Director licensing” on page 20, for more information about IBM Director licensing, including where and how to purchase licenses for these extensions.

- Capacity Manager

  Capacity Manager is a fee-based extension to IBM Director, developed by IBM, that monitors hardware resource utilization such as processor, memory, disk drives, and network traffic; identifies existing or future bottlenecks; and makes recommendations for improvement.
It also allows you to create performance analysis reports in a variety of popular formats. Its predictive, proactive capabilities help enable maximum uptime, reducing downtime costs, and its built-in, intelligent features optimize server throughput, utilization, and performance, maximizing your server investment. By predicting future server bottlenecks and proactively alerting IBM Director, automated corrective actions can be put in place to minimize downtime. See 6.7.1, “Capacity Manager” on page 399, for more information.

Capacity Manager runs on Windows, Red Hat Linux, SUSE LINUX, NetWare and ESX Server. For information about how to purchase licenses for Capacity Manager see 1.6, “IBM Director licensing” on page 20.

► Remote Deployment Manager

Remote Deployment Manager (RDM) is a fee-based extension to IBM Director that handles deployment and configuration of server and client systems. You can also use RDM to update, redeploy, and retire your systems remotely. It provides fast image restoration and deployment using its PowerRestore technology.

See 6.7.2, “Remote Deployment Manager” on page 400, for more information. In addition, a great deal of information is available at the RDM Web page: http://www.ibm.com/systems/management/director/extensions/rdm.html

► Software Distribution Premium Edition

The Software Distribution task included in the IBM Director package includes only IBM Update Assistant, which enables you to distribute to managed systems only software packages created by IBM, such as IBM Director Agent and Console upgrades and packages shipped on the UpdateXpress CD (in addition to the Update Manager task).

Software Distribution Premium Edition is a fee-based extension to IBM Director that enhances the base functionality described above by enabling you to create packages that can be distributed and installed on any managed system. Using this tool, you can create standard software packages and distribute them throughout your organization. Installation can be scheduled and unattended, enabling you to perform software upgrades on large numbers of managed systems overnight, while end users are out of the office.


► z/VM Center

The z/VM Center extension to IBM Director is specific for the virtual Linux server mainframe environment. z/VM Center provides a standardized way to deploy new z/VM virtual Linux systems through the easy-to-use IBM Director interface that does not require specific z/VM knowledge to operate. It
leverages the management access point (MAP) interface to z/VM that offers a CIM-based interface for z/VM system management functions. Its concept of virtual server templates and operating system templates allows you to repeat the creation of z/VM virtual guests and the deployment of Linux into these guests easily in a customized way. See Chapter 11, “IBM z/VM Center” on page 569, for more information.

1.6 IBM Director licensing

As with any software package, it is important to understand licensing implications to make sure all software is used according to the software’s license agreement. IBM programs are licensed under the terms and conditions of the IBM International Program License Agreement. Proofs of Entitlement (POE) are required for all authorized use.

With the introduction of IBM Director support across all IBM Systems platforms, it is important to understand which licenses are included when you purchase these systems. Simply stated, a license for all three IBM Director components (Server, Agent, and Console) is included with the purchase of all IBM System i, System p, System x, System z, and BladeCenter systems.

All Level-2 managed systems require an IBM Director Agent license. Level-0 (agentless) and Level-1 (Core Services) systems do not require an IBM Director Agent license. At the time of this writing, all Lenovo desktop and notebook systems include an IBM Director Agent license.

System x and BladeCenter systems include an additional 20 IBM Director Agent licenses for non-IBM systems. For all other non-IBM systems on which you want to install IBM Director Agent, you need to purchase an IBM Director Agent license.

**Important:** These 20 IBM Director Agent licenses for non-IBM systems are not transferable and cannot be combined. That is, they are valid only for an IBM Director Server installed on the particular hardware purchased. For example, if you buy two System x servers, but install IBM Director Server on only one of them, you are entitled to install IBM Director Agent code on 20 non-IBM systems. Even if you install IBM Director Server on both System x servers (giving you a total of 40 licenses for non-IBM managed systems), each management server is licensed to manage at most 20 of those systems, unless you purchase additional IBM Director Agent licenses.

This means that if you install IBM Director Server on a System x or BladeCenter system and use only IBM or Lenovo desktop or notebook computers, plus up to
20 computers from other vendors, then you do not need to purchase any additional IBM Director Agent licenses.

If you plan to use IBM Director to manage non-IBM systems, you should make sure that you have acquired enough IBM Director Agent licenses for these systems. Also, keep in mind that a single IBM Director Server supports up to 5,000 Level-2 systems running the full IBM Director Agent code. Once this limit is reached the management server will no longer discover or manage additional systems. An additional management server must be installed for each 5,000 Level-2 systems to be managed.

**Note:** Only Level-2 managed systems are counted against the IBM Director Server limit of 5,000 managed systems. Level-0 and Level-1 systems, as well as SNMP and RMON devices, are not counted against the Server limit.

### 1.6.1 Where to get the code

IBM Director installation media is delivered by various methods, depending on the server hardware:

- For System x and IBM BladeCenter, an IBM Director CD is shipped in the box with every system. This includes code for IBM Director Server, Agent, and Console, as well as the install-time extensions. Additional copies can be ordered under program number 5765-DIR.

- For IBM System i servers, *IBM Director for i5/OS* is shipped with every copy of i5/OS. Additional copies can be ordered using Advanced Administrative System (AAS) under program number 5722-DR1.

- For IBM System p servers, IBM Director is not shipped with systems. The IBM Director CD can be ordered for no additional charge using AAS and the eConfig tool.

- For IBM System z servers running Linux, *IBM Director for Linux on System z* can be ordered as program number 5648-DR1.

All IBM customers can download the latest version of IBM Director code from the IBM Director Software Download Matrix page:


Note that the process for ordering and the part numbers above are subject to change. For more information contact your local IBM sales representative.
1.6.2 Upgrades and maintenance

This section describes eligibility and the procedure to get updates to IBM Director.

Included licenses
The IBM Director Server and Agent licenses included with an IBM system are eligible for upgrades at no charge. This includes any IBM Server system and any IBM desktop, mobile computer, or ThinkCenter and ThinkPad systems. It also includes the 20 IBM Director Agent licenses for non-IBM systems you get with a System x or BladeCenter system.

Purchased licenses: Software Subscription Services
If you purchase any IBM Director Server or Agent license for non-IBM systems, or optional extensions, then this purchased license comes with a subscription through which you are entitled to updates for one year. You can also extend previously purchased subscriptions for non-IBM systems and optional extensions using Software Subscription Services.

Software Subscription Services is a convenient program that entitles you to receive future updates of IBM Director software that become available during their subscription period at no additional charge. You receive proactive notification of new upgrades, patches, and support information. Subscription offerings are available for IBM Director and all its fee-based extensions.

For more information about these offerings see:

1.6.3 Software support

It is important to understand that software support is not included with IBM Director. The only support that is available free of charge is an IBM Director forum, which is hosted by IBM to provide a place for System x IBM Director discussion topics. It is meant as a resource to post your System x IBM Director questions and comments, and share your thoughts, ideas, and solutions with other users. Although many IBM service and support personnel visit this forum on a regular basis, there is no guarantee that a question or issue will be addressed. This site is simply a public forum and can be reached at:


In order to ensure a response by qualified IBM support staff, you must purchase a support contract for IBM Director. Support contracts available for IBM Director
varies by server hardware. For more information contact your local IBM sales representative.

**Note**: If you have purchased multiple IBM Server platforms, the support in place for the management server platform covers the other systems in your environment. That is, if you implement IBM Director Server on a System z Linux LPAR, support for non-IBM servers running IBM Director Agent will be covered by the support contract in place that covers IBM Director on System z. Naturally, this assumes that you have purchased the proper number of IBM Director Agent licences and software support coverage for them.

### 1.7 What is new in IBM Director 5.20

IBM Director 5.20 provides a number of new features and enhancements. Several new systems have been added to the support matrix for installation and management. In addition, some functions have changed in this version and some features have been discontinued.

#### 1.7.1 Installation improvements

The following improvements have been made regarding installation.

**Express installation**

IBM Director Express is a simplified installation that installs IBM Director Server using default values for a number of installation options. The resulting management console will display a filtered task list to start with a core set of essential tasks. Additional tasks can be added to the console after installation.

**Installation checking for required drivers**

On System x servers, the installation program for IBM Director Agent automatically checks for required drivers needed for systems management and informs the user if drivers are missing.

**i5/OS**

On systems running i5/OS, IBM Director components can be installed separately from Virtualization Engine™ products by using the RSTLICPGM.

**Collection Services on AIX, Linux on POWER, and i5/OS**

Collection Services is an i5/OS application that collects interval data at the system and job levels of systems in your environment. The framework that is used to collect this data is automatically installed when you install IBM Director.
Implementing IBM Director 5.20 on AIX, Linux on POWER, or i5/OS. When installed with IBM Director, Collection Services provides a cross-partition view of processor user. For information about using Collection Services, go to:


1.7.2 General enhancements

IBM Director 5.20 has the following general enhancements.

**Update management**

The new Update Manager task provides integrated management of updates for managed systems, including new tasks for creating profiles, downloading updates, comparing updates defined in profiles against systems, and generating reports. For more on this see Chapter 7, “Update Manager” on page 411.

**User administration improvements**

IBM Director 5.20 includes the following changes affecting user administration:

- User accounts can be defined on a Lightweight Directory Access Protocol (LDAP) server, which you can use to centralize user administration for multiple management servers.
- Global or domain-local user groups can be hierarchical, with user groups including other user groups.
- User authorization for tasks is more granular, with separate authorization for parent and child tasks.
- Several new dircli commands support command-line implementation of user and group authorization tasks.

**Inventory improvements**

IBM Director 5.20 adds a new dircli command to list inventory, and expands the capabilities of the dircli mkgp command used to create dynamic groups from the command line.

Inventory collection now collects firmware information for more devices, including hard disk drives, Small Computer System Interface (SCSI) tape drives, network interface controller (NIC) adapters, and Remote Supervisor Adapter (RSA) video BIOS for many Level-0, Level-1, and Level-2 managed systems.

For AIX systems, IBM Director 5.20 provides added inventory support for adapters (FC and RAID), devices (IDE, PCI, and SCSI), memory modules, and disk storage (ISCSI, RAID, SSA, FC, virtual disks).
Monitoring of management processor logs
IBM Director 5.20 provides support for monitoring and viewing system event logs of Baseboard Management Controllers (BMCs) and Remote Supervisor Adapters (RSA II) on Level-1 managed systems. The log entries are viewed as Common Information Model (CIM) events, and the logs can be cleared automatically when they reach a threshold value.

Monitoring of i5/OS message queues
IBM Director 5.20 provides support for monitoring i5/OS message queues for specific message IDs without requiring that the message first be displayed on the IBM Director Console. A message ID can now be monitored by entering the message ID into the Event Text field of a Simple Event Filter for the applicable message queue.

Support for high availability environments
When IBM Director 5.20 is run in conjunction with a high-availability system, such as IBM Tivoli System Automation for Multiplatforms or SteelEye’s LifeKeeper, it can be run in a high availability configuration with which IBM Director Server operations can be performed by a redundant IBM Director Server instance in the event of a failure of a management server.

Upward integration module for Tivoli Management Framework
In IBM Director Version 5.20, the Software Distribution feature can be used to distribute software and perform an unattended installation of these packages on any Tivoli endpoint that is running Linux or Microsoft Windows.

IBM Virtualization Manager extension
With the IBM Virtualization Manager extension, IBM Director 5.20 provides a single point of management for both physical and virtual systems in a consistent way across different virtualization technologies. This support includes a Web-based user interface; a dashboard health summary; and a graphical topology with which you can visualize and navigate relationships between virtual and physical resources, and perform simplified virtualization tasks such as creating, deleting, modifying, and relocating virtual servers.
1.7.3 Security enhancement

IBM Director 5.20 improves security for some managed systems through Intelligent Platform Management (IPMI) 2.0 support by communicating using Enhanced Remote Management Control Protocol (RMCP+) on the following managed systems:

- IBM System x3455
- IBM System x3655
- IBM System x3755
- IBM System x3200
- IBM System x3250

1.7.4 Discontinued features in Version 5.20

The following features in previous versions of IBM Director are no longer supported. Content from previous editions of this document that refer to discontinued features has been removed from this edition.

Alert Standard Format
Support for Alert Standard Format is discontinued in Version 5.20. When IBM Director Agent is updated to Version 5.20, this function is removed. You should plan your installation appropriately and continue to use a previous version of IBM Director Agent if this function is needed.

Web-based Access
Support for Web-based Access is discontinued in Version 5.20. When IBM Director Agent is updated to Version 5.20, this function is removed. You should plan your installation appropriately and continue to use a previous version of IBM Director Agent if this function is needed.

1.8 IBM Director resources

Many sources of additional information about IBM Director are available, including the official installation and user’s guides, various IBM Service and Support offerings, and several resources on the intranet.

The IBM Director home page is:

You can download the latest IBM Director software and the IBM-developed Upward Integration Modules from:


Other systems management product downloads are available from:

1.8.1 IBM Director publications

The following publications are included in PDF format on the IBM Director installation CD-ROM:

- IBM Director Release Notes
- IBM Director Planning, Installation, and Configuration Guide
- IBM Director Express Planning, Installation, and Configuration Guide

These publications, plus the following, are available in PDF format from:
http://www.ibm.com/systems/management/director/resources

They are also available from the IBM Director Information Center:
http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/diricinfo_5.20/fqm0_main.html

- IBM Director Hardware and Software Support Guide
- IBM Director Planning, Installation, and Configuration Guide
- IBM Director Express Planning, Installation, and Configuration Guide
- IBM Director Systems Management Guide
- IBM Director Troubleshooting Guide
- IBM Director Commands Reference
- IBM Director Events Reference
- IBM Director Upward Integration Module for HP OpenView Installation and User's Guide
- IBM Director Upward Integration Module for Microsoft Systems Management Server Installation and User's Guide
- IBM Director Upward Integration Module for Microsoft Operations Manager Installation and User's Guide
- IBM Director Upward Integration Module for Tivoli Management Framework Installation and User's Guide
In addition to these documents, many IBM Director extensions have their own sets of manuals or guides. See all documents in the IBM Systems Software Information Center under Product listing in the tree view:

http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/einfo/icmain.htm

The Software Developer's Toolkit documentation is available from:

http://publib.boulder.ibm.com/infocenter/dirinfo/toolkit

In addition, the following IBM Redbooks publications are relevant:

- Virtualization on the IBM System x3950 Server, SG24-7190
- IBM eServer xSeries and BladeCenter Server Management, SG24-6495
- Integrating IBM Director with Enterprise Management Solutions, SG24-5388

You can download these books from the IBM Redbooks Web site:

http://ibm.com/redbooks

1.8.2 IBM Service and support offerings

At the time of this writing no support contract is included with any IBM Director product. Such contracts are available, but must be purchased separately from any licenses or software subscriptions already acquired. A variety of IBM Director service and support offerings are available from IBM and our business partners.

For IBM System x, BladeCenter, and non-IBM Intel processor-based systems, customers can get support in a variety of ways including the following:

- IBM Director support forum is a no-charge IBM-hosted forum staffed by IBM technical specialists familiar with IBM Director. This forum provides an excellent avenue to research IBM Director questions and to learn what others are doing with the product.
  

- Electronic Support through the IBM Support Web site is available at no charge for all IBM clients. This support is provided on a best-effort basis. To ask a question or submit a request, go to http://www.ibm.com/support and click Open a service request in the left column.

- IBM Remote Technical Support Services - ServicePac® offers hardware and software support for System x, BladeCenter, IntelliStation®, and Storage
systems. Coverage includes hardware questions as well as support for Microsoft Windows, Linux, IBM Director, VMware, and Storage Manager.

Access to answers is available 24 hours a day, 365 days a year for severity 1 problems, and Monday through Friday, 8:00 a.m. to 5:00 p.m. in your local time zone for all other questions and problems. With unlimited calls and unlimited callers, almost anyone at your company can call as often as needed and receive quick and efficient responses.

This service is conveniently packaged in ServicePac part numbers and provides the flexibility customers need for smaller environments. For more information about IBM Remote Technical Support Services, refer to:


► *IBM Operational Support Services* - *Support Line* is an annual service contract that provides unlimited calls and unlimited callers at a fixed price. The support line provides the flexibility to choose the support groups (select operating systems, software, and hardware products) that best meet your business coverage needs.

Basic support includes prime-shift coverage, defined as normal business hours, Monday through Friday, excluding national holidays. If you require support beyond prime-shift hours, IBM offers extended/full-shift coverage, available around the clock. For more information about IBM Operational Support Services - Support Line, refer to:


► *STG Lab Services for System x* is a consulting services team you can engage to help with your IBM Director implementation. Whether you are considering installing IBM Director as your first systems management tool or adding IBM Director to an existing system management environment, Lab Services for System x can help with *IBM Director JumpStart™ Implementation and Knowledge Transfer* services. In as few as two to five days, you can receive expert installation assistance and customized training to overcome obstacles with implementing IBM Director, as well as accelerate the return on investment of your IBM system purchase. For more details see:


► Many IBM Business Partners throughout the world offer services to help our customers implement IBM systems management solution. Contact your local IBM Business Partner for more information.
1.9 Features of IBM Director

IBM Director consists of an impressive suite of systems management tools that deliver strong hardware manageability. IBM Director’s industry-standard foundation enables heterogeneous hardware support and works with a variety of operating systems and network protocols.

As the sole systems management application in an environment, it can provide a complete management solution for inventorying hardware features and settings, obtaining general system information, invoking proactive systems management functions, and providing a direct link to IBM service and support Web pages. Leveraging industry standards allows for easy integration with other systems management tools and applications.

1.9.1 Capabilities

The list of capabilities provided by IBM Director is long, with a range of features including easy installation and setup, self-managing smart tools, and seamless integration into leading workgroup and enterprise systems management environments. IBM Director is based on industry standards, so you can use many of the tools it provides to manage non-IBM hardware.

The capabilities of IBM Director can be divided into the following categories:

- **Inventory**
  A critical first step in any systems management strategy is to understand exactly what hardware exists in the environment and how it is configured. IBM Director performs a thorough inventory scan of each managed system it discovers. Hundreds of hardware and software data points are collected and stored in the IBM Director database. Inventory collection can be repeated both manually and through multiple automated processes.

- **Hardware status**
  The moment you install IBM Director, it starts working to let you know about hardware problems that occur on managed IBM System x servers. If there is a problem with a power supply, fan, voltage regulator module (VRM), network interface card (NIC), or other hardware, IBM Director will let you know what the problem is and which system is affected.

- **Event management**
  At the heart of any systems management solution is the ability to alert IT staff in the event of a system problem. IBM Director provides a unique and very powerful method of alerting called event action plans, which enables you to define event triggers independently from actions that might be taken. Then simply combine these two types of items into customized plans for action and
assign them to individual or groups of managed systems. Refer to Chapter 12, “Event management” on page 675, for more information.

- **Process management**

  Using the process management task in IBM Director, you can keep track of all important processes running in your environment. IBM Director can alert you if any monitored process starts, stops, or fails to start. On managed systems running a supported Windows operating system, you can also get status from every service and device driver installed.

- **Resource management**

  Resource management is an important aspect of keeping an IT environment running at peak efficiency. It is important to know whether any given system is overloaded and not able to keep up with the workload demand. IBM Director provides the ability to monitor hundreds of system resources, set individual or group thresholds for these resources, and alert you in the event that a resource threshold has been exceeded.

- **Remote management**

  IBM Director was built to perform remote management. Any management task that can be performed on a local system can also be performed on a system thousands of miles away, provided network connectivity is available. In addition, the remote control task in IBM Director allows you to take control of any managed system in your managed environment.

- **Update management**

  The new Update Manager, introduced in IBM Director 5.20, provides update management through a native IBM Director task. Update functions include tasks for creating profiles, downloading updates, comparing updates defined in profiles against systems, and generating reports. Refer to Chapter 7, “Update Manager” on page 411, for more information.

- **Mass configuration**

  One of the advantages of managing systems using IBM Director is in its ability to make certain configuration changes on multiple managed systems at once. Even in a dynamic host control protocol (DHCP) enabled environment, many critical servers tend to use static addresses. Using Mass configuration profiles, you can, for example, change the IP address these managed systems use to locate their primary DNS server, all without having to physically visit each system. Refer to 6.4, “Mass Configuration” on page 366, for more information.

- **SNMP management**

  In addition to the sophisticated management capabilities IBM Director enables for systems running the IBM Director Agent, any SNMP device can be discovered and managed as well. IBM Director can send and receive
SNMP traps and convert these traps into native IBM Director alerts, delivering more helpful information than a raw SNMP trap normally can provide.

1.9.2 Upward integration

IBM Director can be used as a robust, standalone, yet cost-effective PC management solution. However, most corporate networks today are growing in size and diversity of systems, as are the number and criticality of the applications running on them. Not only are there multiple systems using multiple protocols, but many customers implement more than one systems management solution. IBM Director can provide specific management data to a centralized enterprise or workgroup manager so that it can be incorporated into overall management strategies. Customers can grow naturally into an overall solution that meets their systems management needs while preserving their financial and skill investments.

For more information about upward integration, refer to the IBM Redbooks publication *Integrating IBM Director with Enterprise Management Solutions*, SG24-5388, which describes how to integrate IBM Director with enterprise and workgroup managers.

1.9.3 Grouping systems

A useful feature of IBM Director Console is the ability to organize logical sets of managed systems into groups. When you select a group in the IBM Director Console, the systems that are members of that group are displayed in the Group Contents pane.

- Dynamic groups
  
  Dynamic groups are based on specified inventory or task criteria. You can create a dynamic group by specifying criteria that the attributes and properties of the managed systems must match. IBM Director Console automatically adds or removes managed systems to or from the group when their attributes and properties change to match the group criteria.
For example, you might create a dynamic group that is based on the hardware requirements Microsoft has specified for Windows Server® 2003, such as the one shown in Figure 1-3. Any managed systems that do not meet these minimum requirements would become members of this group. Through a custom query of the IBM Director hardware inventory database, you could determine easily and quickly exactly which hardware components do or do not meet the established requirement for each system in the group.

Figure 1-3   Dynamic Group: Single system fails requirements for Microsoft Windows Server 2003 upgrade
Task-based groups

The contents of a task-based group, such as the one shown in Figure 1-4, are based on the types of tasks for which a managed system is enabled. This type of dynamic group saves you time because you can initiate a specific task on all members of the group with a single drag-and-drop operation without having to consider whether each system supports that task.

Figure 1-4  Task-based group: four systems that have System Availability subagent for IBM Director
Static groups

You can specify a set of managed systems to create a static group such as the one shown in Figure 1-5. Membership in a static group is fixed unless changed by an IBM Director Console user or through an event action plan. You also can copy any dynamic group to a static group, which is a useful way to create a snapshot of managed systems based on any criteria you choose. Then later you can compare the copied static group to the dynamic group to see whether there have been any changes to group membership.

Group categories

The Group Category Editor enables you to organize large numbers of groups by creating group categories. Groups created by the Group Category Editor are static. You might use this feature to differentiate those groups used to manage systems by the IT staff at one location from those used by their colleagues at another location across the country.
Another example is to create group categories for server systems and client systems, as shown in Figure 1-6. Combining group categories with IBM Director Console security (see 3.4.4, “IBM Director Console security” on page 121) enables efficient management and reduces unnecessary clutter in the management console.

![IBM Director Console](image)

Figure 1-6  IBM Director Console: two group categories showing managed Windows clients and servers

You can export groups to archive or back up the contents of a group, or import a previously exported group in order to distribute a selected set of groups to a remote location. You can import and export only dynamic groups and task-based groups.

Refer to Chapter 2 in the product publication *IBM Director Systems Management Guide* for more information about working with groups in IBM Director.

### 1.10 This book

This book describes how to plan for and implement IBM systems management solutions primarily for Intel-based hardware using IBM Director. While its heritage is with System x and BladeCenter servers, IBM Director also supports System i, System p, and System z hardware. We give a brief overview of capabilities associated with those platforms, but focus primarily on the management of IBM System x and BladeCenter hardware. In addition, we discuss in detail the z/VM
Center extension for IBM Director (see Chapter 11, “IBM z/VM Center” on page 569, for more on this topic).

Throughout this text we describe various best practices that we have learned to apply from our own experience, as well as those of the many clients with whom we have worked. Finally, we provide example scenarios that are meant to describe how these products can be made to work together in the real world to provide a solid systems management environment.

IBM Director general planning, installation, configuration, and product usage is comprehensively covered in the publications that are provided in PDF format, either on the IBM Director CD or the online IBM Director Information Center Web site. Anyone interested in establishing an IBM Director managed environment will find the following publications particularly useful:

- *IBM Director Hardware and Software Support Guide*
- *IBM Director Planning, Installation, and Configuration Guide*
- *IBM Director Systems Management Guide*

The IBM Director Infocenter Web site is:

http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/diriminfo_5.20/fqm0_main.html

In general, we avoid duplicating these topics, describing only those steps that we believe require special attention. We highly recommend that you read these guides and have them handy while using this book, because we refer to them often.
IBM Director is a powerful and versatile systems management suite. This much functionality naturally adds a certain level of complexity, so sound planning is paramount to proper implementation of IBM Director. This chapter outlines the pre-implementation planning considerations:

- 2.1, “General considerations” on page 40
- 2.2, “Planning the requirements” on page 44
- 2.3, “User accounts” on page 45
- 2.4, “Database considerations” on page 48
- 2.5, “Express installation” on page 51
- 2.6, “Choosing the right agent” on page 51
- 2.7, “Agent installation” on page 52
- 2.8, “Discovery” on page 55
- 2.9, “Network ports” on page 57
- 2.10, “Update Manager” on page 63
- 2.11, “Software distribution” on page 64
- 2.12, “Migration and upgrading” on page 66
- 2.13, “Redundancy” on page 69
- 2.14, “Performance recommendations” on page 71
- 2.15, “Groups” on page 71
- 2.16, “IBM Director Extensions” on page 72
- 2.17, “Scheduled tasks” on page 76
- 2.18, “Changing your IBM Director infrastructure” on page 76
- 2.19, “Alerting” on page 77
2.1 General considerations

Before focusing on the various IBM Director components, think about these general considerations while planning any systems management implementation:

- **Plan for the size of your organization.**

  The intent of this book is to give valuable information for every IBM client. However, with organizations of all sizes planning to implement systems management using IBM Director, it would be impossible for us to give exact recommendations based on size of organization. Instead, we provide a basic outline and best practices that you can use to design a systems management solution that fits your company.

- **Follow the Development-Integration-Production (DIP) approach.**

  **DIP** refers to the three levels that usually must be completed before implementing new software in a corporate IT environment:

  - **Development** means the initial phase of testing and configuring. This step usually takes place in an isolated environment to avoid harming any productive systems. The development environment need not be a mirror of the productive environment.

  - **Integration** means the phase of porting a product from your development environment to your production platform. The integration environment must be a mirror of your production environment. This ensures that potential problems are identified before they can do harm to the production environment and your business.

  - **Production** refers to the IT environment you are running to support your daily business. A downtime caused by a faulty implementation can cause significant trouble. This is the reason why new and untested products, whatever they might be, should never be introduced into the production environment without going through the integration phase.

Depending on the size of the systems management infrastructure you plan to implement, going through these three steps might be too much of an investment. However, in most cases, following this approach produces much better results.

We recommend having at least a testing platform in place that incorporates development and integration into one step. This precaution is based on the architecture of Intel-based computer systems: There might be dependencies between the products you plan to implement and the ones you already run on your corporate network. Dependencies often are customer-specific and might have been discovered by the manufacturer.
The following list describes an ideal systems management development and integration platform for the implementation of IBM Director. We understand that for some scenarios, having these resources available might not be possible, so use the following list as a general guideline.

You might need to size this recommendation up or down according to your needs, the network topology (protocols, speed of the network, and so on), and other considerations such as Active Directory®.

The recommended environment for each phase is:

- Development (can be merged with integration)
  - One IBM Director Server system
  - One IBM Director Agent system for each operating system used in production
  - One IBM Director Console system
- Integration (can be merged with development)
  - One or two IBM Director Servers depending on the implementation of IBM Director (redundant or not)
  - One IBM Director Agent system for each application or function used in production (for example, one IBM Director Agent installed on a Lotus® Domino® server)
  - Network architecture close to the production LAN, especially if uncommon protocols or slow WAN connections are to be used
- Production
  - One or more IBM Director servers are performing their respective systems management tasks.
  - Numerous IBM Director Agents may be found on various operating systems and hardware platforms.
Figure 2-1 shows the development-integration-production approach to implementing IBM Director Server.

![Figure 2-1](image1.png)

*Figure 2-1  DIP approach to implementing IBM Director Server*

Figure 2-2 shows the development-integration-production approach to implementing IBM Director Agent.

![Figure 2-2](image2.png)

*Figure 2-2  DIP approach to implementing IBM Director Agent*
Figure 2-3 shows the development-integration-production approach to implementing IBM Director Console.

The approach is to:

- Keep it simple.

  This might sound strange, but the versatility of the IBM Director systems management products offers so many possibilities that you might get lost in the vast amount of tasks. Therefore try to focus on implementing the most crucial and valuable functions for your enterprise.

  In order to discern what you will have to implement and what is optional, analyze the cost of integrating a systems management component into your network with the reward you plan to get out of this feature. If cost is higher than reward, then you should consider implementing this feature at a later time.

- Integrate one function at a time.

  Try to get your systems management infrastructure up and running as fast as possible, rather than implementing every functionality in one big release.

  With IBM Director, it is a best practice to first perform a sound installation of the complete IBM Director framework that provides basic alerting in case of a hardware failure. Configuring IBM Director for more sophisticated functions such as performance management should not be your first priority.

  After you have done that, no further installation of software will be needed. (Of course, there might be service packs to apply later in the life cycle of your systems management environment.) Then you can introduce, step-by-step, additional functionality such as performance monitoring.
Introducing all functionality at once not only might delay crucial functionality, but also reduce acceptance within your organization.

- Cooperate with the important stake holders.

Most IT projects fail because of human factors, not technical challenges. Keep this in mind when implementing a systems management strategy with IBM Director as it touches various departments of your enterprise. Try to discern who is affected by this implementation (for example, the network division and the support staff) and actively communicate with them.

- Documenting your implementation.

Having properly documented planning and implementation steps will save time and frustration later. Begin planning this documentation as soon as possible. Your IBM Director environment will consist of many different systems, user IDs, passwords, files, and other details. If you plan early how and where to store this information, bringing your systems management implementation into production will be much easier.

### 2.2 Planning the requirements

The basic requirements for both the hardware-based service processors and IBM Director are described in their respective product manuals (see “Related publications” on page 945). This section discusses requirements that are not covered or that warrant further discussion.

#### 2.2.1 Network considerations for IBM Director

When planning your IBM Director implementation, keep an eye on your network design. Analyze your network and place the system running IBM Director Server in the middle of your network topology. If you use the standard Ethernet topology, this will be in the middle of a star-like architecture.

You should place IBM Director Server in the center because in the event of the failure of a network component, it will be less likely that IBM Director Server gets isolated. In a good design, this will happen only if the core router fails. If IBM Director Server gets isolated from the clients running IBM Director Agent, it will assume that all of the clients have gone offline, and send out alerts about this.

For similar reasons, you also should configure the system running IBM Director Server with a redundant path (two network cards attached to different hubs or switches) to the network.

Because IBM Director performs various tasks such as remote control or software distribution over the network, IBM Director may have an impact on the overall
network load. In typical IBM Director implementations, the network traffic is low but, depending on your planned functionality (for example, software distribution), IBM Director might increase the network traffic, possibly significantly.

In certain cases, such as remote locations, you might even consider installing a second system running IBM Director Server to work as a relay agent. This concept might apply especially if you plan to use IBM Director in large regional organizations. Planning for multiple IBM Director Server systems can drastically reduce the network load.

Software distribution options are discussed in further detail in 4.6.3, “Setting up a file distribution architecture” on page 209.

### 2.3 User accounts

IBM Director user accounts are based on user accounts created in the operating system under which the management server is installed or by authenticating through a Lightweight Directory Access Protocol (LDAP) server. When IBM Director Server is installed, two local groups are created automatically in the operating system:

- Windows: DirAdmin and DirSuper
- Other operating systems: diradmin and dirsuper

Special considerations must be given to i5/OS. These users must have a user profile on the management server that is running i5/OS and be registered in a function usage group. For more about this see the *IBM Director Planning, Installation, and Configuration Guide*.

Members of the DirAdmin (diradmin) group have general access to IBM Director as specified by their user profiles, while members of the DirSuper (dirsuper) group have superuser access (that is, full access to all IBM Director functionality, including the ability to create and edit user profiles). Access and privileges cannot be modified for any account that is a member of the DirSuper (dirsuper) group.

**Important:** Under Windows, any account with local administrator privileges on the management server is treated as though it is a member of the DirAdmin group, whether or not this is actually the case.

Under Linux, the root account is treated as though it is a member of the dirsuper group, whether or not this is actually the case.
Under Windows, the IBM Director service account is added automatically to both the DirAdmin and DirSuper groups. See 3.4.2, “IBM Director service account” on page 120, for more information and recommendations regarding the IBM Director service account. Under other operating systems, the diradmin and dirstuper groups are not populated automatically. A user with root privileges must assign users to the appropriate groups.

**Important:** In IBM Director, the default user access is fully restricted rather than being wide open as in previous releases. This means that although accounts added to the DirAdmin (diradmin) group will be able to log on, they will see a blank management console and will not be able to perform any actions until a superuser (member of DirSuper/dirstuper) configures privileges and access rights for these accounts.

### 2.3.1 LDAP support

Starting with Version 5.20, IBM Director can authenticate user login requests against a Lightweight Directory Access Protocol (LDAP) server.

LDAP is an open protocol that uses TCP/IP to provide access to directory services and perform user authentication. Using LDAP for IBM Director user authentication has the following advantages:

- Many organizations already have existing LDAP directories that can be used for IBM Director user authentication. This saves the time and effort required to create user accounts on management servers.
- User access can be immediately modified or terminated on all instances of IBM Director Server by changing the user’s LDAP group memberships.
- Users only need a single ID and password, which can centralize user administration for multiple management servers.

**Note:** LDAP administrators should note that IBM Director determines group membership using only the *members* attribute of the group entry. IBM Director ignores other methods of specifying group membership, including attributes (such as memberOf) on user entries.

**LDAP considerations**

Before deploying IBM Director, you should determine what IBM Director user roles to define for your organization. In addition, you should determine the user authentication type that will best meet your needs.
Decide what kind of user authentication to use for IBM Director:

- LDAP server
- Using accounts on the operating system of the management server

With LDAP authentication, it is easy to implement common roles and access for users across multiple instances of IBM Director Server. However, the LDAP server must be secure in order to avoid unauthorized access to management tasks and managed objects in IBM Director.

Consider how IBM Director will be used to manage systems and objects in various locations:

- How many users will be authorized to access IBM Director?
- Will a single management server be used for the entire organization, or will multiple management servers be used?
- If multiple management servers will be used, will the same user accounts be needed on more than one of the management servers, or should user accounts be unique for each management server?
- Is there an existing LDAP directory, such as IBM Directory Server or Microsoft Active Directory, for your organization?

Refer to 3.2, “LDAP” on page 102, for more details on LDAP support.

### 2.3.2 Active Directory Global Groups

IBM Director has the ability to add existing Active Directory Global Groups (ADGGs) to the DirAdmin or DirSuper local groups on the management server and delegate access based on these ADGGs. Using this method you can easily apply your current Active Directory group strategy to reflect access to IBM Director.

An example would be to have an ADGG called _Helpdesk New York_. You could add this group to DirAdmin and customize access to the management console such that member accounts would only be able to manage desktops at the New York location. Any new Active Directory users added to the ADGG _Helpdesk New York_ would automatically get the proper access to IBM Director Console.

Refer to 3.4.4, “IBM Director Console security” on page 121, for more information about setting security levels for the management console. Refer to “Active Directory Global Group support” on page 116 for more details on the implementation of ADGG support.
2.4 Database considerations

IBM Director stores all inventory in a database. Before you install the IBM Director Server, you should decide which database you want to use.

IBM Director Servers support several databases on several platforms. Depending on your current environment, select the best platform for your database:

- **Linux (System x, System p, System z)**
  - Apache Derby (included with IBM Director) (local install only)
  - IBM DB2
  - Microsoft SQL Server (remote install only)
  - Oracle
  - PostgreSQL

- **Windows**
  - Apache Derby (included with IBM Director) (local install only)
  - IBM DB2
  - Microsoft SQL Server 2000
  - Microsoft SQL Server 2000 Desktop Engine (MSDE) (local install only)
  - Microsoft SQL Server 2005
  - Microsoft SQL Server 2005 Express Edition (local install only)
  - Oracle
  - Microsoft Jet (upgrades only; cannot be selected for new installations)

- **AIX:**
  - Apache Derby (included with IBM Director) (local install only)
  - IBM DB2
  - Oracle

- **i5/OS**
  - IBM DB2 (local install only)

See Chapter 2 of the publication *IBM Director Planning, Installation, and Configuration Guide* for details of specific version numbers supported.

**Tip:** When IBM Director Server is configured in High Availability mode, we recommend that you use a supported remote database instead of the embedded Apache Derby database. The database should be configured for high availability, as described in the database documentation.

If you already have existing database licenses, you may want to keep your existing database technology and use IBM Director with that.
Apache Derby is now the default IBM Director database that is bundled with the product. It is supported on all operating systems on which IBM Director Server can be installed with the exception of i5/OS, where the database must be DB2.

The Apache Derby database is a pure open source Java relational database engine, with zero administration and a small memory footprint. Although Apache Derby is a full functional relational database, the version IBM Director uses is an embedded version with limited functionality. This means that none of the tools available for Apache Derby are supported with IBM Director.

**Note:** The Microsoft Jet database will still be supported, but only for upgrade of an existing IBM Director installation.

Full database installation instructions are described in Chapter 3 of the product publication *IBM Director Planning, Installation, and Configuration Guide*.

Although you can install and use IBM Director without the use of a database, the best practice is to always install IBM Director with at least the default Apache Derby database. IBM Director Server uses the database to store inventory information in a central point. This inventory information can then be used for managing your assets, for example. IBM Director also uses the inventory data for many of its advanced features. The features of IBM Director that depend on a database include:

- Inventory
- Dynamic groups creation
- Asset ID™
- Capacity Manager
- Electronic Service Agent
- System availability
Figure 2-4 is a flow chart to help you decide whether you need to install a database or use a database other than the default Apache Derby database.

In addition, you will need to decide whether to use a local database (installed on the same server as IBM Director Server) or a remote database (installed on a different machine than the one running IBM Director Server).

Both implementations have their advantages and disadvantages. A local database server offers better ease of use. Connectivity and security are simpler. Additionally, you have no dependencies (for example, you would not have to contact the database department to change the database settings), and a separate server is not required for housing the database. On the other hand, you must plan backup carefully, because you would have a single point of failure with the database and application server residing on the same machine. Also, the system needs more memory to maintain the database server.

The advantage of using a remote database is if you already have a consolidated database infrastructure and want to reuse your current environment.
2.5 Express installation

New in IBM Director 5.20 is the option to perform an express installation of the management server. IBM Director Express is a simplified installation that installs IBM Director Server using default values for a number of installation options. The resulting management console will display a filtered task list to start with a core set of essential tasks.

IBM Director Express is intended to provide a simplified installation mechanism and management console for those customers needing to manage a small IT infrastructure. It is also suitable for those who are interested in getting up and running with IBM Director as quickly as possible, allowing for additional functionality to be added after initial installation.

**Important:** Installing IBM Director using the *standard* installation method enables users with local administrative rights to log on to the management server. However, user access is fully restricted and users will be unable to access any groups or tasks until they are granted access by an IBM Director user administrator or they are a member of the DirSuper group.

Installing IBM Director using the *express* installation method enables users with local administrative rights to log on to the management server. However, unlike the standard installation, users access is *unrestricted* and users can access all groups and tasks and perform user administration. Users do not need to belong to the IBM Director groups DirAdmin or DirSuper.

For more information refer to 4.1, “Express installation” on page 150.

2.6 Choosing the right agent

There are three levels of the agent that are used to categorize managed systems:

- Level-0 (Agentless): no IBM Director components installed; limited functionality
- Level-1 (Core Services): IBM Director Core Services installed; additional functionality
- Level-2 (IBM Director Agent): full IBM Director Agent installed; full management of object

Depending on the type of managed object and the management tasks you want to perform, you must decide which agent to install. See 6.1, “Tasks by agent level” on page 282, for a summary of IBM Director tasks by agent level.
Choose Level-0 if:
- You do not want to install additional software on the system.
- You do not require any functionality such as the ones provided by Level-1 or 2.
- You want to be able to restart the server.
- You want to be able to create a remote session to the system (Linux only).
- You want to upgrade easily to a Level-1 or Level-2 Agent.
- You do not have an IBM Director Agent license.
- Your system is already memory constrained.

Choose to install IBM Director Core Services (Level-1) if:
- You want to get hardware status (IBM systems only).
- You want to use record events in the event log.
- You want to use event action plans.
- Your system is already memory constrained.
- You already have a supported workgroup or enterprise management agent installed.

Choose to install IBM Director Agent (Level-2) if:
- You have systems that do not use TCP/IP.
- You want to remote control your systems (Windows only).
- You want to use Capacity Manager.
- You want to use Electronic Service Agent (Linux and Windows).
- You want to use ServeRAID Manager.
- You want to use System Availability.
- You want to use IBM Virtualization Manager (Linux, Windows, and Xen).
- You want to use Asset ID.
- You want to use the CIM Browser.
- You want to use File Transfer.

2.7 Agent installation

With IBM Director 5.x, there are three types of supported agents, but since one of them is agentless (without any agent installed), we are only concerned with installing the other two agents:
- Core Services (Level-1)
- Full IBM Director Agent (Level-2)
The procedure to install these agents is basically the same; only the files, packages and response files are different.

The new installation method is the option of discovering a system as a Level-0 agent, and using the Software Distribution task to install the agent onto the server.

You can install IBM Director Agent or Core Services to your client systems in several ways, depending on your current software deployment and installation strategy and the operating systems on which you will install IBM Director Agent.

**Important:** Before installing IBM Director Agent on a System x server or IBM blade server, you must first install the system management processor drivers. If you do not install the driver, you will not have in-band access to the service processor on that system.

IBM Director setup will display a warning if a systems management processor is detected, but the IPMI or RSA II driver is not installed. Refer to 4.4.3, “Driver installation” on page 181, for more information.

The choices for installation are:

- **Manual installation (all operating systems)**

  Manual installation is the basic method of installing IBM Director. The source can be the IBM Director CD shipped with your system or a network file share. Either way, you will perform the installation process manually.

  While this method of deployment makes sense in development scenarios or in smaller or specialized scenarios, it is too much manual work for larger installations. If you plan to install IBM Director Agent on more than 20 systems, you may want to use one of the other deployment methods.

- **Cloned installation (mostly Windows systems)**

  Cloned installations are not pure IBM Director Agent installations. A cloned installation refers to cloning a system using a tool such as Symantec Ghost or DeployCenter. For ease of installation, the source system used to generate the clone image should have IBM Director Agent already installed.

  Due to the nature of cloning, only new systems can use this method of deploying IBM Director Agent. Cloning an IBM Director Agent system can cause some problems related to the identification mechanism used by the management server.

**Important:** Before cloning a system with IBM Director Agent installed, read 4.6.2, “IBM Director Agent and cloning” on page 206.
Remote Deployment Manager (RDM) is a fee-based extension to IBM Director that enables you to perform a native (unattended) operating system install or create an image (clone) of an entire donor system. With RDM you can clone a system that includes IBM Director Agent, then distribute these images from IBM Director Console to any system in your network. For more information about RDM go to:


Installation using Software Distribution task (Windows and Linux)

For systems already up and running, you can use the Software Distribution task to install the agent unattended. As long as the systems have been discovered, you can push the agent to the systems. This includes systems that do not already have IBM Director Agent installed (agentless or Level-0 systems).

Using the Software Distribution task is also the preferred method when upgrading from a previous version.

See 2.11, “Software distribution” on page 64, for more information about software distribution, and 13.2, “Automated IBM Director Agent promotion” on page 776, for a comprehensive discussion of promoting systems from one level of support to a higher level.

Unattended installation (Windows)

The IBM Director Agent installation routine supports the use of answer files for the unattended installation of the software. This enables you to run a silent installation that requires no user input. This way of deploying the IBM Director Agent will probably suit most demands and deployment strategies.

An advantage of this deployment method is that it can be used equally in new installations (for example, as a RunOnce command in a Windows 2000 unattended installation) and in existing installations (such as running a batch file that launches the installation).

The process of implementing a unattended installation is described in 4.6.1, “Unattended installation of IBM Director Agent for Windows” on page 201.

Windows Installer and other software distribution suites (Windows and NetWare)

The installation routine for IBM Director is based on InstallShield, so you can install the IBM Director Agent using the Windows Installer Service (Microsoft Installer or MSI) or any other software distribution suite that is compatible with InstallShield, such as ZEN for Servers in a NetWare environment.

This way of distributing IBM Director Agent is most suited to environments where a software distribution suite is already in use. We recommend using
this deployment methodology in environments where you plan to distribute the IBM Director Agent software to desktop computer systems that already use a software deployment suite.

- **Scripted installation (Linux, AIX)**
  
The easiest way to install the IBM Director Agent on multiple Linux-based systems is to use an installation script. Installation scripts are easy to create and, compared to unattended script files for Windows-based machines, Linux scripts pay off when planning to install as few as five systems.

- **Scripted Installation (NetWare)**
  
Due to the architecture of NetWare, you can easily copy an initial installation of an IBM Director Agent to multiple systems. After copying the IBM Director code, run a simple batch file to make the necessary changes and registrations. This is a very simple and fast way to deploy the IBM Director Agent onto your NetWare servers.

### 2.8 Discovery

Before a system can be managed by IBM Director, it first must be discovered by IBM Director Server. By default, automatic discovery is disabled for all systems. During discovery, the management server searches for systems running. The management server then stores those systems’ IP addresses and adds them to the management console.

To discover managed systems, IBM Director can use either push or pull algorithms. Depending on the complexity of your network, you should spend some time planning how your managed systems will be discovered.

You will need detailed information about the layout of your network, especially the information about subnets and VLANs. We also suggest that you plan the discovery method used by IBM Director with your network staff to ensure that no unwanted side effects (for example, high unicast traffic) occur.

The different discovery methods are discussed in the following sections.

#### 2.8.1 Agent-initiated discovery

The term *agent-initiated discovery* in IBM Director refers to managed systems contacting the IBM Director Server rather than IBM Director Server searching for managed systems. This is a push-based discovery. This implementation has several advantages. First, no matter how complicated your network might be (if you implement VLANs, for example), an agent-initiated discovery will always succeed as long as there is a TCP/IP connection from the management server to
the managed systems. Also, compared to a server-initiated discovery, the network traffic due to discovery requests will be negligible.

The three available agent-initiated discovery algorithms are:

- Using the Add known server entry in a unattended installation of IBM Director. For detailed information about unattended installation of the IBM Director Agent, refer to 4.6.1, “Unattended installation of IBM Director Agent for Windows” on page 201.

- Using a batch file with the genevent command that sends an event to the management server with the managed system’s name and IP address. For detailed information about genevent, refer to “Checking the communication using genevent” on page 220.

- Receiving an SNMP trap from a device. IBM Director can be configured to discover and manage any device from which it receives an SNMP trap. For detailed information about SNMP configuration, refer to 5.4, “SNMP configuration” on page 250.

### 2.8.2 Server-initiated discovery

The term server-initiated discovery refers to IBM Director Server searching the network for systems. Normally, this is referred to simply as discovery. The big advantage of this solution is ease of configuration: you simply enter the discovery settings once at the management server. IBM Director offers five ways to do server-initiated discovery:

- **Broadcast discovery**
  
  Broadcast discovery performs a broadcast in a specified subnet. Generally the subnet will be the one where the management server is installed, but you can also send broadcasts to other subnets if broadcasts are not filtered by your network infrastructure. (By default most gateways will not permit broadcasts to pass over subnets.)

- **Multicast discovery**
  
  A multicast discovery sends a request to the standard multicast address 224.0.1.118 and waits for reply from Level-1 and Level-2 agents in reach (as defined by the TTL of the packet). If your network infrastructure filters broadcast requests (most of them will) but not multicast requests, consider this method.

- **Unicast discovery**
  
  Unicast discovery enables you to specify an exact address or a range of addresses. Each address will be contacted individually. You may want to use this discovery method if your network filters both broadcast and multicast
requests. The disadvantage of an unicast discovery is that an IP packet must be sent for each individual IP address, increasing network traffic.

- **Broadcast relay agents**

  By using a broadcast relay agent you can avoid the disadvantages of a broadcast discovery. The only thing you will need is one Level-2 agent per subnet. IBM Director will then contact these systems in order to perform a broadcast within their respective subnet. Only Level-2 agents will reply directly to the management server.

- **Service Location Protocol Discovery**

  SLP discovery is used for discovering Level-1 systems. Refer to 1.4.5, “Service Location Protocol” on page 7 for more about SLP.

Depending on the layout of your network you might want to consider different approaches. Server-initiated discovery is described in more detail in 5.2, “IBM Director discovery” on page 229.

### 2.9 Network ports

Table 2-1 lists the ports used by IBM Director components to communicate with one another and IBM service processors. Depending on which components are installed and which functionality is required, the proper ports must be open and available. For more on configuring software firewalls to accommodate IBM Director management, see 5.2.1, “Firewalls” on page 230.

<table>
<thead>
<tr>
<th>Category</th>
<th>Connection</th>
<th>Destination port</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Director interprocess</td>
<td>IBM Director Server &lt;&gt; IBM Director Agent</td>
<td>14247 UDP and TCP&lt;sup&gt;1&lt;/sup&gt;, 14248 TCP, 4490 IPX™ (read), 4491 IPX (write)</td>
</tr>
<tr>
<td>communication</td>
<td>IBM Director Console &gt; IBM Director Server</td>
<td>2033 TCP</td>
</tr>
<tr>
<td></td>
<td>DIRCLI client &lt;&gt; IBM Director Server</td>
<td>2044 TCP</td>
</tr>
<tr>
<td></td>
<td>DIRCMD client &lt;&gt; IBM Director Server</td>
<td>2034 TCP</td>
</tr>
<tr>
<td></td>
<td>IBM Director Console &gt; IBM Director Console</td>
<td>Any free port (for use of BladeCenter Switch Management launch pad)</td>
</tr>
<tr>
<td></td>
<td>IBM Director Console &gt; IBM Director Server over SSL; DIRCLI client &lt;&gt; IBM Director Server</td>
<td>4066 TCP</td>
</tr>
<tr>
<td>Category</td>
<td>Connection</td>
<td>Destination port</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IBM Director Web-based Access</td>
<td>Web Browser &gt; IBM Director Agent Web Server</td>
<td>411 TCP (HTTP) Configurable at installation&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>Web Browser &gt; IBM Director Agent Web Server</td>
<td>423 TCP (HTTPS) Configurable at installation&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>IBM Director Agent Web Server &gt; IBM Director Agent Web Server</td>
<td>8009 TCP (loopback)</td>
</tr>
<tr>
<td>CIM-XML over HTTP&lt;sup&gt;3&lt;/sup&gt;</td>
<td>IBM Director Server &gt; Level-1 or Level-2 managed system, or SMI-S storage device</td>
<td>5988 TCP 15988 TCP (SUSE Linux and Red Hat Linux for System z)</td>
</tr>
<tr>
<td>CIM-XML over HTTPS&lt;sup&gt;3&lt;/sup&gt;</td>
<td>IBM Director Server &gt; Level-1 or Level-2 managed system, or SMI-S storage device</td>
<td>5989 TCP 15988 TCP (SUSE Linux and Red Hat Linux for System z)</td>
</tr>
<tr>
<td>HTTP</td>
<td>IBM Director Server &gt; BladeCenter switch module</td>
<td>80 TCP</td>
</tr>
<tr>
<td>Microsoft Windows DCOM</td>
<td>IBM Director Server &gt; Level-0 system</td>
<td>137 UDP, 138 UDP, 139 TCP, 445 TCP</td>
</tr>
<tr>
<td>ServeRAID interprocess communication</td>
<td>ServeRAID CIM Provider &gt; ServeRAID Manager</td>
<td>34572 TCP</td>
</tr>
<tr>
<td>Service processors</td>
<td>IBM Director Server &lt;&gt; service processor</td>
<td>6090 TCP</td>
</tr>
<tr>
<td></td>
<td>Service processor &gt; IBM Director Server (alerts)</td>
<td>13991 UDP</td>
</tr>
<tr>
<td></td>
<td>IBM Director Server &gt; service processor (ASF, ASF 2.0, and IPMI)</td>
<td>623 and 664 UDP</td>
</tr>
<tr>
<td></td>
<td>Service processor &gt; IBM Director Server (ASF, ASF 2.0, and IPMI)</td>
<td>Random port in the 1024-65535 range&lt;sup&gt;4&lt;/sup&gt;</td>
</tr>
<tr>
<td>SLP</td>
<td>IBM Director Server &lt;&gt; SLP service agents or SLP directory agents</td>
<td>427 TCP and UDP</td>
</tr>
<tr>
<td>SNMP</td>
<td>IBM Director Server &gt; SNMP agent</td>
<td>161 TCP and UDP&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td></td>
<td>SNMP agent &gt; IBM Director Server</td>
<td>162 TCP and UDP&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td>SSH</td>
<td>IBM Director Server &gt; SNMP devices (Remote Session task)</td>
<td>22 TCP</td>
</tr>
<tr>
<td></td>
<td>IBM Director Server &gt; Level-0 system</td>
<td>22 TCP</td>
</tr>
</tbody>
</table>
In the Connection column, the component to the left of the arrows indicates the initiator of the communication and the component to the right of the arrow indicates the listener or receiver of the communication.

For the TCP ports listed, the initiator opens a random port in the 1024-65535 range and then connects to the listener on the port listed in the Destination Port column. When the listener responds, it connects back to the random port in the 1024-65535 range opened by the initiator. For example, if the entry in the Connection column is IBM Director Console > IBM Director Server, then IBM Director Console is the initiator and IBM Director Server is the listener.

### 2.9.1 Ports used by Remote Supervisor Adapter II

As well as communicating in-band to the RSA II using IBM Director Agent and the service processor device driver, you can also communicate out-of-band directly to the RSA II. Table 2-2 and Table 2-3 on page 60 list all of the ports used by the RSA II, some of which are fixed and some of which can be changed.

#### Table 2-2  User configurable TCP/IP ports used by the RSA II

<table>
<thead>
<tr>
<th>Port name</th>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http</td>
<td>80 (default)</td>
<td>Web server HTTP connection - TCP</td>
</tr>
<tr>
<td>https</td>
<td>443 (default)</td>
<td>SSL connection - TCP</td>
</tr>
<tr>
<td>telnet</td>
<td>23 (default)</td>
<td>Telnet command-line interface connection - TCP</td>
</tr>
</tbody>
</table>
Some other ports are fixed and cannot be changed.

Table 2-3  Fixed TCP/IP ports used by the RSA II

<table>
<thead>
<tr>
<th>Port name</th>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>22 (default)</td>
<td>Secure Shell (SSH) command-line interface - TCP</td>
</tr>
<tr>
<td>SNMP Agent</td>
<td>161 (default)</td>
<td>SNMP get/set commands - UDP</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>162 (default)</td>
<td>SNMP traps - UDP</td>
</tr>
</tbody>
</table>

2.9.2 Ports used by the BMC

The BMC service processor on System x servers also uses several TCP/UDP ports for communication (Table 2-4).

Table 2-4  TCP/IP ports used by the BMC

<table>
<thead>
<tr>
<th>Port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>623</td>
<td>IPMI communications to SMBridge and IBM Director</td>
</tr>
<tr>
<td>664</td>
<td>IPMI communications (secondary)</td>
</tr>
<tr>
<td>161</td>
<td>SNMP get/set commands</td>
</tr>
<tr>
<td>162</td>
<td>SNMP traps and PET alerts to Director</td>
</tr>
</tbody>
</table>
2.9.3 Ports used by the Advanced Management Module

The BladeCenter Advanced Management Module uses the TCP/UDP ports listed in Table 2-5 for communication.

Table 2-5 User-configurable Advanced Management Module ports

<table>
<thead>
<tr>
<th>Port name</th>
<th>Default port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http</td>
<td>80</td>
<td>Web server HTTP connection - TCP</td>
</tr>
<tr>
<td>https</td>
<td>443</td>
<td>SSL connection - TCP</td>
</tr>
<tr>
<td>telnet</td>
<td>23</td>
<td>Telnet command-line interface - TCP</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
<td>SSH command-line interface - TCP</td>
</tr>
<tr>
<td>SNMP Agent</td>
<td>161</td>
<td>SNMP get/set commands - UDP</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>162</td>
<td>SNMP traps - UDP</td>
</tr>
<tr>
<td>FTP</td>
<td>21</td>
<td>Listen port for the FTP server - TCP</td>
</tr>
<tr>
<td>FTP data</td>
<td>20</td>
<td>FTP data port - TCP</td>
</tr>
<tr>
<td>TFTP</td>
<td>69</td>
<td>TFTP server - TCP</td>
</tr>
<tr>
<td>Remote disk</td>
<td>1044</td>
<td>Remote disk function - TCP</td>
</tr>
<tr>
<td>Remote disk on-card</td>
<td>1045</td>
<td>Persistent remote disk (disk on card) - TCP</td>
</tr>
<tr>
<td>Remote KVM</td>
<td>3900</td>
<td>Remote Console - TCP</td>
</tr>
</tbody>
</table>

The ports listed in Table 2-6 are fixed. You cannot change them.

Table 2-6 Fixed Advanced Management Module ports

<table>
<thead>
<tr>
<th>Fixed port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>e-Mail alerts - TCP</td>
</tr>
<tr>
<td>53</td>
<td>UDP Domain Name Server (DNS) resolver - UDP</td>
</tr>
<tr>
<td>68</td>
<td>DHCP client connection - UDP</td>
</tr>
<tr>
<td>427</td>
<td>Service Location Protocol (SLP) connection - UDP</td>
</tr>
<tr>
<td>6090</td>
<td>IBM Director commands - TCP</td>
</tr>
<tr>
<td>13991</td>
<td>IBM Director alerts - UDP</td>
</tr>
</tbody>
</table>
2.9.4 Ports used by the Management Module

The BladeCenter Management Module uses the TCP/UDP ports listed in Table 2-7 for communication.

Table 2-7 User-configurable Management Module ports

<table>
<thead>
<tr>
<th>Port name</th>
<th>Default port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http</td>
<td>80</td>
<td>Web server HTTP connection - TCP</td>
</tr>
<tr>
<td>https</td>
<td>443</td>
<td>SSL connection - TCP</td>
</tr>
<tr>
<td>telnet</td>
<td>23</td>
<td>Telnet command-line interface connection - TCP</td>
</tr>
<tr>
<td>SSH</td>
<td>22</td>
<td>Secure Shell (SSH) command-line interface - TCP</td>
</tr>
<tr>
<td>SNMP Agent</td>
<td>161</td>
<td>SNMP get/set commands - UDP</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>162</td>
<td>SNMP traps - UDP</td>
</tr>
</tbody>
</table>

The ports listed in Table 2-8 are fixed. You cannot change them.

Table 2-8 Fixed Management Module ports

<table>
<thead>
<tr>
<th>Fixed port number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>e-Mail alerts - TCP</td>
</tr>
<tr>
<td>53</td>
<td>UDP Domain Name Server (DNS) resolver - UDP</td>
</tr>
<tr>
<td>68</td>
<td>DHCP client connection - UDP</td>
</tr>
<tr>
<td>427</td>
<td>Service Location Protocol (SLP) connection - UDP</td>
</tr>
<tr>
<td>1044</td>
<td>Remote disk function - TCP</td>
</tr>
<tr>
<td>1045</td>
<td>Persistent remote disk (disk on card) - TCP</td>
</tr>
<tr>
<td>5900</td>
<td>Remote Console - TCP</td>
</tr>
<tr>
<td>6090</td>
<td>IBM Director commands - TCP</td>
</tr>
<tr>
<td>13991</td>
<td>IBM Director alerts - UDP</td>
</tr>
</tbody>
</table>
2.10 Update Manager

The Update Manager task provides integrated management of updates for IBM System x and IBM BladeCenter systems. Update Manager includes new tasks for creating profiles, downloading updates, comparing updates defined in profiles against systems, and generating reports.

Update Manager uses profiles to manage system updates. Profiles can be created for individual updates or for update bundles (UpdateXpress System Packs). You use profiles to specify criteria that determine compliance reports and generate Software Distribution tasks. Using profiles, you can also determine which systems in your IBM Director environment are out-of-date and use IBM Director Software Distribution to distribute the system software and firmware.

We cover Update Manager in detail in Chapter 7, “Update Manager” on page 411.

2.10.1 Comparing to Update Assistant

Update Assistant is still available in IBM Director and is useful for importing updates from media such as UpdateXpress CDs or downloaded packages from the Web.

Update Assistant can provide advantages over Update Manager in the following scenarios:

- Your Director Management server does not have access to the Internet.
- You have new managed systems that are not currently supported by Update Manager or have no available updates.
- You wish to manually control what updates are downloaded.
- You already have the latest updates on CD or other media.
- Newer or critical updates are available on the IBM support Web site, which are not in available in Update Manager.
- You have standardized firmware and drivers that are supported by your organization and you do not want to download or use the newer updates that may be available through Update Manager.

2.10.2 UpdateXpress System Pack

An UpdateXpress System Pack is an integration-tested bundle of online firmware and driver updates for IBM System x and IBM BladeCenter servers for a specific operating system.
UpdateXpress System Packs simplify the downloading and installation of all
driver and firmware updates for a given system, ensuring that you are always
working with a complete, current set of updates that have been tested together
and bundled by IBM.

**Note:** Some BladeCenter updates can be distributed over an out-of-band
(OOB) path through the management module of the BladeCenter chassis. The
OOB distribution method has no requirements on the operating system or
installed applications.

### 2.10.3 Update Manager considerations

We suggest that you take the following points into account:

- Location for updates (Updates Library) on the IBM Director Server
- Maximum download size per request (downloaded profile)
- Scheduling of downloads to minimize network traffic
- Scheduling of updates to maintain core operational services
- Internet connection method to access IBM updates, direct or via an HTTP
  Proxy

**Important:** The Update Manager task only supports vasic authentication with
proxy servers. If Digest or NTLM authentication are required, Update Manager
will be unable to access update packages from IBM.

### 2.11 Software distribution

The Software Distribution task that is included with the base installation of IBM
Director is limited to distribution of IBM-provided packages. These packages can
be found on UpdateXpress CDs, the IBM Director installation CD, and Web
downloads of many system BIOS, firmware, and driver installers (look for the
presence of an XML file). Also, IBM Director Agent, IBM Director extensions, and
IBM Director service packs are available for import using IBM Update Assistant.
IBM Director Software Distribution can distribute software packages to Level-0, Level-1, and Level-2 systems. Refer to Table 2-9 for limitations.

Table 2-9  Software distribution for Level-0, Level-1 and Level-2 systems

<table>
<thead>
<tr>
<th>Agent type</th>
<th>Software distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level-0</td>
<td>Only one software package can be distributed to non Level-2 systems at any time. Updates are performed consecutively.</td>
</tr>
<tr>
<td>Level-1</td>
<td>Software packages can be distributed to multiple Level-2 systems simultaneously. Updates are performed concurrently.</td>
</tr>
<tr>
<td>Level-2</td>
<td></td>
</tr>
</tbody>
</table>

For more details about IBM Update Assistant and the types of packages it is able to import, see 6.3.19, “Software Distribution (base)” on page 352.

If you plan to use software distribution, we recommend that you plan each of your software distribution scenarios. Depending on the size and complexity of your network, implementing unplanned software distribution may have serious implications to network traffic.

We suggest that you take the following points into account:

- IBM Director can distribute software or files by two methods:
  - Streaming directly from IBM Director Server
  - Redirected distribution with file servers

The advantages of the streaming technology are that it is easy to configure, and it includes a resume function in case the network connection should fail. However, in large environments, streaming from one central management server can significantly affect network performance (for example, when you distribute software packages over a WAN link). This is where you might want to use a redirected distribution.

The advantage of redirected distributions is that file servers can be placed in any subnet or branch office and feed the systems close to them with software. This is a big advantage, especially in huge IBM Director implementations, as you will not jam WAN links but still you will be able to control and schedule any software distribution from your central management server.

The downside of using file servers for a redirected distribution is that in case of a network failure you will have to start over, and setting up file servers and shares is more complex.

- If you decide to use redirected distribution, plan the use of file servers carefully. Ideally, software distribution servers should be placed according to your network topology. Identify areas of good network connection and draw...
them as logical units (such as branch offices or isolated subnets). Ideally, you should have at least one distribution share per logical unit.

- Plan your software distribution schedules carefully. While distributing software, firmware and driver updates, or IBM Director fixes you should not run any other software that is disk-intensive or network-intensive.

For details about implementing a software distribution solution, see 4.6.3, “Setting up a file distribution architecture” on page 209.

2.12 Migration and upgrading

If you already have a systems management environment in place (for example, an earlier version of IBM Director), this section provides the necessary information about migrating to IBM Director 5.x.

2.12.1 Upgrading from earlier versions

If you upgrade from earlier versions of IBM Director, consider these facts when planning the upgrade:

- IBM Director 5.20 only supports upgrading of IBM Director Agent from Versions 4.x and 5.x. Such upgrades can only be to the full IBM Director Agent (Level-2 system). Upgrading to IBM Director Core Services (Level-1 system) is not supported.

- IBM Director 5.x does not support all operating systems supported in IBM Director 4.x (for example, Microsoft Windows NT® 4.0 and Novell NetWare 5.x), but does support managing IBM Director 4.x Agents, so you may want to keep your IBM Director 4.x agents on these systems.

Upgrading of the IBM Director components is as follows:

- Upgrading IBM Director Server
  If you are currently using IBM Director 3.x, you cannot install IBM Director 5.x over the top of the existing installation. You must manually uninstall the previous version, then install the current version. Furthermore, we recommend that you uninstall the management server and do a clean installation of the current version. If you are reinstalling, remember to document all settings before uninstalling. These include:
  - Dynamic group definitions
  - Discovery preferences
  - IBM Director user rights
– Event action plans and the systems to which they are applied

- Upgrading IBM Director Console

If you upgrade IBM Director Server, you must also upgrade all IBM Director Console installations that will connect to the new management server, since the versions of the console and the server must match. We recommend that you uninstall the previous version, then install the current version of IBM Director Console on all appropriate systems. This can be scripted for mass rollouts.

- Upgrading IBM Director Agent

Upgrading a system running a previous version of IBM Director Agent to the current version can involve several steps. The prerequisites for IBM Director Agent 5.x have changed, including the list of supported operating systems. You should evaluate the need for upgrading the management agents as well as ensure support of the current version on any given managed system.

Remember that IBM Director Server 5.x supports IBM Director Agents 4.x, so you can upgrade your IBM Director Server system first. Then, in a second step, proceed with an upgrade of your managed systems.

**Important:** The Server Plus Pack for IBM Director 4.x has been discontinued and is no longer available. For more information about steps necessary to upgrade to IBM Director 5.x if these extensions are already installed, see 4.3, “Server Plus Pack considerations” on page 177.
Use the flowchart in Figure 2-5 to determine the implications of your IBM Director Agent upgrade.

![Flowchart](image)

**Figure 2-5 Decision criteria for upgrading IBM Director Agent systems**

### 2.12.2 Migration from Insight Manager

There are two ways to migrate from a systems management environment that uses HP Systems Insight Manager:

- Leave the systems using Insight Manager as is and integrate them using their native SNMP protocol into IBM Director. IBM Director Server will be able to detect and group these systems as Level-0 systems.

  IBM Director will be able to receive and filter all alerts sent by the Insight Manager systems. However, you will not be able to make use of the advanced functionality of IBM Director, such as process management.

  This method is preferred if you have a functioning environment of Insight Manager systems and you just want alerting sent to IBM Director.
Install IBM Director Level-2 Agent on the systems currently running Insight Manager. This will give you the advantage of using the full functionality of IBM Director (for example, remote control and inventory).

The downside of this implementation is that it requires substantially more work to be done. You will have to plan for the distribution of the IBM Director Agent to all Insight Manager systems. We strongly recommend that you use the development and integration steps mentioned in 2.1, “General considerations” on page 40, to reduce possible risks.

### 2.13 Redundancy

If you intend to use IBM Director to manage a large number of systems or you have significant service level agreements with your customers, you might want to consider setting up a redundant IBM Director Server system. When planning the implementation of redundant IBM Director Server systems, consider these two questions:

- What is the impact of IBM Director Server downtime (for example, alerts not being sent, no remote control capabilities)?

- How long can IBM Director Server be down?

If the answer to the first question is that the impact of downtime is severe, you might consider redundancy. But the level of redundancy yet remains unclear. You might plan your IBM Director Server simply being highly redundant in one system (for example, redundant fans or redundant network connections) or you might consider implementing two redundant IBM Director Server systems.

The answer to the second question will decide this. If you cannot sustain downtime longer than a few minutes, implementing two redundant IBM Director Servers is crucial.

However, keep in mind that implementing redundant IBM Director Server installations adds complexity to your solution. If you can sustain downtime of about an hour or two, consider, for example, using a disaster recovery scenario. A possible solution is to clone your IBM Director Server. Reapplying the clone image will not take very long and you will be fully operational again. Of course, you will need to save the image of the IBM Director Server system on another machine. Also, you will need to have the hardware ready to reapply the image.

#### 2.13.1 High availability

IBM Director high-availability configuration allows IBM Director Server operations to be performed by a redundant IBM Director Server in the event of a
management server failure. The IBM Director management server is run in conjunction with a high-availability system such as IBM Tivoli System Automation for Multiplatforms or SteelEye LifeKeeper.

There are several advantages of running IBM Director Server in a high-availability configuration:

- You can still manage systems while performing scheduled maintenance on one of the management servers.
- IBM Director events and event action plans are performed, even in the event of an unexpected failover of the management server.
- Data loss is minimized in the event of an unexpected failover of the management server.
- Non-interactive tasks, including scheduled jobs, save runtime checkpoints, and will restart from the last saved checkpoint in the event of an unexpected failover of the management server.

We recommend that you consider the following:

- If your management server is installed on a Linux platform, use SteelEye LifeKeeper or Tivoli System Automation for Multiplatforms.
- If your management is installed on a Windows platform, use SteelEye LifeKeeper.
- Both management servers need to have a dynamic IP address and should have identical network configurations.
- Both management servers should have synchronized passwords and user IDs, possibly via an authentication service such as LDAP or Active Directory.
- We recommend that you use a supported remote database for IBM Director management servers. The database should be configured for high availability, as described in the database documentation.
- If using the embedded Apache Derby database, SteelEye LifeKeeper is available as a no charge download. This is highly desirable for proof-of-concept testing for the IBM Director High Availability solution. See 4.2, “SteelEye LifeKeeper for high availability” on page 166, for more about this solution.

For more about configuring High Availability options, refer to Chapter 3 of the *IBM Director Planning, Installation, and Configuration Guide*. 
2.14 Performance recommendations

Depending on the version and type of operating system that you are using, usually it can be tweaked and tuned in many different ways. Many people use performance tuning to gain optimization and speed, but for your IBM Director Server, we are more concerned with reliability, usability, stability, and security.

Here are some tips for how we optimized performance on our IBM Director Server:

- **Database**
  Locate the database on a high-speed file system, for example, RAID-1 with as many drives as possible when building the RAID array.

- **Memory**
  More memory is always good. Our testing showed that IBM Director definitely runs better with more memory. We recommend at least 1 GB of memory on the management server, and more if you plan to manage more than 1,000 systems.

- **Services**
  Stop or disable services that are not necessary on your management server. In particular, under Windows this might include the print spooler, zero wireless service, 802.11b access, indexing services, fast user switching, FTP, IMAPI CD burning, and other services that not required.

- **Antivirus**
  Exclude the directories where IBM Director JAR files reside to speed up IBM Director Server startup.

- **High availability**
  Normally, the default IBM Director Server configuration provides an acceptable balance between reliability and performance. In some situations, some intermediate data might be lost in the event of a failure, but performance is not adversely affected by near-constant logging of events to disk. Implementing IBM Director Server in high availability mode will decrease overall performance, but offer better protection and failover capability in the case of an unexpected failure.

2.15 Groups

Groups are a powerful instrument within IBM Director. You can use groups to ease administration (for example, a group of all servers with firmware revision X)
and for security purposes, such as enabling a Web administrator access only to the group of Web servers.

We highly recommend a proper planning of groups, especially when using groups for security purposes. The attributes of dynamic groups should be planned and tested carefully. If your attributes have not been planned thoroughly, it is possible, for example, that a mission-critical database server could be manipulated by someone who should not have the authority.

Another aspect of group planning is if you use software distribution to install packages and software. On an individual group basis, you can define from which location the software will be installed, thus saving bandwidth.

See 5.3, “IBM Director groups” on page 243, and the IBM Director Planning, Installation, and Configuration Guide for details on groups.

2.16 IBM Director Extensions

IBM Director extensions add additional functionality to the base IBM Director product. This section covers an overview of the extensions and licensing and planning considerations.

2.16.1 Capacity Manager

In IBM Director, capacity management can generally be performed using the Capacity Manager and Resource Monitors tasks.

**Note:** Capacity Manager is a fee-base IBM Director extension. Refer to 1.6, “IBM Director licensing” on page 20, for more information.

When planning for capacity management, follow the *keep it simple* principle. Our experience has shown that only a few of the available monitors make sense in everyday use.

For example, monitoring all UDP ports on a normal server causes significant overhead without providing any added value. Monitor unusual resources only if you have a special need to do so. Otherwise, keep the number of monitored resources as low as possible.

For details on using Capacity Manager and performance tuning, we suggest that you read Chapter 17, “Capacity Manager,” of the IBM Redbooks publication Tuning IBM System x Servers for Performance, SG24-5287.
If you intend to save or export resource utilization data, consider ahead of time where this data will be stored, including a network available file system.

### 2.16.2 Electronic Service Agent

Electronic Service Agent (ESA) monitors hardware events of IBM System x and IBM BladeCenter systems and transmits system inventory to IBM. Electronic Service Agent has two key functions:

- **Automatic hardware problem reporting**
  
  Hardware errors that meet certain criteria for criticality are automatically reported to IBM and a service request is generated.

- **Inventory collection**
  
  Performs hardware and software inventory collections and reports inventory changes to IBM. All information sent to IBM is stored in a secure IBM database and used for improved problem determination such as down-level firmware or software drivers.

**Note:** Electronic Service Agent is an IBM Director extension that can be downloaded and installed at no charge from:


We suggest that you take the following points into account:

- Personnel within your organization who will be the primary contacts for service requests
- Personnel within your organization who can track service requests via the IBM electronic Web portal
- Internet connection method to access IBM
  
  - Modem
  - Direct
  - HTTP proxy

For more information about configuring Electronic Service Agent refer to Chapter 8, “IBM Electronic Service Agent” on page 459.

### 2.16.3 PowerExecutive

PowerExecutive enables customers to manage power and thermal needs of IBM System x and IBM BladeCenter systems. IBM PowerExecutive enables
customers to monitor actual power draw and thermal loading information, which can help with:

- More efficient planning of datacenter construction and or modification
- Proper power input sizing based on physical systems
- Capping of power when resource demands are exceeded or in the event of a power crisis
- Justification of incremental hardware purchases based on available input power capacity
- Better utilization of existing resources

PowerExecutive is an IBM Director extension that can be downloaded at no charge from:


PowerExecutive works at the Physical Platform Management Object (PPMO) level and queries power and thermal information through the following interfaces:

- Baseboard Management Controller
- Remote Supervisor Adapter II
- BladeCenter Management Module

We suggest that you take the following points into account:

- Ensure that your systems are supported by PowerExecutive.
- Ensure that your systems have the latest BIOS and system processor firmware to take advantage of PowerExecutive.
- Verify that you have out-of-band (OOB) connectivity to the BMC, RSAII, or BladeCenter Management Module.

For more information refer to Chapter 9, “IBM PowerExecutive” on page 485.

2.16.4 Remote Deployment Manager

Remote Deployment Manager (RDM) enables customers to remotely configure, deploy, and retire systems on both IBM and non-IBM systems, including updating system firmware, changing configuration settings, installing operating systems and applications, backing up and restoring partitions, and securely erasing data from disks.

**Note:** Remote Deployment Manager is a fee-based IBM Director extension. Refer to 1.6, “IBM Director licensing” on page 20, for more information.
RDM utilizes the Preboot Execution Environment (PXE) and therefore requires Dynamic Host Configuration Protocol (DHCP) to be enabled for Remote Deployment Manager target systems.

Special consideration must be made when implementing RDM in large or complex networks. We suggest that you read Chapter 3, “Planning your RDM installation,” of the *IBM Remote Deployment Manager 4.3 Installation and Configuration Guide*.

### 2.16.5 IBM Virtualization Manager

IBM Virtualization Manager is an extension to IBM Director and helps customers manage both physical and virtual resources from a single console. IBM Virtualization Manager enables you to work with virtualized environments that are managed by IBM Hardware Management Console (HMC), Microsoft Virtual Server, VMware, and Xen virtualization.

IBM Virtualization Manager can be downloaded at no charge from:


IBM Virtualization Manager is installed on x86 hardware, but can discover and manage additional x86 systems as well as any IBM System i or IBM System p hardware that is under the control of an HMC in your environment.

We suggest that you take the following points into account:

- Types of virtualized environments you are planning to manage.
- Ensure that the operating system is supported by IBM Virtualization Manager.
- Event action plans (EAPs) to drive migration and other virtualization tasks.

For more information refer to Chapter 10, “IBM Virtualization Manager” on page 513.

### 2.16.6 IBM z/VM Center

IBM z/VM Center can provision and manage Linux systems on virtual hardware that is based on IBM System z hardware and the z/VM hypervisor. You can also use z/VM Center to configure Linux utilities for IBM System z that have been installed on Linux systems that run under the control of the z/VM hypervisor.

**Note:** The z/VM Center extension is a chargeable feature.
z/VM Center requires a System z server running z/VM 5.2 and one of the following operating systems:

- SUSE Linux Enterprise Server 9 for IBM System z
- SUSE Linux Enterprise Server 10 for IBM System z
- Red Had Enterprise Linux AS 4 for IBM System z

If you will be using DirMaint™ for the directory manager on z/VM you will need to apply some APARs before using z/VM Center. For more information refer to Chapter 11, “IBM z/VM Center” on page 569.

### 2.17 Scheduled tasks

Plan to schedule resource-intensive tasks such as inventory collection and the generation of capacity management reports for times of low utilization. IBM Director features an integrated and very useful Scheduler, which is particularly helpful if you need to coordinate the execution of several tasks that are resource-intensive or that could compromise the uptime of your managed systems.

Plan on scheduling tasks such as IBM Update Assistant to run during planned maintenance windows, since Update Assistant may need to reboot target managed systems one or more times.

Plan these schedules carefully. An Update Assistant task running parallel with a weekly backup could interrupt the backup with a reboot. Or an Inventory Collection task could take place while a huge batch job is being performed, consequently slowing down the system.

### 2.18 Changing your IBM Director infrastructure

As we stressed earlier, a complete systems management environment can be a complex structure with numerous dependencies. Changing one component within this structure might render the whole non-functioning.

Therefore, do not change your production environment without careful consideration. If you have to make changes that could compromise your IBM Director implementation (such as changing the IBM Director service account), go through the steps mentioned in the DIP approach described in 2.1, “General considerations” on page 40.

One particular aspect of this is that the IP address of the system running IBM Director Server must not change. We recommend that you assign a static
address. The reason is that the IP address of the management server is saved in IBM Director Agent, so that it knows where to send any events. See 5.5, “Using cimsubscribe to process local events” on page 254, for more information.

2.19 Alerting

It is important to plan which events you will monitor and to whom you will send the alert. You should also plan the format in which you would like to receive the events.

IBM Director has the ability to send alerts in many different formats to an unlimited number of receivers. In this section we first have a look at planning which events you want to monitor and where you want to send the alerts. Then we discuss the event architecture in IBM Director and how you can set up your event action plans.

To configure a useful event action plan, complete these steps:

1. Plan the event action plan implementation.
2. Create the event filters.
3. Create actions.
4. Create the event action plan.
5. Associate the event action plan to a system or a group of systems.
6. Maintain the event action plans.

The following terms are used when describing alerting:

- **Event**
  The occurrence of a predefined condition that identifies a change in a process or device (a managed system goes offline, a process stops, or a hard drive fails). As a result, a notification of the change is generated and tracked.

- **Action**
  If an event is flagged, you execute an action. IBM Director has a variety of actions to create the best suitable solution for your infrastructure.

- **Alert**
  The result of an event, and a very common action. If you configure an action to send an e-mail, the alert is the e-mail itself.

- **Event filter**
  A criterion that determines whether an incoming event should be acted upon.
- **Event filter subgroup**
  A group of criteria from the same event source that determine whether an incoming event should be acted upon.

- **Event action plan**
  A group containing actions and either event filters or event filter subgroups. Event action plans are central to IBM Director’s handling of events. They are associated with one or more managed systems or groups.

### 2.19.1 Planning for event action plans

There are many ways to implement event action plans (EAPs), but we recommend that you keep them simple. This makes them easy to maintain and update without having to restructure an entire EAP.

Before you open the Event Action Plan Builder for the first time, start by planning the EAP. How you configure your EAPs is based on your infrastructure. A small company with one or two IT staff members and a few managed systems and applications will need different EAPs than a company with hundreds or thousands of managed systems and applications, and many locations and IT departments.

The managed systems that are servers are the most critical systems because if they have a problem, both users and customers can be affected. Single-user managed systems (desktop and notebook computers) are generally not considered as important because a failure will only affect that user.

**Tip:** Try to make your EAPs as generic as possible in order to minimize the number of EAPs you must manage. Increasing the number of EAPs increases the complexity of your implementation. More EAPs also mean more complex maintenance, since changing something in one EAP can require making the same change in several others.

### 2.19.2 Event action plans for servers

The following information is important for creating EAPs for servers.

**Geography**
Know how many locations you will have with managed systems, and whether each location has IT staff or if the IT in that location is managed remotely.

If you are implementing IBM Director in a large enterprise or for locations great distances apart, it might make sense to have a management server at each
location. TCP/IP communication over long distances can be limited and possibly unstable, so if communication goes down, all EAPs for those locations will be useless since events may not reach a remote management server.

If locations do not have local IT staff, you might consider forwarding events to locations that do. Table 2-10 shows the locations for our example.

**Table 2-10  Locations**

<table>
<thead>
<tr>
<th>Location</th>
<th>Local IT staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oslo</td>
<td>Yes</td>
</tr>
<tr>
<td>Drammen</td>
<td>No</td>
</tr>
<tr>
<td>Grimstad</td>
<td>No</td>
</tr>
<tr>
<td>Bergen</td>
<td>Yes</td>
</tr>
<tr>
<td>Tromsø</td>
<td>No</td>
</tr>
</tbody>
</table>

**Number and type of managed systems**

Although it makes no difference to IBM Director whether you have 10 or 1,000 systems, it does affect the number of alerts you receive. A system management application provides value only if alerts are read and acted upon.

**Table 2-11  Managed systems in the environment**

<table>
<thead>
<tr>
<th>Managed systems</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers (IBM and non-IBM)</td>
<td>135</td>
</tr>
<tr>
<td>Clients (IBM and non-IBM)</td>
<td>1900</td>
</tr>
</tbody>
</table>

If you already have implemented IBM Director, you can use the Inventory function to gather this information.
Applications
Make a list of applications you want to monitor on your servers. (We use this list later in the book to determine the type of actions you configure and who you want to alert.) Then categorize the applications into groups based on their importance. An example is shown in Table 2-12.

Table 2-12  An example of application priority

<table>
<thead>
<tr>
<th>Application</th>
<th>Function</th>
<th>Fault tolerant</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2</td>
<td>Database engine containing all customer information; source for the WebSphere® application</td>
<td>Yes, two-node cluster</td>
<td>1</td>
</tr>
<tr>
<td>WebSphere</td>
<td>Online product information and e-commerce</td>
<td>Yes, two-node cluster</td>
<td>1</td>
</tr>
<tr>
<td>Lotus Domino</td>
<td>Mail and internal applications</td>
<td>No</td>
<td>2</td>
</tr>
<tr>
<td>Sametime®</td>
<td>Instant messaging</td>
<td>No</td>
<td>2</td>
</tr>
<tr>
<td>Citrix Terminal Server</td>
<td>Terminal server for 50% of the users</td>
<td>Yes, 20 servers in a farm</td>
<td>3</td>
</tr>
<tr>
<td>Active Directory</td>
<td>Provides logon validation; integrated with the Citrix application</td>
<td>Yes, four AD controllers</td>
<td>3</td>
</tr>
<tr>
<td>DHCP, DNS, and WINS</td>
<td>Provides infrastructure traffic for clients</td>
<td>Yes, four servers</td>
<td>3</td>
</tr>
</tbody>
</table>

Levels of application importance:

- Priority 1: business-critical applications without which the company cannot operate. A priority 1 application must be available 24x7.

- Priority 2: critical applications that affect most workers in the company, but their absence does not prevent customers from ordering your products on the Web. Priority 2 applications must be available each day from 0700 to 2200.

- Priority 3: applications or services that are required for the infrastructure to work properly, but without them primary applications will still be available. There are no time considerations for these applications, and most of them have backup systems that will take over if they fail.

Some applications might be priority 1 but can be degraded to a priority 2 or 3 if you have a fault-tolerant solution implemented. Examples of fault-tolerant solutions are clusters, terminal server farms, and multiple Active Directory servers.
People

Some of the alerts in your event action plan will not require user intervention because the response to the problem is automated. However, serious problems in your infrastructure that could lead to, or already have caused, one of your priority 1 or 2 applications to go down require notifying a responsible person.

In small or medium-sized businesses, where the IT department has only one or two people, both can receive the alert. In a bigger scenario, staff members have different responsibilities, and the right alert must be forwarded to the right person. Large companies often have personnel who specialize in one application or technology, but when the specialist is not available, backup might be needed for key applications.

Our scenario in Table 2-12 on page 80 shows two priority 1 applications that must be running 24x7. We have assumed that our help desk can solve most of the problems, but when it is critical, we need an application specialist.

For priority 2 applications, we rely on the help desk to solve problems at night, and an application specialist is always available between 0700 and 2200.

Table 2-13  Support staff

<table>
<thead>
<tr>
<th>Person</th>
<th>Location</th>
<th>Responsibility</th>
<th>Assigned to on-call service?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help desk</td>
<td>Oslo</td>
<td>All</td>
<td>Yes (24 hours)</td>
</tr>
<tr>
<td>Martin</td>
<td>Oslo</td>
<td>DB2 and WebSphere</td>
<td>First week every month</td>
</tr>
<tr>
<td>Lisa</td>
<td>Oslo</td>
<td>DB2 and WebSphere</td>
<td>Second week every month</td>
</tr>
<tr>
<td>Eddy</td>
<td>Oslo</td>
<td>WebSphere and DB2</td>
<td>Third week every month</td>
</tr>
<tr>
<td>Carla</td>
<td>Oslo</td>
<td>WebSphere and DB2</td>
<td>Fourth week every month</td>
</tr>
<tr>
<td>John</td>
<td>Oslo</td>
<td>Infrastructure, Norton Antivirus</td>
<td>Yes, from 0900 to 1700</td>
</tr>
<tr>
<td>Angela</td>
<td>Tromso</td>
<td>Firewall, infrastructure</td>
<td>Yes, from 0700 to 1500</td>
</tr>
<tr>
<td>Fred</td>
<td>Tromso</td>
<td>Citrix and infrastructure</td>
<td>Yes, from 0800 to 1600</td>
</tr>
<tr>
<td>David</td>
<td>Tromso</td>
<td>Citrix, Lotus Domino</td>
<td>Yes, from 0700 to 1500</td>
</tr>
</tbody>
</table>

Note: Availability-critical applications require that personnel be available in case of problems, even in the middle of the night. This means that you cannot define a priority 1 for an application if you do not have people to support it 24 hours every day.
Severities

If you define the severities first, it is easier to decide which actions you will use to record the events and to whom you want to send alerts. You can create several different severities. We have selected four as an example:

- **Log only**
  An event that we want to log in case we need the information for troubleshooting. However, we do not want to send an alert for this event.

- **Information**
  A problem in the infrastructure should be fixed, but the system is still operating so the problem can be researched the next day.

- **Critical**
  There is a serious problem in the infrastructure, but all of the priority 1 and 2 applications are online. This problem must be fixed as soon as possible because it can lead to a fatal severity.

- **Fatal**
  Customers cannot purchase products, or workers within the company cannot access their data. This is an emergency situation.

Events can have different severities at different times. In our example, if the Lotus Domino server is down outside of working hours, it is not critical, but it will be critical if the mail server is unavailable during the next business day.

Actions

Now that we have an overview of our infrastructure we can determine which actions to use for the different alerts. Consider the following when you decide on your actions:

- **Number of alerts**
  A staff member who receives too many alerts might stop reading them after a while because they might not seem important, especially after a series of alerts for the same event.

- **Out-of-band alerts**
  When a fatal event has occurred, it is very important that the person who should receive the alert really receives it. (Sending an e-mail that the mail server is down probably is not a good idea.) Fatal and critical alerts require more than one action in the event one kind of alert does not work due to the event that triggered it. An out-of-band solution with a modem or a separate mail server often is a good solution.
- **Action type**

  To make sure that the alerts reach the receiver, choose the right action. For fatal actions, an SMS message to an on-call service person is probably the most appropriate. Do not send information messages in the same format because this could draw attention away from the fatal alert.

- **Knowledge level of the person receiving the alert**

  It is important that the person who receives an alert understands the meaning and importance of the alert. The planning and implementation of the event action plan should reflect this.

  In organizations that have personnel who specialize in certain types of technology, it makes sense to, say, send server hardware alerts to a person with expertise in server hardware.

  You can use event substitution in the alert message that will forward the original event. An original ServeRAID event can look similar to Example 2-1.

  __Example 2-1  Typical ServeRAID event__

  Fatal - Defunct drive (FRU Part# 36L8773) - I/O subsystem error on controller 1, channel 3, SCSI ID 2. at Halden the 12/17/2005 at 10:50 AM EST Source: Storage.ServeRAID Controller.Physical Drive.State.Failed

  However, a recipient who does not know RAID technology and hardware might not understand the importance of the message. It can be better to convert the text to something more understandable, using event substitution, as in Example 2-2.

  __Example 2-2  ServeRAID event in text__

  A disk drive has failed in Halden and the storage subsystem is in a critical state. All users still have access to their data but the disk drive should be replaced as soon as possible. Call 1-800-IBM-SERV to report the problem and get the disk drive replaced. You need to know the machine type and serial number of the server before you call, and this can be obtained from the inventory database on the IBM Director server. The text of the event is as follows: Defunct drive (FRU Part# 36L8773) - I/O subsystem error on controller 1, channel 3, SCSI ID 2.

IBM Director has a broad and flexible set of predefined actions. Select the actions that are most appropriate for your environment. See Appendix A, “Event actions” on page 891, for a complete description of event actions.
The selected action should correlate to the severity of the event so that all information alerts are sent in one format, critical alerts in another format, and fatal alerts in yet another format, as in Table 2-14. This will make it easier to manage your event action plans. Using too many actions can be detrimental. It is better to keep the number of action methods to a minimum to make your event action plans easier to maintain.

Table 2-14  Mapping severities to actions

<table>
<thead>
<tr>
<th>Severity</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log</td>
<td>Log</td>
</tr>
<tr>
<td>Information</td>
<td>E-mail, log</td>
</tr>
<tr>
<td>Critical</td>
<td>E-mail, log, alphanumeric message</td>
</tr>
<tr>
<td>Fatal</td>
<td>E-mail, log, alphanumeric message</td>
</tr>
</tbody>
</table>

Mapping events to severities

Now we have a full overview of our infrastructure, and we know which alerts to send and who will receive them. The next task is more complicated because we have to specify the severity for each and every event.

One way to do this is quite simple, and the other way requires a lot of time:

- Set the severity of the event to the severity level set by the application.
- Pick out single events and create a custom action for each event you want to monitor.

First, we look at the simple method.

When you create an event filter, you can choose different severities. (See 12.4, “Event filters” on page 687 for more information.) Using the simple approach, just say that all error messages in the Windows event log from Lotus Domino Server are considered to be critical alerts in our EAP. A warning alert in the Windows event log is an information alert, and so on, as in Table 2-15.

Table 2-15  Event examples for servers

<table>
<thead>
<tr>
<th>Event source</th>
<th>Event</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lotus Domino</td>
<td>Error message in the Windows event log</td>
<td>Critical</td>
</tr>
<tr>
<td>Lotus Domino</td>
<td>Warning and information messages in the Windows event log</td>
<td>Information</td>
</tr>
<tr>
<td>Event source</td>
<td>Event</td>
<td>Severity</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>DNS</td>
<td>Error message in the Windows event log</td>
<td>Information</td>
</tr>
<tr>
<td>DNS</td>
<td>Warning message in the Windows event log</td>
<td>Information</td>
</tr>
<tr>
<td>Hardware RAID</td>
<td>All fatal events</td>
<td>Fatal</td>
</tr>
<tr>
<td>Hardware RAID</td>
<td>All critical events</td>
<td>Critical</td>
</tr>
<tr>
<td>Hardware RAID</td>
<td>All events except fatal and critical</td>
<td>Information</td>
</tr>
<tr>
<td>Hardware</td>
<td>All fatal events</td>
<td>Fatal</td>
</tr>
<tr>
<td>Hardware</td>
<td>All critical events</td>
<td>Critical</td>
</tr>
<tr>
<td>Hardware</td>
<td>All events except fatal and critical</td>
<td>Information</td>
</tr>
<tr>
<td>Managed system</td>
<td>Server offline</td>
<td>Fatal</td>
</tr>
<tr>
<td>Managed system</td>
<td>Server online</td>
<td>Fatal (see the tip below)</td>
</tr>
</tbody>
</table>

**Tip:** It is important to send an alert when a problem is resolved. System online and system offline are good examples of this. When a problem is resolved after a system has been offline, a message should be sent noting this.

This is the reason we have set the *system online* alert as a fatal severity, because the alert will be sent in the same format to the same person when the managed system is back online.
The advanced way to categorize events and map them to severities is to create simple event filters for all of the events you want to monitor, and apply a customized action to each event filter. This is time consuming to plan and implement, but it enables you to create customized actions for all events. We have picked one event as an example in Figure 2-6.

![Simple Event Filter Builder: License service](image)

*Figure 2-6  Example of an event*

This corresponds to the event in the Windows event log in Figure 2-7 on page 86.

![Event Properties](image)

*Figure 2-7  Example of Windows 2000 event log message*
It is usually very difficult to start with this method, so we suggest that you begin with the easy method, then pick out events that you would like to monitor more closely, or create a customized action for and use the advanced method.

**Grouping**

Now that we know how we will implement our event action plan, it is time to look at the grouping aspect of the event action plans. After it is created, the event action plan must be applied to a managed system or a group of systems.

We recommend that you apply event action plans to groups. When you associate an event action plan to a group, all systems in that group, both current and future, will have that event action plan associated with them. If a system is removed from the group, it will no longer be associated with the event action plans for that group. This makes both deployment and maintenance of event action plans easier.

There are three different group categories in IBM Director. They are:

- Static groups
- Dynamic groups
- Task-based groups

Refer to 1.9.3, “Grouping systems” on page 32, for more information about the group categories.

**Grouping tips:** Remember these tips when setting up groupings.

- Apply event action plans to groups, not to individual systems. If you only have one system, create a group with that system in it. When you install other systems later, they will have the event action plans automatically associated with them as soon as you add them to the group.

- Applying an event action plan to a system that does not meet the criteria for the event is still a valid association. This can be useful when associating event action plans to groups of systems.

  For example, if your event action plan is related to alerts from a ServeRAID adapter, and you associate that plan to a group of servers, it does not matter that some of those servers do not have ServeRAID adapters installed. The plan simply never will get executed by those systems.

- It is possible to have the same event action plan associated with a system multiple times, which can lead to multiple alerts. For example, if you have a process monitor applied both to a system and a group, you will receive two notifications when the event occurs.
For small implementations of IBM Director running on fewer than 10 to 20 servers, you can apply all of the event action plans to the default group All Director Systems. This will make the implementation easier to maintain because all changes you make in the Event Action Plan Builder will affect all systems immediately. All managed systems will always be in this group, so you are guaranteed that the action plans are applied to the systems.

In our scenario, we want to send alerts based on the severity of the server. Therefore, we also need to create groups for the different locations and apply the event action plans to the location groups. As shown in Figure 2-8 on page 88, we built four event action plans based on severities and created different actions depending on where we want to send the alerts.

![Event action plan example with three severities](image)

Now that the EAPs have been created, the next step is to associate them with groups of systems.

We recommend two ways to create the groups to use for your event action plans. These are just suggestions, and because almost all infrastructures are different,
it is likely that you will need to modify these examples or invent a different grouping plan.

- Use static groups for event action plans.

  The objective is to separate the servers from the client systems, because these two groups need different action plans. One way to do this is to create a static group and drag all servers into that group. This is a manual process in IBM Director Console, and if you forget to put a system in a group, you will not get alerts. Also, if you bring a new server online, remember to add it to the group.

  On the other hand, you have total control of which systems are in the static group, and they will stay there until you manually remove them. In a small or medium-sized business that has up to 200 managed systems that are servers, this method is a good choice.

  In Figure 2-9 we have created static groups based on the severity of the systems and applied the event action plans to the appropriate groups.

- Use dynamic groups for the EAPs.

  The second method is based on the use of dynamic groups for the event action plans. If a new system is installed in your infrastructure, no manual action has to be performed other than to install the IBM Director agent on the system. The system automatically goes to the dynamic groups that meet its criteria, and event action plans are associated with the system automatically.

  However, creating the dynamic group criteria can require more testing and configuration tasks. Depending on your infrastructure, the criteria will vary.
One method is to use hardware-specific criteria and create your groups based on the server hardware. In Figure 2-10, our dynamic group contains systems of a specific type, or those with a service processor or ServeRAID controller. You might need to update this formula if you add servers (such as the x205, for example) that do not meet the existing criteria.

**Tip:** A dynamic group does not give the same control because a managed system that no longer meets group criteria can disappear from the group.

Another method is to use location criteria, which can be based on keyboard settings, time zone, or other language-specific values. If all servers are in the same country but in different locations, use the Mass Configuration tool to write a location name to the appropriate Asset ID field on the servers. You can then create a group based on this information. You can use different logon servers or TCP/IP gateway addresses, or other network-related differences in your locations as a criteria for your groups.

In our scenario, we use application criteria (as seen in Figure 2-11) to pick out the managed systems we want, then apply our EAP to that group.

**2.19.3 Event action plans for client systems**

The EAP implementation for client systems often is easier and less important because a client system failure affects the person working on that client, but a server failure can potentially affect all users and customers of the company. Sometimes it is a good idea to use certain client system EAPs on servers as well.
Some of the events you want to monitor, such as a nearly full disk or a system virus, are similar on both servers and client systems.

The process of making EAPs for client systems is similar to making one for servers, but some of the planning tasks are not appropriate for client systems, and we already have some of the information we need in our server example.

### What you want to monitor

To help you make a list of what you want to monitor on your client systems, we have provided some examples in Table 2-16.

<table>
<thead>
<tr>
<th>Event source</th>
<th>Event</th>
<th>Severity</th>
<th>Receiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Critical events in the Windows 2000 event log</td>
<td>Log</td>
<td>Help desk</td>
</tr>
<tr>
<td>Operating system</td>
<td>User logged on with bad password</td>
<td>Information</td>
<td>Help desk</td>
</tr>
<tr>
<td>Operating system</td>
<td>Disk 80% full and 90% full</td>
<td>Information</td>
<td>Help desk</td>
</tr>
<tr>
<td>Norton Antivirus</td>
<td>Virus found</td>
<td>Critical</td>
<td>Help desk and Norton Antivirus administrator</td>
</tr>
<tr>
<td>Norton Antivirus</td>
<td>Old virus definition file, unable to update virus definition file, service is stopped</td>
<td>Information</td>
<td>Help desk</td>
</tr>
<tr>
<td>Hardware failures</td>
<td>All fatal and critical hardware events</td>
<td>Information</td>
<td>Help desk</td>
</tr>
</tbody>
</table>

### Severities

We use the same severities as we did for servers. In this example, only a virus alert is important enough to be sent as an SMS message to the virus administrator because it can affect more users and possibly also servers.

### Grouping

Groupings of client systems differ depending on whether you want to send alerts to different locations.

- One destination for all alerts

  In our example, all events are sent to the company help desk in Oslo, so we need not be concerned about different location groups for client systems. The easiest way is to apply EAPs for client systems to one of the default groups, such as Level-2: IBM Director Agents. All managed systems, including servers, with IBM Director Agent installed are members of this group. If you do not want servers to inherit the client system EAPs, you need to create a dynamic or static group containing all client systems and apply the EAPs to that group.
Different destinations for alerts

Sending alerts to different destinations based on location requires location groups for the client systems. We recommend one location group for client systems and one for servers, since this approach gives you a better overview of all managed systems.
Security planning and implementation

Systems management tools are, by their very nature, potentially dangerous pieces of software, especially in the wrong hands. As systems management agents typically have full access to the hardware and software of the managed system, they can cause serious problems if not secured properly. It is extremely important to understand what security risks are present, what security capabilities exist in IBM Director, and how to plan for the safest and most efficient use of these features.

This chapter highlights the security features built into IBM Director and describes in detail how to implement a secure systems management environment, both from a hardware and software perspective. We pay particular attention to securing the IBM Director management environment and detail security measures designed into IBM Director Server, Agent, and Console.

The flow of this chapter is arranged as follows:

- 3.1, “Security basics” on page 94
- 3.2, “LDAP” on page 102
- 3.3, “Planning for a secure environment” on page 107
- 3.4, “Implementing IBM Director security” on page 119
3.1 Security basics

In order to plan and implement effective security, you must understand a few basic concepts and principles. If you are comfortable with security terminology and practice, skip ahead to 3.3, “Planning for a secure environment” on page 107.

This section begins with an explanation of a few key concepts, including authentication, encoding, and encryption. Then we discuss various security protocols, and finish with information about other industry-standard protocols used by the IBM systems management solution.

3.1.1 Authentication

Authentication is the process whereby one entity proves its identity to another entity. We do this all the time in the form of IDs. When you go to the airport you are required to prove who you are (authenticate) by showing a photo ID. In this case, a trusted third party, the issuer of the ID, authenticates you by giving you a recognizable ID with your photograph. In a perfect world, if someone steals your ID they cannot use it, as either the picture would not match or the ID would show evidence of tampering. Another example is the user ID and password you provide to access a computer system or the Internet. The fact that you are the only person who knows the password is what makes this authentication valid.

3.1.2 Encoding

Encoding is the process of making data compatible with a transfer medium or, as it is used here, making it more difficult for unauthorized individuals to read the data. Many children play a game where they send secret messages by assigning a different number to each letter of the alphabet and writing down the numbers rather than the letters. This is the same thing we do when we represent telephone numbers as words, such as 1-800-IBM-4YOU. As both of these encoding schemes are fairly well known, they are a poor choice for keeping important secrets. However, using a proper encoding system does provide protection against snooping.

3.1.3 Encryption

Encryption is the process of manipulating data so that it is unrecognizable without a proper encryption key. Unlike encoding, which translates a message from one form to another, encryption involves performing a mathematical operation to change the data itself. As a simple example, if you want to encrypt the name (we use lower case for simplicity), we could use the encryption key 123
and the encryption algorithm for each letter add the number of letters represented in the key. For the name we have chosen to encrypt, this yields \textit{qgwftcqcq}, as Example 3-1 demonstrates.

\textbf{Example 3-1 Simple encryption example}

\begin{tabular}{l}
\textit{john done} \\
123123123 \\
\
\textit{---------} \\
\textit{----------} \\
\textit{qgwftcqcq}
\end{tabular}

While this is a very simplistic example, you can see that \textit{qgwftcqcq} does not look much like \textit{peter pan}. While even an unsophisticated decryption program could easily crack this code, more-complicated systems make it very difficult to decrypt messages, even with massive amounts of computer power.

\textbf{Data Encryption Standard}

The Data Encryption Standard (DES) is the name of the Federal Information Processing Standard (FIPS) 46-3 standard, which describes the data encryption algorithm (DEA). The DEA also is defined in the American National Standards Institute (ANSI) standard X9.32. The terms \textit{DES} and \textit{DEA} often are used interchangeably, but we use DES throughout this book. DES has been studied extensively since its publication and is the best known and the most widely used symmetric encryption algorithm in the world.

DES is a robust algorithm used in many applications where security is a prime concern. The obvious method of attack is a brute-force exhaustive search of the key space. This process takes \(2^{55}\) steps on average. Many experts consider DES to be unsecure, and DES encryption is no longer allowed for US government use.

When using DES, several practical considerations can affect the security of the encrypted data. You should change DES keys frequently, in order to prevent attacks that require sustained data analysis. In addition, you must find a secure way of communicating the DES key from the sender to the receiver. In the IBM Director environment, this is handled by the Diffie-Hellman key exchange protocol. (See “Diffie-Hellman key exchange protocol” on page 98 for more about this.) Using this approach, a different DES key is generated for each session, which increases the level of security by orders of magnitude.

\textbf{Triple-DES}

Triple-DES uses three DES algorithms in parallel, which effectively lengthens the key to 168-bit. However, the way Triple-DES works is that the #1 and #3 keys are the same, which results in a 112-bit key (128-bit with parity). The cryptographic community at large feels that Triple-DES is more secure than DES.
IBM Director can be set to use Triple-DES encryption, using the Diffie-Hellman key exchange protocol to ensure that a new secure key is generated for each session between IBM Director Agent and IBM Director Server.

**Advanced Encryption Standard**

Advanced Encryption Standard (AES) is a block cipher created as a result of a worldwide call for submissions of encryption algorithms issued by the US Government's National Institute of Standards and Technology (NIST) in 1997. After nearly five years of standardization, AES was adopted by NIST as FIPS-197 in November 2001. In June 2003 the U.S. National Security Agency (NSA) announced that AES is secure enough to protect classified information up to the TOP SECRET level, which is the highest security level.

AES was developed to replace DES and Triple DES. The primary motivation for a new standard was the fact that DES has a relatively small 56-bit key, which was becoming vulnerable to brute force attacks. In addition, DES was designed primarily for hardware implementation and is relatively slow when implemented in software. AES solves these issues, offering a block size of 128 bits, key sizes of 128, 192, and 256 bits, and significantly improved performance.

The AES algorithm uses one of three cipher key strengths: a 128-bit, 192-bit, or 256-bit encryption key. Each encryption key size causes the algorithm to behave slightly differently, so increasing the key size not only offers a larger number of bits with which you can scramble the data, but also increases the complexity of the cipher algorithm.

### 3.1.4 Security protocols

As protocols are merely standard ways of doing things, security protocols are standardized ways of performing security tasks. IBM Director uses multiple security protocols, depending on how the management server, management console, and managed systems are configured. These protocols include Challenge-Handshake Authentication Protocol (CHAP), Digital Signature Algorithm (DSA), and Diffie-Hellman Key Exchange Protocol.

**Challenge-Handshake Authentication Protocol**

Both CHAP and its Microsoft-extended version, MS-CHAP, work by two systems having a shared secret. Think of it as trying to get into a club with a secret handshake. Everyone in the club knows this secret. If you want to get into the club, you must prove that you know the secret.

It works basically the same way with computers. You and the computer you want to access share a secret, your password. If you want to log on to a computer service such as MSN®, you have to prove that you know your password. You do
not want your password to be seen by anyone else in the network, so you and your service must agree on a way to share the password so that no one else can discover it. The method used is called a hash.

A hash is simply a mathematical formula that cannot be reversed. You and your service agree on a hash. This occurs between the services server and the client software. When you access the service, you send your hashed password across the network. The service knows how your password was hashed, so you are authenticated without sending your password out in the network in the clear. Example 3-2 shows how a hashed password might appear if intercepted by a network sniffer program.

\begin{verbatim}
password = "password"
hashed password = "X03MO1qnZdYdyfeuILPmQ"
\end{verbatim}

Example 3-2 Sample hashed password

CHAP works basically the same way. When you access a server it challenges you to prove who you are. You respond to the challenge with a user name and password. The password is hashed and sent. The server looks up your user name and your hashed password. If everything matches, you are authenticated and allowed access. This allows CHAP to provide basic authentication with a minimum of security.

Digital Signature Algorithm

Digital signatures provide a more robust method of authenticating users and systems. DSA works using pairs of digital keys, one public and one private. These keys are used with complimentary one-way encryption algorithms, meaning once something is encrypted with one key it can only be decrypted with the other. One of the most common places you can see digital signatures is when you download Web browser plug-ins from the Internet.

This is how it works: you decide to download a piece of software from IBM. IBM has signed the package using its private key. When you install the package the installer finds that IBM is listed as the signing authority and tries to decode the signature block using the IBM public key. Because only the IBM private key can encrypt something that can be decrypted by its public key, if the installer can decode the signature block successfully it knows that the package came from IBM.

If you access a secured Web site using SSL, a certificate is generated so that the data can be encrypted and authenticated using digital signatures. Also, when you log on to a Windows 2000 domain using an Active Directory client, every attempt to communicate with a Windows 2000 Server in the domain is authenticated using digital signatures.
Secure Sockets Layer
Secure Sockets Layer (SSL) is a protocol designed to enable secure communications on an insecure network such as the Internet. SSL provides encryption and integrity of communications along with strong authentication using digital certificates, such as those provided by DSA encryption.

SSL encryption is available for communications between IBM Director Server and IBM Director Console. To enable SSL encryption, simply select the Use SSL check box in the IBM Director Console Login window. Encryption up to 128-bit is supported using a variety of cipher schemes. See Appendix M of the publication *IBM Director Systems Management Guide* for details.

Most Web-based online purchases and monetary transactions are now secured by SSL. When you submit your credit card information to purchase a product from an online merchant, the order form information is sent through a secure tunnel so that only the merchant's Web server can view it. With online banking, financial institutions use SSL to secure the transmission of your PIN and other confidential account data.

Diffie-Hellman key exchange protocol
Strictly speaking, this is called the Diffie-Hellman key agreement protocol (also called exponential key agreement) and was developed by Whitfield Diffie and Martin Hellman in 1976. This protocol allows two users to exchange a secret digital key over an insecure medium without any prior secrets. Diffie-Hellman is used by IBM Director when establishing encrypted sessions between the management server and its managed systems and management consoles.

3.1.5 Standard systems management protocols

Now we examine some other standard protocols used in an IBM Director environment, including the Simple Network Management Protocol (SNMP), Hypertext Transfer Protocol (HTTP), and Telnet.

Simple Network Management Protocol
The most common management protocol currently in use, the Simple Network Management Protocol (SNMP), is designed to allow systems to perform management functions in heterogeneous environments. While SNMP is widely used and available for most systems, it is not a strict standard and is not always closely adhered to. In fact, it is not uncommon for the Management Information Base (MIB) from an agent to require modification before it can be implemented on some management servers.
SNMP is an application layer protocol that facilitates the exchange of management information between network devices and is part of the TCP/IP suite.

This book does not cover SNMP in detail. However, because several IBM System x products can use the SNMP standard, the basic implications of SNMP security should be discussed.

The Remote Supervisor Adapter and Remote Supervisor Adapter II can use SNMP to send traps and for inventory purposes. To secure SNMP, you should plan the SNMP communities used by these SNMP devices. If your company already uses SNMP you probably will have done this planning step already. You can easily apply the settings in your network to Remote Supervisor Adapters.

Whenever possible, you should use SNMPv3, because it was designed to be highly secure. Note that both SNMPv1 and SNMPv2 have serious security holes, including the following:

- SNMP is based on User Datagram Packet (UDP), which is a connectionless protocol, so there is no guarantee that a message sent is actually received or that the sender is who they say they are.

- Access privileges are controlled by a community name. A community name is simply a string of characters that identifies a group of managed systems. This means that all you need to know to manage a system is the proper community string.

This is rather like having to specify a user name without a password. To make matters worse, most SNMP devices use the default community name public, which is known to anyone with more than a passing interest in SNMP. Some additional control can be added by removing the public community name and by configuring the SNMP agent to accept only SNMP packets from certain IP addresses, but this is difficult to manage, as each agent has to be configured with the proper addresses.
All SNMPv1 and SNMPv2 traffic is sent in clear text. Many tools exist to help analyze (or sniff) network traffic, including Microsoft Network Monitor (see Figure 3-1). Using such a tool, a hacker could pick out the SNMP traffic, look at the community string, then attempt to hack into your systems. Considering how commonly the connectionless properties of UDP are exploited by hackers, this can leave you vulnerable to a serious attack.

If you are not using SNMP at the moment, also consider the following. By default, most SNMP devices give read-only access to the community named public. We recommend that you use an SNMP community other than public. Also, try not to use SNMP community names that can be guessed easily, such as company names.

In addition, certain SNMP devices, such as the Remote Supervisor Adapter, are able to communicate only with trusted hosts. Consider this option to allow SNMP queries only from the IBM Director Server.

The latest version of SNMP, SNMPv3, is also supported by IBM Director. The SNMPv3 specifications primarily add user-based security and remote
configuration capabilities to SNMP, making it much more secure than previous
versions. SNMPv3 also supports proxies.

**Hypertext Transfer Protocol**

With everything becoming Web-enabled these days, it is not uncommon for
clients to ask that their management products be Web-enabled as well. On the
surface, this sounds good. You get easy access from a variety of systems. You
probably already use HTTP traffic for any remote or virtual private network (VPN)
access to your environment.

Unfortunately, unless your Web access agent uses some form of security
protocol such as SSL or a Java applet to encode the data, all of your
management information is being sent in an easily readable format. It takes only
a little more work to read an HTTP data stream than it does to read an SNMP
data stream.

**Pluggable Authentication Module**

On systems running a UNIX®-based operating system (Linux or AIX for this
discussion), the pluggable authentication module (PAM) framework provides
system administrators with the ability to incorporate multiple authentication
mechanisms into an existing system through the use of pluggable modules.
Applications enabled to make use of PAM can be plugged-in to new technologies
without modifying the existing applications.

When IBM Director Server is installed under Linux or AIX it uses PAM for
authentication much like it uses Active Directory when installed under Microsoft
Windows. When a user attempts to log on to a UNIX-based IBM Director Server,
it simply makes a call to the PAM for authentication. PAM is responsible for the
authentication mechanism itself, which varies depending on how the
administrator has chosen to configure the environment.

**Tip:** Under Linux implementations of IBM Director Server, the number of
unsuccessful console logon attempts before account lockout can be
configured in /etc/pam.d/ibmdir. To do this, change the number on the account
line to the number of attempts you prefer. At the time of this writing, the default
number of attempts is 6.

**Secure Shell**

Secure Shell (SSH) is a protocol for creating a secure connection between two
systems. In the SSH protocol, the client machine initiates a connection with a
server machine. After an initial connection, the client verifies its connection to the
same server during subsequent sessions, transmitting its authentication
information to the server, such as a user name and password, in an encrypted
format. All data sent and received during the connection is transferred using 128-bit encryption.

IBM Director can use SSH, rather than the simple and unsecure Telnet protocol when using the Remote Session task.

**Service Location Protocol**
The Service Location Protocol (SLP) provides a flexible and scalable framework for providing hosts with access to information about the existence, location, and configuration of networked services. Traditionally, users have had to find services by knowing the name of a network host (a human readable text string), which is an alias for a network address. SLP eliminates the need for a user to know the name of a network host supporting a service.

**Telnet**
Command-line interfaces are useful to manage systems in bulk. Like HTTP, Telnet is easy to set up and available on most platforms today. And like HTTP, Telnet is easily read by prying eyes. Unlike HTTP though, Telnet does not have an encryption capability such as SSL to help make it more secure. SSH is far more secure than standard Telnet and should be used whenever security is a concern.

### 3.2 LDAP

IBM Director 5.20 now supports Lightweight Directory Access Protocol (LDAP) Authentication. LDAP provides centralized user administration for multiple management servers using a common directory as opposed to users and groups defined for the operating system of each management server. If LDAP is enabled, IBM attempts authentication using LDAP credentials. If LDAP authentication fails, the IBM Director management server attempts authentication using local operating system accounts.

The following four steps are required to successfully enable LDAP users and groups for IBM Director:

1. Enable LDAP authentication.
2. Create user groups on the LDAP server.
3. Authorize and modify authority for user groups.
4. Add user accounts to the appropriate user groups.
3.2.1 Enable LDAP authentication

LDAP properties are defined in the dirlap.properties file located in the following locations (where install_root is the install path for the IBM Director management server):

- Windows: install_root\data\dirldap.properties
- AIX, Linux, and Windows: install_root\data\dirldap.properties
- i5/OS: /QIBM/UserData/Director/data/dirldap.properties

**Note:** The hash/pound (#) character at the beginning of a line indicates that the line is treated as a comment. For changes to take effect you must stop and restart the IBM Director Server service.

For details on authentication details that can be modified, refer to the comments section at the start of the dirlap.properties file or Appendix L, “Lightweight Directory Access Protocol authentication properties for IBM Director server,” in the *IBM Director Systems Management Guide.*

### Sample configuration files

Example 3-3 illustrates configuration settings for a System i platform running of i5/OS using a local LDAP server for authentication.

**Example 3-3**  dirlap.properties configured to use Directory Server for System i on the i5/OS management server as the LDAP server

```properties
ldap.enabled=true
ldap.host=localhost
ldap.port=389
ldap.dn="cn=groups,dc=IBMDirSrv,dc=IBM,dc=COM"
ldap.auth.jndi=true
ldap.auth.mechanism=anonymous
ldap.group.name.attribute=cn
ldap.group.member.attribute=member
ldap.group.auth.mechanism=anonymous
```

Example 3-4 illustrates configuration settings for a System x platform using a remote Windows Active Directory (LDAP) server for authentication.

**Example 3-4**  dirlap.properties configured to use Active Directory on a remote server as the LDAP server

```properties
#Active Directory using remote LDAP server configuration
ldap.enabled=true
ldap.host=myldap.mycompany.com
```
Example 3-5 disables LDAP so that authentication is performed by the operating system on which the IBM Director Server is installed. This means that the login account will need to be a local account or, if IBM Director Server is running on a Windows system in a domain, the login account can also be an Active Directory account.

Example 3-5 dirldap.properties configured to authenticate on the operating system of the management server only

Use local Operating system on management server for authentication
ldap.enabled=false

### 3.2.2 Create user groups on the LDAP server

These groups should correspond with both managed-object access authority and task authority. Refer to Table 3-1 for sample group types.

<table>
<thead>
<tr>
<th>Managed object group authority</th>
<th>Task group authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>ibmdir_newyork</td>
<td>ibmdir_cli</td>
</tr>
<tr>
<td>ibmdir_raleigh</td>
<td>ibmdir_remotecontrol</td>
</tr>
<tr>
<td>ibmdir_seattle</td>
<td>ibmdir_useradmin</td>
</tr>
</tbody>
</table>

**Tip:** All members of authorized groups share authority in IBM Director, so you should create groups that are only used for IBM Director.

With authority correctly configured for the groups, you could authorize a user to perform remote control in New York by adding the user to the groups ibmdir_newyork and ibmdir_remote_control.
After creating the groups, you will need to configure authority for each user group to access the IBM Director management server and gain access to privileges, managed objects, and tasks.

### 3.2.3 Authorize and modify authority for user groups

To authorize a user group that exists on an LDAP server issue the following command from the command prompt:

```bash
dircli authusrgp name=groupname type=ldap
```

Where `groupname` is the name of the user group you want to authorize on the LDAP server.

**Tip:** Using `-v` with `dircli` displays verbose output, which helps verify that commands are executed correctly or for troubleshooting any problems. For example:

```bash
dircli authusrgp -v name=ibmdir_raleigh type=ldap
```

The user group is created and granted access to IBM Director, but initially the user group has no authority to access managed objects or perform tasks.

Verify that user groups have been created successfully by issuing the following command from the command prompt:

```bash
dircli lsusrgp
```

You should see which groups have been granted access to IBM Director. Example 3-6 shows sample output.

**Example 3-6 Groups granted access to IBM Director**

```bash
dircli lsusrgp
```

NUCLEUS\ibmdir_cli
NUCLEUS\ibmdir_newyork
NUCLEUS\ibmdir_releigh
NUCLEUS\ibmdir_remotecontrol
NUCLEUS\ibmdir_seattle
NUCLEUS\ibmdir_useradmin

The next step is to edit privileges, group access for managed objects and tasks for the user group, which can be done by issuing the following command from the command prompt:

```bash
dircli chusrgp -P privilege_list -N mo_group -T task_list usergroup
```
Where:

- `privilege_list` is a comma-delimited list of privileges assigned to the user group.
- `mo_group_list` is a comma-delimited list of managed objects that the user group can access.
- `task_list` is a comma-delimited list of tasks that the user group can perform.
- `usergroup` is the user group you are modifying.

**Note:** If the name of the task, managed-object group, or privilege includes a space character, you must enclose the name in quotation marks.

You can use the keywords `all` or `none` in place of a task, managed-object group, or privileges.

To view available privileges, managed-object groups, and tasks lists that can be assigned to user groups, refer to table Table 3-2

<table>
<thead>
<tr>
<th>Function</th>
<th><code>dircli</code> command</th>
</tr>
</thead>
<tbody>
<tr>
<td>List all privileges</td>
<td><code>dircli lspriv -l -o</code></td>
</tr>
<tr>
<td>List all managed-object groups</td>
<td><code>dircli lsgp -o</code></td>
</tr>
<tr>
<td>List all IBM Director Tasks</td>
<td><code>dircli lstask -o</code></td>
</tr>
<tr>
<td>List all authorized user groups</td>
<td><code>dircli lsusrgp</code></td>
</tr>
</tbody>
</table>

**Examples**

The following examples use the `dircli chusgrp` command to configure user group privileges, managed-object group access, and access to IBM Director tasks for a specified group.

Example 3-7 shows the command to assign user group `ibmdir_usradmin` User Administration privileges, no access to managed objects, and access to Launch Command Line interface and User Administration tasks.

**Example 3-7  `dircli chusgrp` example**

```
dircli chusgrp -P engine.useradmin -N none -T "Launch Command Line Interface","User Administration" ibmdir_usradmin
```
Example 3-8 shows the command to assign user group ibmdir_raleigh all privileges, all tasks, and access to the managed-object group Raleigh Systems.

```
Example 3-8   dircli chusgrp example
dircli chusrgp -P all -N "Raleigh systems" -T all ibmdir_raleigh
```

For more information about configuring LDAP and authorizing groups, see Appendix O of the publication IBM Director Systems Management Guide.

### 3.2.4 Add user accounts to the appropriate user groups

The last step is to add user accounts to the appropriate user groups. Refer to your LDAP or Directory Services documentation for information about adding users to groups.

### 3.3 Planning for a secure environment

Systems management software is integrated with the system on which it runs. This is intentional, because systems management software has to be able to perform important system tasks. However, this architecture is also a possible security threat to your company’s IT infrastructure. IBM Director offsets this possible threat by offering various security features.

#### 3.3.1 Service processors

Planning and being aware of the security implications of hardware-based systems management helps to avoid some of the most dangerous security threats. Depending on the type of system management processors you plan to use, different security considerations can apply.

**Remote Supervisor Adapter and Remote Supervisor Adapter II**

The Remote Supervisor Adapter and Remote Supervisor Adapter II feature multiple user accounts that can be configured with either read or read/write access. Plan the use of these accounts carefully and distinguish between users who have read/write access and users who have read-only access (be able to check the servers status).

To enable the Remote Supervisor Adapter’s remote control feature, you must set a single password in the system BIOS. This password is not set by default. If you define a password, we recommend that you do not use the same password for all servers because this could compromise security.
The Remote Supervisor Adapter can also send SNMP traps and function as an SNMP agent. Refer to the next section for more information about SNMP.

The traffic between a Web browser and a Remote Supervisor Adapter is secured and the content of a remote control session is encrypted and should therefore be no threat to corporate security. Here, IBM uses a 128-bit key encryption algorithm to authorize an active session. The Remote Supervisor Adapter then secures the active remote control session’s content using an IBM proprietary encryption algorithm. The Remote Supervisor Adapter II uses 128-bit SSL for this purpose.

**Baseboard Management Controller**

The Baseboard Management Controller (BMC) is a base-level system management controller included on the system board of many System x servers. To maintain a secure environment, it is critical to modify the default security settings for all BMCs in your environment. The reason for this is that the default login credentials for all IBM service processors are USERID and PASSW0RD, which are well known.

Intelligent Platform Management Interface (IPMI) is a standardized, abstracted, message-based interface that defines records for describing platform management devices and their characteristics. This interface allows for standard communication between systems management software like IBM Director and IPMI-compliant system management hardware like IBM BMCs.

IPMI v2.0 adds enhanced authentication, encryption, and a firmware firewall to ensure that reasonable security is maintained when communicating with a management controller. The BMCs in some IBM System x servers support IPMI v2.0.

### 3.3.2 IBM Director Server

Access to IBM Director Server through IBM Director Console is discussed in 3.4.4, “IBM Director Console security” on page 121. What you should plan, however, is the general operating system security of your management server, the system running IBM Director Server.

Access to the management server on an operating system level could compromise your company’s security. Plan how to secure this server, such as by applying the latest security fixes from Microsoft, setting NTFS permissions, and disabling Telnet access under Linux. Remember, security is a chain made up of all of your connected systems and is only as strong as the weakest link.
3.3.3 IBM Director Agent

An important aspect of planning your IBM Director implementation is the use of advanced security features on the IBM Director Agent side. We cover implementation of agent security in detail in 3.4.5, “IBM Director Agent security” on page 133.

Encrypting communication

One of the most effective ways to increase security in your managed environment is to secure all IBM Director Agents and to enable encryption between the management server and its managed systems.

To use server-agent encryption, you must enable it on IBM Director Server and IBM Director Agent during installation:

1. During IBM Director Server installation, check the box Encryption data transmissions, as shown in Figure 3-2. Beginning with IBM Director 5.10, encryption is enabled by default and the Advanced Encryption Standard (AES) method is selected by default. We recommend leaving this setting and using AES to increase security.

![Figure 3-2 Enabling server-agent encryption during IBM Director Server installation](image)

You can also enable or disable encryption settings after IBM Director Server is installed. See “Agent-server encryption” on page 142 for instructions.
2. During IBM Director Agent installation, select the option **Encryption data transmissions**, as shown in Figure 3-3. Beginning with IBM Director 5.10, both secured state and encrypted communication are enabled by default.

**Tip:** Encryption must be enabled at both the server and the agent for communications to be encrypted between those two systems. In addition, specify the type of encryption at the server.

![Figure 3-3 Enabling server-agent encryption during IBM Director Agent installation](image)

We recommend leaving these default settings to maximize security. These settings result in the managed system initially appearing in the Access Denied state with a padlock icon (🔒) in the management console.

To change these settings after IBM Director Agent is installed, run the installation routine again. For Windows installations:

a. Select **Add/Remove Programs** in the Control Panel.
b. Click **Change** to start the installation process.
c. Click **Modify**.
d. Proceed through the install dialogs.
e. When you see Figure 3-3, **deselect** the check box.

To unlock the system and remove the padlock icon, right-click the managed system (you can select more than one), and click **Request Access**. Submit proper credentials to gain access. Proper credentials, in this case, are those of
any account that has local administrative rights on that system. For more detailed information about agent-to-server security, see 3.4.6, “IBM Director Server access control” on page 134, and 3.4.7, “IBM Director encryption” on page 141.

**Important:** Encryption is not supported for managed systems running NetWare, nor any Itanium-based managed system. Also, out-of-band management tasks such as SNMP, Telnet, and FTP are not secured by encryption.

**Agent-initiated discovery**
To make discovery of a new IBM Director Agent automatic, you can specify (by IP address) all legitimate IBM Director Servers in your environment. This option is new to the standard IBM Director 5.10 installation method.

**Tip:** Although the AddKnownServerAddress parameter in the unattended installation response file has been available with unattended installs in previous versions (see “DIRAGENT.RSP contents” on page 202), the ability to specify management servers when running the installer manually is new since Version 5.10.
This causes the managed system to announce itself to the management servers, rather than requiring a discovery process to be initiated by the management server. The format used for specifying management servers must include both the protocol and IP address to use, in the format protocol::address, as shown in Figure 3-4.

Figure 3-4   Specifying the IP address of the management server during Agent installation

For this function to work properly, you must enable the “Auto-add unknown agents which contact server” option in the Discovery Preferences on the IBM Director Server. This setting is not enabled by default.

We recommend using agent-initiated discovery when security concerns are particularly high. You can maximize IBM Director Agent-Server security by combining this functionality with encrypted data transmission and a securely installed IBM Director Agent. For more information regarding agent-initiated discovery, see 2.8.1, “Agent-initiated discovery” on page 55.

3.3.4  IBM Director Console

The IBM Director Console is the main interface to an IBM Director management environment. Therefore, understanding and planning the access and privileges granted to a console user can help eliminate serious security risks. Although your first thought regarding IBM Director Console security might be toward establishing and managing user accounts, there are two other aspects that must be considered in order to maximize security.
Restricting console access
By default, IBM Director Server accepts connections from IBM Director Console running on a system with any IP address. However, you can restrict management console access to the management server based on the IP address of the management console. Restriction is accomplished by specifying a set of IP addresses or IP address ranges that are permitted access to the management server.

This aspect of security is configured by modifying the TWGServer.prop file, discussed in 3.4.4, “IBM Director Console security” on page 121. After this function is configured, any management console with an excluded IP address will fail to log on to the management server, even if a valid user ID/password pair is provided. In addition, an IBM Director security event is generated and logged as a result of the unauthorized access. Event action plans can generate actions based on these events.

Encrypting console-server communication
For the most security conscious environments, consider encrypting all communication between the management console and management server using SSL. This is achieved very simply by checking the Use SSL box in the IBM Director Login window, as shown in Figure 3-5. Implementation of SSL is automatic and managed within IBM Director.

![IBM Director Login window](image)

*Figure 3-5  Enabling Console-Server SSL encryption at the login panel*

For more information about SSL see “Secure Sockets Layer” on page 98.
IBM Director user accounts

Use the IBM Director User Administration window to configure user access and
privileges to prevent unauthorized user access to IBM Director.

IBM Director user accounts are based on user accounts created in the operating
system under which the management server is installed or by authenticating
through an LDAP server. When IBM Director Server is installed, two local groups
are created automatically in the operating system.

- Windows: DirAdmin and DirSuper
- Other operating systems: diradmin and dirsuper

Under i5/OS, these users must have a user profile on the management server
running i5/OS and be registered in a function usage group. For more about this
see the *IBM Director Planning, Installation, and Configuration Guide*.

Members of the DirAdmin (diradmin) group have general access to IBM Director
as specified by their user profiles. Members of the DirSuper (dirsuper) group
have superuser access, full access to all IBM Director functionality, including the
ability to create and edit user profiles. Access and privileges cannot be modified
for any account that is a member of the DirSuper (dirsuper) group.

**Important:** Under Windows, any account with local administrator privileges on
the management server is treated as though it were a member of the
DirAdmin group, whether or not this is actually the case.

Under Linux, the root account is treated as though it is a member of the
dirsuper group, whether or not this is actually the case.

Because of these groups, all accounts with administrative rights in the respective
operating system are authorized to log on to the IBM Director environment.
Additional user accounts are authorized through the normal user administration
processes of the applicable operating system. In a Windows installation, for
example, a user account is simply added to the DirAdmin group on the
management server (or an Active Directory Global Group).

This makes user account administration straightforward and consistent with the
underlying operating system. The validity (disabled or not), password, and
expiration are handled by the operating system under which the management
server runs. In addition, in a Windows domain structure, user accounts from
trusted domains can be authorized for management console logon.

Under Windows, the IBM Director service account is added automatically to both
the DirAdmin and DirSuper groups. See 3.4.2, “IBM Director service account” on
page 120, for more information and recommendations regarding the IBM Director
service account. Under other operating systems, the diradmin and dirsuser groups are not populated automatically. A user with root privileges must assign users to the appropriate groups.

**Important:** In IBM Director 5.x the default user access is fully restricted rather than being wide open, as in previous releases. Although accounts added to the DirAdmin (diradmin) group are able to log on, they see only a blank management console and are not able to perform any actions until a superuser (member of DirSuper/dirsuser) configures privileges and access rights for these accounts.

1. If you install IBM Director server using the Express Installation method, the user access for local administrators is unrestricted.

We recommend not adding accounts to the DirSuper (dirsuser) group unless absolutely necessary, in order to maximize security of the environment. It is much safer to add accounts to the DirAdmin (diradmin) group, even if a given account requires full access and privileges. This way, if access or privileges need to be tightened later, it is simply a matter of modifying the user profile inside IBM Director, rather than modifying group membership under the operating system.

There are a few changes in IBM Director 5.10 related to user administration of which you should be aware. First, the default user properties have been reduced to a minimum. Such a user will not have access to any groups or tasks and will have no privileges in the IBM Director environment. This is a change from the wide-open access granted to unconfigured user accounts in previous versions of IBM Director.

Although the default user properties can be modified, we recommend that you leave these properties at their default. This ensures that any user accounts inadvertently added to the DirAdmin (diradmin) group will not have access to the IBM Director environment. To learn about default user properties, refer to the IBM Director Planning, Installation, and Configuration Guide.
Active Directory Global Group support

IBM Director 5.x supports Windows Active Directory Global Groups (ADGGs) as members of the DirAdmin and DirSuper groups. That is, you can now add ADGGs to the DirAdmin or DirSuper group and administer user authority based on these group objects, as shown in Figure 3-6.

![Figure 3-6 IBM Director 5.10 User Administration window showing the new Groups tab](image)

There are a few key points to keep in mind with regard to ADGG rights administration inside IBM Director:

- Nested ADGGs are supported in 5.20. If an ADGG that is added to the DirAdmin or DirSuper group contains one or more groups, the member groups are enumerated.

- There is no mechanism for Active Directory to notify the IBM Director Server when an ADGG's group membership has changed. Therefore, it is possible for the IBM Director Server to have outdated ADGG group membership information at any given time. ADGG membership is checked and updated only when a user logs into the IBM Director Console or opens the User Administration tool.

- If a user account is a member of multiple ADGGs that are members of the DirAdmin group, the IBM Director user account authority is set to the union of the authorities of each of the ADGGs of which the account is a member. For example, if an account is a member of two ADGGs, one of which is allowed access only to Windows XP systems and the other access only to Windows Server 2003, this account will have access to all Windows XP and Windows Server 2003 systems.

- Authority of user accounts supersedes authority of ADGGs. If a user logs into the management console using an account that is contained in the DirAdmin or DirSuper group, authority is set based on that user account, and the login proceeds without checking ADGG membership.

- Finally, you cannot manage access and privileges for any ADGG added to the DirSuper group, because by definition all DirSuper members have global
authority. We strongly recommend that you do not add ADGGs to the DirSuper group. This is even more important than our earlier recommendation regarding user accounts, because any user account added to such an ADGG under the operating system would have unrestricted access to the full power of IBM Director.

- LDAP is now supported with IBM Director 5.20 and provides more centralized and cross-platform control over user administration than using ADGGs.

Having discussed the basics of IBM Director Console security and user accounts, it is time to turn our attention to the issue of who should have access to the functions of IBM Director Console and what rights and access those users should have.

**Who should have access to the IBM Director Console**

Keep the structure of your IT in mind when determining who should have access to the IBM Director Console. Depending on the size of your organization, you might have different IT departments performing various tasks.

In general, consider who in your organization needs access to IBM Director, and who could benefit from the information provided by this systems management tool. Certainly IT administrators need access to IBM Director. In addition, perhaps another department has the responsibility for support tasks. Some developers could use the performance monitoring tools of IBM Director, or a customer help desk might need up-to-date system status reports to answer incoming calls.

**What rights should be granted**

Now that you know who should be able to access the IBM Director Console, the next step is to plan access so that all users can perform their respective tasks without being a security threat. IBM Director has three ways to restrict functionality:

- Limit the privileges a user can have.
- Limit the groups of systems a user can access.
- Limit the tasks a user can perform.

**Privileges**

Generally, privileges should be restricted to only a few per user, as these rights can lead to security exposures. Restricting privileges is discussed in “Restricting IBM Director privileges” on page 125.

**Group access**

Group access is perhaps the most efficient way to make sure users cannot harm any systems not assigned to them. If you have planned your IBM Director groups...
carefully, you can use group access to allow a specific group access only to areas and information they require to do their jobs.

Carefully evaluate what groups users should be able to access. Granting access to global groups such as *all director systems* may open up systems and information not intended for their use. Also consider configuring read-only access. Read/write access is needed only for those who administer IBM Director and need to change or create groups.

An example of implementing group access is described in the last paragraph of “Restricting access to groups” on page 127.

**Task access**

It is also important to plan access to the various IBM Director tasks. IBM Director runs in the system account in Windows-based machines or in the root context in Linux-based systems. This means, for example, that even if a user normally only has user rights to a system, when they use the File Transfer task in IBM Director, they will be accessing that task as an administrator.

Implementing task access is described in “Restricting access to tasks” on page 129.

### 3.3.5 z/VM Center

If a z/VM system is to be managed by IBM Director with the z/VM Center extension, then the system running IBM Director must be managed to the same security level as the z/VM system itself. The core function of z/VM Center is to make changes to the z/VM directory, make changes to the DASD volumes in the disk pool, and to start and stop guest operating systems running under z/VM.

With this level of access, it is vitally important that the IBM Director system be protected just as well as the z/VM system it will be managing. Users with DirSuper access to the IBM Director system must also be managed as though they had DirMaint privileges on the z/VM system.

The z/VM Systems Management API also requires special consideration. It must be protected so that only authorized systems can initiate communication sessions with it, and the communication channel between the z/VM Management Access Point and the z/VM Systems Management API must be protected from third parties. The z/VM SM API is a plaintext RPC interface. z/VM user passwords will be passed over the network connection between the z/VM MAP and the z/VM SM API unencrypted. A technical solution to this issue is described in Chapter 11, “IBM z/VM Center” on page 569.
3.4 Implementing IBM Director security

Managed systems authenticate with management servers rather than specific users, so controlling access to the management servers is of paramount importance when securing an IBM Director implementation. This section discusses the implementation of console security at the management server.

3.4.1 Communicating with IBM Director Server

As a first step in controlling access to the management server, it is important to understand how administrators communicate with this system. IBM Director uses a Java-based console to access the management server. This same application is used whether you are working locally on the management server or accessing it remotely over the network. The management console communicates with the management server using TCP/IP only.

To access the management console, you must log on with an authorized user account. It is important to understand the relationship between the IBM Director Server service account and authorized user accounts. We discuss authorized user accounts in detail in 3.4.3, “Console user logon” on page 121.
3.4.2 IBM Director service account

During IBM Director Server installation on Windows, you are prompted to enter account information for the IBM Director service, as seen in Figure 3-7. Under Linux, IBM Director Server runs under the root account.

![Figure 3-7 IBM Director Server installation - service account information](image)

If you install IBM Director Server on a Windows system, we recommend creating a user account expressly for the purpose of running the IBM Director Server service. Do not use this account for any other purpose. Here are some specific requirements for such a service account:

- If you install IBM Director Server on a system that is not a member of a Windows domain, the IBM Director service account need only have local administrator rights on the management server.

- If you install IBM Director Server on a system that is a member of a Windows domain, the IBM Director service account must at minimum be a domain user account that has local administrator rights on the management server.

- If you intend to use Active Directory Global Groups (ADGGs) to configure IBM Director Console user privileges and access rights, you must install IBM Director Server on a system that is a member of a Windows domain. In addition, the IBM Director service account must have full Domain Admin rights. This is required in order for the management server to enumerate the ADGGs and to access their contents during user logon.
3.4.3 Console user logon

Access to IBM Director Console requires a valid operating system user account, as discussed in “IBM Director user accounts” on page 114. The logon process works as follows:

1. When a user attempts to log on to IBM Director Console, the user ID and password are sent to the IBM Director Server specified in the logon window. The password is encrypted for security. IBM Director never sends passwords in clear text. IBM Director Server requests authentication from the operating system.

2. If the operating system rejects the credentials supplied, logon fails.

3. If the operating system replies positively to the authentication request, IBM Director Server looks for the user account in the local DirAdmin (diradmin) and DirSuper (dirsuper) groups.

4. If the user account is found in one of the local groups, the user is authorized to access IBM Director Console with the privileges, group access, task access granted to the user profile defined on the management server for that user account. If there is no user profile defined, the account is assigned the default user profile currently in effect. IBM Director user profiles are discussed further in the next section.

5. If the user account is not found in either of the local groups and the management server is a member of a Windows domain, it checks for the presence of ADGGs in the DirAdmin and DirSuper groups. If at least one ADGG is found, it contacts Active Directory to enumerate all ADGGs that were found. If the user account is a member of one or more of these ADGGs, the user is authorized to access IBM Director Console. Privileges, group access, and task access will be the union of the authorities for each ADGG of which the user account is a member. That is, if the user account is a member of an ADGG that has group access to server systems as well as an ADGG that has group access to client systems, the user will be authorized to access both server and client system groups.

6. If user logon has not succeeded to this point, it fails with a displayed error message. All logon failures are recorded in the IBM Director Event Log.

3.4.4 IBM Director Console security

By default, IBM Director Server accepts IBM Director Console connections from any system. The primary method of securing connections between the management server and console is through a password challenge, which in most cases is acceptable. This section discusses both types of security and how to implement each.
Restricting management console access
IBM Director can be configured to accept only connections from specific IP addresses or ranges. Therefore, the first step in managing IBM Director Console security is to decide whether you want to restrict the management console from accessing IBM Director Server based on IP address.

You might want to do this if you want to limit management console access to an internal network or subnet, or simply to reduce the possibility of illicit use of these powerful management tools. You can even prohibit IBM Director Console, installed on the management server, from making a local connection to IBM Director Server.

If restricted management console access is implemented, only IBM Director Consoles running on systems with an allowed IP address (or host name) can connect to IBM Director Server. If a management console with an excluded IP address attempts connection, logon fails even if valid use account credentials are entered. In this case, an IBM Director security event is generated and recorded in the IBM Director Event Log.

To implement this piece of security and restrict the IP addresses from which the management console is allowed to contact the management server, follow these steps, working on the management server:

1. Ensure that all management consoles (local and remote) are logged off.
2. Stop the IBM Director Support Program. At a command prompt enter `net stop twgipc` (Windows) or `twgstop` (Linux default path `/opt/ibm/director/bin`).
3. Open the TWGServer.prop file with a text editor.

   This file is located in `C:\Program Files\IBM\Director\data` (Windows) or `/opt/ibm/director/data` (Linux).

   **Tip:** It is good practice to make a copy of any file you intend to modify before you make changes, to assist in recovering from unexpected results.

4. Near the beginning of this file, look for the line that reads:

   `# twg.gateway.link.1.initparam=*`

5. Edit this line to restrict incoming connections from IBM Director Console. The file is documented to assist in configuration.

   - To allow connection from one or more individual IP addresses, modify the line using the format:

     `twg.gateway.link.1.initparam=* -allowedAddress x.x.x.x`
Where x.x.x.x is a single IP address or host name that should be allowed to connect to the management server. Notice that we have removed the pound character (#) at the beginning of the line, which was used to mark the line as nonexecuting.

You can add additional lines using this format to authorize connections from additional IP addresses or host names.

- To allow connection from one or more IP address ranges, modify the line using the format:

```
twg.gateway.link.1.initparam=* -allowedRange y.y.y.y z.z.z.z
```

Where y.y.y.y is an IP address that marks the lower bound of the IP address range that should be allowed to connect to the management server and z.z.z.z is an IP address that marks the upper bound of the IP address range that should be allowed to connect to the management server. Notice that we have removed the pound character (#) at the beginning of the line, which was used to mark the line as nonexecuting.

You can add additional lines using this format to authorize connections from additional IP address ranges.

6. Restart the IBM Director Server service using `net start twgipc` (Windows) or `twgstart` (Linux).

**Important:** If you neglect to include the management server's own IP address when configuring console access, the local management console (installed on the management server itself) will not be able to connect to IBM Director Server. This can be a valid configuration for some installations where the management server is to be left alone, or is located at a remote site.

**User administration**

In addition to restricting management console access to the management server based on the IP address of the management console, IBM Director Console is secured through the management of user accounts and profiles.

IBM Director user logon security is based on profiles created for each authorized user. As a member of the DirSuper (dirsuper) group, you can establish different access privileges for each type of user who will access the management server. A long list of privileges can be granted or denied on an individual basis for each user. In addition, access to specific groups of managed systems and devices can be allowed or prohibited. Finally, the ability to execute IBM Director tasks can be enabled or disabled, providing exceptional flexibility and security in the management environment.

To access console security, select **Options → User Administration**. Refer to the *IBM Director Planning, Installation, and Configuration Guide* for information...
about how to create and change user and group profiles, including the default user profile.

**User profiles**

When a user account is first authorized, it is not given a profile. You can easily identify which accounts do not have a profile assigned to them in the User Administration window by the lack of a profile icon (●) to the left of a user name, as seen in Figure 3-8. When a user without a profile logs on to the management console, the account is given the default profile in effect at that time.

In IBM Director 5.10, the out-of-the-box default user profile is fully restricted. No privileges, group access, or task access is granted. This is a change from previous versions of IBM Director. This results in an empty management console window for any user whose account has not been granted additional rights.

![IBM Director User Administration window with Users tab selected](image)

**Figure 3-8  IBM Director User Administration window with Users tab selected**

Right-clicking a user account and clicking **Edit** brings up the user profile. The following three headings augment information presented in the *IBM Director Planning, Installation, and Configuration Guide*, expanding on the three sets of options that can be restricted in an IBM Director user profile.
Restricting IBM Director privileges

Securing the management server begins with restricting IBM Director privileges. Privileges are those activities an administrator does to maintain the IBM Director environment as a whole. This includes changing the management server preferences, modifying the database configuration, performing encryption administration, and granting user account privileges.

In a small IT environment, where a small number of administrators manage everything from hardware platforms to software applications, any given administrator might need access to every piece of functionality in IBM Director. However, in a larger organization, where there are different groups of administrators for different areas of the infrastructure, it might become very important to limit access to certain IBM Director features.

Obvious areas of restriction include database configuration and user account management. You might allow only a certain user to change the IBM Director database configuration. Central to the whole concept of privilege restriction is the ability to restrict nearly all users from modifying user account settings, which keeps them from granting themselves privileges they should not have.
Figure 3-9 shows the Privileges pane of the User Editor window in its default state for a new user, which is to deny all privileges. Note that this set of default user properties reflects a change from previous versions of IBM Director. Although the default user properties can be modified, we recommend that you leave these properties at their default. This ensures that any user accounts inadvertently added to the DirAdmin (diradmin) group will not have access to the IBM Director environment.

![IBM Director User Editor window: Privileges tab showing default user privileges set to none (deny all privileges)](image)

In a particularly security-conscious environment, you might want to enable encryption of IPC data between management server and managed system (see 3.4.7, “IBM Director encryption” on page 141), then restrict all users from modifying the Allow Encryption Administration setting.
Restricting access to groups

The next step involves restricting access to managed systems and devices so that each managed group is visible only to appropriate IT staff members. If a user cannot see a system or device on the management console, that user cannot manage the system or device.

This is achieved by restricting the groups to which the user has access. By turning off specific groups on the Group Access tab of the User Editor, you can disallow management of any discovered system or device. Another useful setting on the Group Access tab is the “Limit user to read-only access of groups” check box. Select this check box before enabling “Limit user access only to the groups listed” if you want to allow the user access to the groups, but not to make changes to the groups.

It is important, then, to structure IBM Director groups with this capability in mind. In addition to creating groups based on hardware or software configuration, it might make sense to design dynamic or static groups that will form the basis for group access restriction. Remember that any managed system can be a member of multiple groups. If a user is given access to any group that contains a particular managed system, the user will have access to that managed system.
Implementing IBM Director 5.20

Figure 3-10 shows the Group Access pane of the User Editor window in its default state for a new user, which is to *deny access to all groups*. Note that this set of default user properties reflects a change from previous versions of IBM Director. Although the default user properties can be modified, we recommend that you leave these properties at their default. This ensures that any user accounts inadvertently added to the DirAdmin (diradmin) group will not have access to the IBM Director environment.

![IBM Director User Editor window: Group Access tab showing default user group access set to none (deny access to all groups)](image)

You might, for example, want to keep your servers organized in separate management groups in order to ensure that only e-mail administrators have access to e-mail servers, only database administrators have access to database servers, and only general systems administrators have access to file/print servers.
You could create dynamic groups for the e-mail and database servers based on the software installed on each type of server. You could then create a static group for all file/print servers (or create a dynamic group based on a specific printer driver being present). After the groups are created, it is a simple matter to configure group access for each of the administrator types. Figure 3-11 shows one way to configure group access for a database administrator, based on this example.

![Sample database administrator group access list](image)

**Figure 3-11** Sample database administrator group access list

**Restricting access to tasks**

The final security option discussed in this section is that of restricting the IBM Director tasks a user can perform. As with restricting access to groups, a user cannot perform a task that is not visible on the management console.
This is achieved by restricting the tasks to which the user has access. By turning off specific tasks on the Task Access tab of the User Editor, you can prohibit the execution of any task by a given user.

IBM Director 5.20 incorporates more precise user authorization of tasks with hierarchy-based authorization for parent and child tasks. This differs from previous versions and provides more granular control of task access.

Figure 3-12 shows the Task Access pane of the User Editor window in its default state for a new user, which is to deny access to all tasks. Note that this set of default user properties reflects a change from previous versions of IBM Director. Although the default user properties can be modified, we recommend you leave these properties at their default. This ensures that any user accounts inadvertently added to the DirAdmin (diradmin) group will not have access to the IBM Director environment.
For example, you might want to allow help desk employees to use the management console to check error logs and inventory. You decide it would also be useful to allow them to use IBM Director’s Remote Control task in order to help walk end users through various Windows desktop procedures. Tasks not related to these functions should not be used by this staff. Simply remove all of the unwanted tasks from the profiles of these users. Figure 3-13 shows one way to configure task access, based on these requirements.

![Figure 3-13 Sample help desk user task access list](image)

If your IT organization is divided between server administrators and client administrators, you might consider denying access to tasks associated with server management from the client administrators’ consoles. Server-oriented tasks in IBM Director include the following:

- BladeCenter Management.
- Capacity Manager.
- Configure Alert Standard Format.
- HMC Manager Tools.
- Launch command-line interface.
- Launch Web interface.
- Management Processor Assistant.
- Microsoft Cluster Browser.
- Rack Manager.
- ServeRAID Manager.
- Server Configuration Manager.
- System availability.
- System identification.

Removing these tasks from the management console of client administrators can help ensure that servers are not misconfigured or rebooted accidentally, and simplifies the console considerably for these users. For this example, you might also consider denying access to the Configure SNMP Agent and SNMP Browser tasks, unless SNMP is used to manage the client PC population.

**Important:** There are sometimes unexpected results of certain combinations of group and task access permissions. For example, a help desk person who works only with client PCs might be given access only to groups that include client systems (not servers), as well as access only to tasks as discussed previously. However, since the Event Log task does not require a target system for it to execute, the user will be able to see *all events on all systems*, including server systems, simply by opening the *all events* subtask.

Always test your selections thoroughly to make sure that access for a particular user is exactly as you intend. You can do this by creating a bogus user account that is used specifically for this purpose. After testing, remember to revoke all management console access for this account.
As mentioned previously, IBM Director 5.10 supports the use of Windows Active Directory Global Groups (ADGGs) as members of the DirAdmin and DirSuper groups. For more about this functionality and a list of key points to keep in mind regarding ADGGs, see “IBM Director user accounts” on page 114. Figure 3-14 shows the User Administration window with the Groups tab selected. You add and subtract privileges, group access, and task access for ADGGs exactly the same way as for individual users.

![User Administration](image)

Figure 3-14 IBM Director User Administration window with Groups tab selected

### 3.4.5 IBM Director Agent security

Regardless of the operating system on the managed system, after it is installed, IBM Director Agent runs in a superuser security context. This means that IBM Director Agent itself has full control and authority to all parts of the system. On Windows systems, this is accomplished by having the service run with Local System Account security. Under Linux, the Agent daemon runs as root. In all cases, it is important to remember that IBM Director Agent has privileges to all parts of the system.

**Important:** Several changes have been made to IBM Director Agent and its installer to enhance security of your managed environment. If you have any concern for security, read through this section carefully, even if you are familiar with earlier versions of IBM Director.
As discussed in Chapter 1 of *IBM Director Planning, Installation, and Configuration Guide*, IBM Director Agent provides various methods with which to gain access to and control of a managed system. The methods available depend on the operating system installed on the managed system.

- **Managed system running a supported Windows operating system**
  - IBM Director Server with IPC
  - Web browser with HTTPS (not supported for IBM Director 5.20 systems)
  - Any SNMP manager with SNMP

- **Managed system running a supported non-Windows operating system**
  - IBM Director Server with IPC
  - Any SNMP manager with SNMP

These access methods are listed in descending order of security, from most secure to least secure, assuming the following guidelines are used to maximize security of each method.

In the following sections we discuss the IPC and SNMP methods:

- 3.4.6, “IBM Director Server access control” on page 134
- 3.4.7, “IBM Director encryption” on page 141
- 3.4.8, “SNMP access control” on page 145

### 3.4.6 IBM Director Server access control

The process by which the management server gains access to a managed system depends on the agent level of the system.

Requesting access to Windows managed systems provides some challenges if domain credentials are supplied. The format of the *user name* and *domain name* varies depending on the level of IBM Director Agent installed on the managed system. Refer to Table 3-3 for acceptable formats for supplying domain credentials to Windows-based systems.

<table>
<thead>
<tr>
<th>Director agent level</th>
<th>Domain credential formats accepted</th>
</tr>
</thead>
</table>
| Level-0 (agentless)    | *username@domain*  
                          | Blank passwords are not acceptable.                                    |
| Level-1 (core services)| *username@domain*  
                          | *domain\username*  
                          | Blank passwords are not acceptable.                                    |
| Level-2 (full agent)   | *domain\username*  
                          | Blank passwords are not acceptable.                                    |
Level-0 systems
For Level-0 systems (agentless), the process depends, generally, on the operating system of the target. More accurately, it depends on the protocol used for communication. By default, IBM Director uses DCOM to communicate with all Level-0 Windows systems, while using SSH for all other operating systems on all platforms. You can choose to use SSH on Windows systems as well by installing the Open SSH software included on the IBM Director installation CD (found in the coresvcs directory).

During Level-0 system discovery, these systems are discovered and added to the management console in a secure state (padlock icon). Management of these systems is not possible until access is granted using the request access task.

Requesting access to Level-0 Windows systems
Level-0 Windows systems require an account with local administrative privileges to successfully be granted access from the request access task. You can specify either a local administrative account or domain administrative account, but you must specify the account in one of the following formats:

- `username` (local accounts)
- `username@domain` (domain accounts)

If the user name on a Windows Level-0 secured system is a local system account and the same user name exists as a domain account, IBM Director will use the local account for authentication, unless you specify the domain using `username@domain`. This can cause problems if you have a domain account with the same user name as a local account.

Tip: You cannot use the syntax `domain\username` to unlock Level-0 systems.

Level-1 systems
For Level-1 systems (IBM Director Core Services), SSL is used to secure all communication. When IBM Director Server is installed, a self-signed security certificate is created. During Level-1 system discovery, these systems are discovered and added to the management console in a secure state (padlock icon). Management of these systems is not possible until access is granted using the request access task.

Requesting access to Level-1 Windows systems
Level-1 Windows systems require an account with local administrative privileges to successfully be granted access from the request access task. You can specify
either a local administrative account or a domain administrative account, but you must specify the account in one of the following formats:

- `username` (local accounts)
- `username@domain` or `domain\username` (domain accounts)

**Tip:** Unlike Level-0 or Level-2, you can use either `username@domain` or `domain\username` to unlock Level-1 systems.

Upon acceptance of the proper request access credentials, the security certificate is pushed to the CIMOM (WMI for Windows, Pegasus for all other operating systems and platforms) on the managed system. This certificate is used to open a secure pipe between IBM Director Server and the managed system for all subsequent sessions.

**Tip:** The `certmgr` command, available in the DIRCLI command-line interface to IBM Director Server, can be used to generate, import, distribute, and revoke security certificates for Level-1 managed systems. Note, however, that the certificates created using this command expire after one year.

For more information about this and other DIRCLI commands, see Appendix A, “IBM Director commands,” in the *IBM Director Systems Management Guide*.

**Level-2 systems**

For Level-2 systems (IBM Director Agent), the process is a bit more complex, although invisible to the management console user. It works like this:

1. IBM Director Server attempts to access IBM Director Agent. IBM Director Server bids the public keys that correspond to the private keys it holds.
2. IBM Director Agent checks these keys. If it considers the keys to be trusted, IBM Director Agent replies with a challenge that consists of one of the trusted public keys and a random data block.
3. IBM Director Server generates a digital signature of the random data block using the private key that corresponds to the public key included in the challenge. IBM Director Server sends the signature back to IBM Director Agent.
4. IBM Director Agent uses the public key to verify that the signature is a valid signature for the random data block. If the signature is valid, IBM Director Agent grants access to IBM Director Server.

The following sections describe this process in more detail.
**Requesting access to Level-2 Windows systems**

Level-2 Windows systems require an account with local administrative privileges to successfully be granted access from the request access task. You can specify either a local administrative account or a domain administrative account, but you must specify the account in one of the following formats:

- `username` (local accounts)
- `username\domain` (domain accounts)

**Tip:** You cannot use the syntax `username@domain` to unlock Level-2 systems.

**Windows authentication issues**

Issues can arise if you have duplicate user names for local users and domain users or supply domain credentials in the incorrect format, which may prevent you from accessing Windows-based managed systems.

**Scenario 1**

Local administrator account - user name: JohnD, password: 1234  
Domain administrator account - JohnD, password: 5678

If you request access to the system with the user name JohnD, IBM Director uses the local system account JohnD and will authenticate against password 1234. If you specify JohnD with the password 5678, the request will fail, as the password is incorrect for the local system account. You should specify the local system account JohnD with the password 1234 or specify the domain account `JohnD@domain` (Level-0, Level-1) or `domain\JohnD` (Level-1, Level-2) with the password 5678 to gain access.

**Scenario 2**

Local user account - user name: JohnD, password: 1234  
Domain administrator account - JohnD, password: 5678

If you request access to the system with the user name JohnD, IBM Director uses the local system account JohnD and will authenticate against password 1234. If you specify JohnD with the password 1234, the request for access will fail, as the user does not have local administrative privileges. If you specify JohnD with password 5678, the request will fail, as the password is incorrect for the local system account. You need to specify `JohnD@domain` (Level-0, Level-1) or `domain\JohnD` (Level-1, Level-2) with the password 5678 to gain access.

**Initial managed system contact**

Since IBM Director Agent has full control of the managed system, it is important to understand how IBM Director Server contacts a managed system, and
subsequently tries to manage it. Consider this: If someone installs an unauthorized IBM Director Server on your network and initiates system discovery, any unsecured systems discovered could be managed by that rogue management server.

IBM Director Agent can be installed such that it will initiate discovery upon its first startup. This is perhaps the most secure method of discovery, because the managed system can be set to announce itself to a specific management server and that management server can be configured to secure each IBM Director Agent that makes contact. For more on this see “Agent-initiated discovery” on page 111.

If you choose not to implement agent-initiated discovery, IBM Director Server can contact IBM Director Agent either explicitly or by discovery:

- **Explicit initial contact**
  An administrator can identify a system for IBM Director Server to contact by entering the name, protocol, and address used by that system. The management server will use this data to initiate contact with that particular system.

- **Discovery**
  IBM Director Server can use a discovery process to locate systems to be managed in the network. The management server sends out discovery packets, then listens for responses from IBM Director Agents.

  IBM Director Server can use four types of discovery: broadcast discovery, multicast discovery, Unicast discovery, and broadcast relay agents. For further details about each of these discovery types and information about how to configure each, refer to 2.8.2, “Server-initiated discovery” on page 56, of this book; and Chapter 3 of the *IBM Director Planning, Installation, and Configuration Guide*.

**Server-agent authentication**
Once the managed system and management server recognize one another, IBM Director Agent must determine whether the IBM Director Server requesting access is a known and trusted entity. As you will recall from 3.1.4, “Security protocols” on page 96, DSA encryption uses a one-way private/public key-pair encryption algorithm. Any data encrypted by one key can only be decrypted by the other. In a public key-private key setup, the private key is kept only by the authenticating entity (the management server in this case), while the public key is freely distributed. IBM Director uses this capability for the management server to authenticate itself to managed systems.
This digital signature scheme has the following benefits:

- The public keys stored on the managed systems can be used only for verifying access.
- Using a random data block for signing makes replay attacks unusable.
- Generating a private key corresponding to a given public key is cryptographically improbable, requiring \(2^{128}\) or more operations to accomplish.
- As this process is executed for each IPC session between the management server and the managed system, the odds against cracking the private key increase even further.

IBM Director Server offers the DSA public keys it possesses as authentication tools. This process is sometimes referred to as bidding its keys. One management server can possess multiple DSA public keys. In fact, this is typical when multiple IBM Director Servers exist in the same environment, as IBM Director Agent is part of a management server configuration.

IBM Director Agent checks to see whether it already possesses any of the public key files that have been bid. If it does, it continues the authentication process with the management server (see “Authentication challenge” on page 140). If the managed system does not already possess one of the public keys bid, the next step depends on the security state of IBM Director Agent. If it is set to the secured state, the managed system will only allow access to management servers from which it received digital signature keys (DSA*.PUB files) prior to being set to the secured state.

- Unsecured state

  The managed system accepts all of the public keys bid by the management server, storing them for future authentication, and responds to the management server, confirming that it is in an unsecured state. The authentication process proceeds as described below.

  After authentication succeeds and the IPC session is opened, a check of the discovery preferences on the management server is executed. If the managed system is Windows-based and if the management server is configured to automatically secure unsecured systems, it copies its SECI3.INI file to the managed system, thereby placing it in the secured state. The server-agent session proceeds.

- Secured state

  The management server still discovers the managed system, but the managed system cannot actually be managed, and will appear as inaccessible, with a padlock symbol (🔒) next to the system icon in the IBM Director Console.
To manage this system you must request access. Right-click the inaccessible system and select Request Access. Specify an account with administrative privileges (see Table 3-3 on page 134 for Windows systems if you are using a domain account, or use root in Linux) on the system you are attempting to access. Note that you can select multiple systems before requesting access by using Shift+click or Ctrl+click. In this manner, you can request access to all systems using the same credentials in a single operation.

**Note:** Linux and UNIX managed systems are secured by default.

![Request Access to Systems](image)

CHAP is used to authenticate the credentials supplied in this window. If the user name and password are valid, IBM Director Server is granted access, the server’s DSA*.PUB file is copied to the managed system, and you receive a confirmation message.

**Authentication challenge**

If IBM Director Agent does have one or more keys, it selects one of these public keys, generates a random block of data, and challenges the management server with the public key it has selected and the random data block. The management server then encrypts this random data block using the *private* key (DSA*.PVT files) corresponding to the public key sent by the managed system, and responds with the encrypted data.

IBM Director Agent decrypts the data block using the management server’s public key and compares it to the original data block transmitted. This public key
can successfully decrypt only data that has been encrypted using its corresponding private key. Because only the management server possesses the private key, if the data block decrypts successfully then the management server is authenticated. If the data does not decrypt successfully, then the management server is rejected and the IPC session is not established.

Upon successful authentication, the management server checks the encryption setting for the managed system. If encryption is enabled (which is done during IBM Director Agent installation), then secure IPC communication begins. If the managed system does not have encryption enabled, then the IPC connection is made using plain text communication.

### 3.4.7 IBM Director encryption

This section describes how to enable encryption between IBM Director components.

**Console-server encryption**

IBM Director offers support for Secure Sockets Layer (SSL) to protect data flowing between IBM Director Server and IBM Director Console. In previous versions of IBM Director, you had to modify properties files on the management server and management console to enable SSL communication between these components.
Beginning with IBM Director 5.10, you can choose whether to use SSL security between the management server and the management console during each logon simply by selecting the **Use SSL** box in the IBM Director Login window, as shown in Figure 3-16. There are no special requirements needed during installation or during initial configuration to make use of SSL.

![IBM Director Login window with SSL security enabled](image)

**Figure 3-16   IBM Director Login window with SSL security enabled**

**Agent-server encryption**

You can also choose to encrypt the interprocess communication (IPC) between the management server and managed systems. IBM Director Server to Agent communication uses Diffie-Hellman key exchange, along with encryption based on the DES, Triple-DES, or AES standards.

In previous releases of IBM Director, a single encryption key was used for all managed systems. Beginning with IBM Director 5.10, the management server generates a unique, symmetric key for each Level-2 system and sends that key to IBM Director Agent using the Diffie-Hellman protocol. The use of multiple keys, unique to each managed system, has implications for encryption administration, which are discussed below.

To encrypt IPC traffic, you must enable encryption on both IBM Director Server and IBM Director Agent, which is an option during installation. In a change from previous versions, encryption is now enabled by default during installation of both IBM Director Server and IBM Director Agent.
The encryption standard used is based on the method selected on the management server. The default method during installation is now AES, which is the most secure of the three methods offered. You can modify the encryption options on the management server after installation. To do this, from the management console click **Options → Encryption Administration.** This brings up the Encryption Administration window shown in Figure 3-17. Check **Enable encryption of data using** and select the desired encryption method before clicking **OK.**

![Encryption Administration window](image)

**Figure 3-17** Encryption Administration window with the proper selections made to enable AES encryption between the management server and console

To modify encryption settings on IBM Director Agent running under Windows, do the following:

1. Select **Add/Remove Programs** in Control Panel.
2. Select **IBM Director Agent** from the list of installed programs.
3. Click **Change** to start the installation wizard.
4. Click **Modify.**

**Important:** Encryption is not supported for managed systems running NetWare, nor any Itanium-based managed system. Also, out-of-band management tasks such as SNMP, Telnet, and FTP are not secured by encryption.
5. Proceed through the install dialog boxes without changing other settings.
6. In the Security Settings window (Figure 3-3 on page 110) you can enable or disable encryption between agent and server.

To modify encryption settings on IBM Director Agent running under Linux or AIX, do the following:

1. Stop the IBM Director Agent using the `twgstop` command.
2. Run the command `cfgsecurity` (in the `/opt/ibm/director/bin` directory).
3. Follow the instructions that are displayed to configure encryption settings.
4. Restart IBM Director Agent when configuration is complete.

The management server automatically generates a unique key for each encryption-enabled Level-2 managed system based on the encryption algorithm selected. IBM Director Server stores these keys in memory and presents them to each managed system each time IBM Director Agent is started. This makes it unnecessary for a key to be stored on each managed system.

When either the management server or a Level-2 managed system is restarted, encryption keys are regenerated and exchanged using the Diffie-Hellman protocol. When a Level-2 managed system is shutdown gracefully, the management server receives a shutdown ping from IBM Director Agent. It then removes that system from its list of active systems to which it has sent keys. When IBM Director Agent is restarted, it contacts the management server using bootping, signaling the server to generate a new unique key and send it to the managed system. The management server also resends a key on a presence check if necessary (for example, if a Level-2 managed system is shutdown or powered off immediately).

During any period where the key held by IBM Director Agent does not match the current unique key assigned to it by the management server, the managed system appears with a question mark icon (_QUESTION_MARK_). As soon as new keys have been exchanged, the question mark is removed. This provides the user with a visual indication of the condition.
You can resend encryption keys from the management server to all managed systems using the Encryption Administration window shown in Figure 3-17 on page 143. Simply click **Resend**. The Encryption Administration Success window should be displayed, as shown in Figure 3-18.

![Encryption Administration Success window](image)

*Figure 3-18  Encryption Administration Success window, showing successful resending of encryption keys to all IBM Director Agents*

You can also regenerate an encryption key for a specific managed system. To do this, right-click a managed system and select **Reset Encryption Keys**. IBM Director Server regenerates a new, unique key for the managed system.

It is important to understand that both IBM Director Agent and IBM Director Server must have encryption enabled before secure transmission takes place, as shown in Table 3-4. Also, keep in mind that if the management server has encryption disabled, it is not able to communicate with any IBM Director Agents that have encryption enabled. These managed systems would show up as unmanageable Level-2 systems and display the padlock icon (🔑).

<table>
<thead>
<tr>
<th></th>
<th>IBM Director Agent (encryption enabled)</th>
<th>IBM Director Agent (encryption disabled)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Director Server</td>
<td>Encrypted</td>
<td>Unencrypted</td>
</tr>
<tr>
<td>(encryption enabled)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM Director Server</td>
<td>No data transmission possible</td>
<td>Unencrypted</td>
</tr>
<tr>
<td>(encryption disabled)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 3.4.8 SNMP access control

SNMPv1 and SNMPv2 have only the most rudimentary security. SNMPv3 has more robust security, and so should be used whenever possible. However, it is not necessary to use SNMP at all in an IBM Director managed environment. If you are not currently using SNMP to manage systems or network devices and do not plan to use IBM Director to monitor SNMP traps, it is not necessary to install or configure this functionality.
It is possible to use the SNMP protocol to communicate with IBM Director Agent. Access to the managed system with SNMP is controlled by a community string. This alphanumeric string identifies a community of SNMP agents and servers. Based on this string and the address of the sender, the SNMP protocol will accept or reject commands from a management server.

In addition, different communities can have different levels of access to a particular agent. The community *public* generally has read-only access. Depending on how you intend to use SNMP for managed systems in your environment, you might want to enable read-write access.

In Figure 3-19 we see the Windows 2000 SNMP Security Configuration window, accessible from the SNMP Service in the list of services in Control Panel.

![Figure 3-19 Windows 2000 SNMP Security Configuration window](image)

This system is configured to accept SNMP packets from the default community named *public*, and to accept SNMP packets from any host.

As the community string *public* is well known, and as SNMP provides such limited security, it is important to define SNMP security standards and make sure that they are implemented on each managed system. We recommend that you remove the *public* community name completely and add a unique community
name for your environment, such as Director. In any case, it is definitely not a good idea to allow read/write access to the public community.

For additional security, you might also select **Accept SNMP packets from these hosts** and add your management servers to the authorized list. Figure 3-20 shows how the window might look after it is properly configured.

![Image of SNMP Service Properties window]

Figure 3-20   Example of properly configured SNMP security properties

IBM Director Agent enables you to modify SNMP settings using the Web browser or MMC interface. However, using this approach means that you must change these settings on each IBM Director Agent individually. This is little better than having to visit each managed system physically to make the appropriate changes.

A much better method is to use the **mass configuration** feature of IBM Director to make SNMP configuration changes to entire groups of managed systems with a single operation. See 6.4, “Mass Configuration” on page 366, for details.
IBM Director installation

This chapter is an addendum to the installation chapters in the product publication *IBM Director Planning, Installation, and Configuration Guide* and provides additional and deeper information about how to install the BMC and RSA-II service processors and IBM Director.

Topics covered here are:

- 4.1, “Express installation” on page 150
- 4.2, “SteelEye LifeKeeper for high availability” on page 166
- 4.3, “Server Plus Pack considerations” on page 177
- 4.4, “System x service processors” on page 179
- 4.5, “Installing service processor drivers for ESX Server” on page 194
- 4.6, “Automating the installation process” on page 201
- 4.7, “Troubleshooting IBM Director Agent installation” on page 215
- 4.8, “Uninstall” on page 224
4.1 Express installation

New in IBM Director 5.20 is the option to perform an *express* installation of the management server. *IBM Director Express* is a simplified installation that installs IBM Director Server using default values for a number of installation options. The resulting management console will display a filtered task list, allowing the user to start with a core set of essential tasks. Additional tasks can be added to the console after installation.

IBM Director Express is intended to provide a simplified installation mechanism and management console for those customers needing to manage a small IT infrastructure. It is also suitable for those who are interested in getting up and running with IBM Director as quickly as possible, allowing for additional functionality to be added after initial installation.

4.1.1 Express or standard

Before installing IBM Director Server, consider the differences between performing an Express installation and performing a standard installation, as shown in Table 4-1.

<table>
<thead>
<tr>
<th></th>
<th>Standard installation</th>
<th>Express installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>You select the database that you will use and provide configuration information during installation.</td>
<td>Apache Derby database is automatically installed and configured for IBM Director.</td>
</tr>
</tbody>
</table>
| Event action plans     | No event action plans are created by default.                  | An event action plan is created on installation, which automatically creates Update Manager profiles when inventory is collected for new types of managed objects. Additionally, when you first start IBM Director Server, the Event Action Plan wizard is started so you can create event action plans.
<table>
<thead>
<tr>
<th></th>
<th>Standard installation</th>
<th>Express installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Action Plan wizard</td>
<td>The standard Event Action Plan wizard is available.</td>
<td>The Event Action Plan wizard does not include security events or IBM Director Agent offline event filters. In addition, you cannot specify a time range for event action plans. The time range is always 24 hours.</td>
</tr>
<tr>
<td>IBM Director extensions</td>
<td>Extensions can be installed, as long as the specific requirements for the extension are met.</td>
<td>Extensions should not be installed for IBM Director after an Express installation.</td>
</tr>
<tr>
<td>Initial discovery of managed systems</td>
<td>You must manually configure discovery preferences and start discovery.</td>
<td>When you start IBM Director the first time, you are prompted to enter Level-0 discovery options in the Express Start wizard, then discovery is performed.</td>
</tr>
<tr>
<td>Security</td>
<td>You must manually configure security event notifications.</td>
<td>Ticker-tape display of security events is automatically configured.</td>
</tr>
<tr>
<td>Tasks</td>
<td>All tasks are available to users after installation.</td>
<td>The following subset of tasks is available to users after installation:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Inventory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Event Action Plans</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Event log</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- File transfer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Hardware status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remote control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Software Distribution</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Update Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>After installation, you can make other tasks available to users.</td>
</tr>
</tbody>
</table>

At the time of this writing, various IBM Director documents state that if you want to install an IBM Director extension into IBM Director Express you must uninstall IBM Director Express and reinstall, using the standard installation option. This is not true. The Express installation does not install a *crippled* version of IBM Director. All internal capabilities and mechanisms are installed—only the management console presentation of functionality is changed. For more information about converting to a standard installation, see 4.1.3, “Converting Express installation to standard” on page 159.
4.1.2 Performing an Express installation

To perform an Express installation, simply select the appropriate check box on the Installation Type page of the installation wizard, as shown in Figure 4-1.

IBM Director provides several first-time-use startup activities to help integrate IBM Director Server into the Small and Medium Business space.

The Express Installation option provides the following conveniences:

- Decreases the number of panels that are displayed during the installation
- Installs a subset of the tasks for IBM Director Console
- Launches a new EAP wizard when you initially start IBM Director

Figure 4-1  IBM Director Server installation window with Express installation selected
Once Express installation has been selected, there are very few choices to be made during the rest of the installation. You can choose the install directory, as shown in Figure 4-2, but we recommend *always* using the default installation directory for IBM Director, unless there is a compelling reason to choose a different location.

Figure 4-2  IBM Director Express installation asking where to install
As in any IBM Director Server installation, you must provide credentials for the IBM Director Server service account, including the local computer name or domain name, and the service account user name and password. This is shown in Figure 4-3.

![IBM Director service account information](image)

*Figure 4-3  Express installation asking for service account credentials*

For important considerations that need to be made regarding the service account, see 3.4.2, “IBM Director service account” on page 120.
As in any IBM Director Server installation, you must specify the directory in which to place software distribution packages. Note that this now includes a third directory for Update Manager packages, as seen in Figure 4-4.

![IBM Director Server - InstallShield Wizard](image)

**Figure 4-4** Express installation asking for software distribution installation directories

Additional information about this important new task is available in Chapter 7, “Update Manager” on page 411.
With these few decisions made, Express installation is ready to begin the install, as seen in Figure 4-5.

![IBM Director Server - InstallShield Wizard](image)

**Figure 4-5  Express installation is ready to begin**

After completing an Express installation of IBM Director, you can use the Express Start wizard to configure the settings that are applicable to your environment. When you first start IBM Director Console after an Express installation on the management server, the Express Start wizard is launched automatically.
This consists of two steps, the Express Start window and the Event Action Plan wizard. First, discovery preferences are configured in the Express Start window, as shown in Figure 4-6. If you want to perform discovery on Level-0 (agentless) systems, select the check box and specify an appropriate IP address range. If you do not want to discover agentless systems, leave this check box unselected.

![Express Start window](image)

**Figure 4-6**  Express Start wizard allows setup of discovery preferences

Once you click **OK**, the Event Action Plan wizard is launched to help configure initial event notification. See 12.2, “The Event Action Plan Wizard” on page 677, for more on this topic.

**Note:** The Event Action Plan Wizard that is launched during Express installation does not include the security events or IBM Director Agent offline event filters. In addition, you cannot specify a time range for event action plans. The time range is always 24 hours.
Once the Event Action Plan wizard has completed, IBM Director Console opens and discovery is performed according to the selections made in the Express Start wizard. Notice in Figure 4-7 that only a few of the tasks normally available along the button bar are available immediately after installation. Additional tasks can be added after Express installation has been performed.

Figure 4-7  IBM Director Express management console
4.1.3 Converting Express installation to standard

It is possible to convert IBM Director Express to a standard installation without a full uninstall/reinstall cycle. In fact, the process is quite simple. To do this, follow these steps:

1. Open the Add or Remove Programs control panel on the management server, as shown in Figure 4-8. Locate IBM Director Server in the list and click Change.
2. When the InstallShield Wizard opens, as shown in Figure 4-9, click **Modify**.

![InstallShield Wizard](image)

*Figure 4-9  InstallShield Wizard allows modification and repair of management server*
The wizard bypasses the window on which you initially chose the Express installation method. You are taken directly to the Feature and installation directory selection window, as shown in Figure 4-10.

Figure 4-10  Feature and installation directory selection window
3. Make your selections, as shown in Figure 4-11, and click **Next**.

![Figure 4-11](image1.png)

*Features have been selected for modified installation*

The Ready to Modify the Program window is presented, as shown in Figure 4-12.

![Figure 4-12](image2.png)

*Installation is ready to proceed*
4. Click **Install** to begin the installation of any features you added on the previous window.

After installation is complete, the network driver configuration application opens, as shown in Figure 4-13. Note that this step was skipped during the initial Express installation.

![Network driver configuration window](image)

*Figure 4-13  Network driver configuration window allows customization*
5. Make configuration changes in this window as desired and click **OK** to save your changes and close the window.

The IBM Director database configuration window opens, as shown in Figure 4-14. This step was also skipped during Express installation.

![Database Configuration Window](image)

**Figure 4-14**  Database selection can be made during modified installation

6. Make your database selection and click **Next**. If you choose Use existing database configuration, IBM Director Server will use the same Apache Derby database from the previous Express installation and the current installation will finish without requiring a reboot. All discovered objects and inventory data will remain intact.

7. To finish the reconfiguration, open the management console and access the user administration function.
8. Open the User Editor for the account under which you performed the Express installation, as shown in Figure 4-15. You will need to deselect the **Limit user access to only the selected tasks** check box in order to allow the user to see all IBM Director tasks, rather than the limited number provided by IBM Director Express.

![User Editor](image)

*Figure 4-15 User Editor allows granting of full access to all tasks if desired*

You are now working with a fully functional **standard** version of IBM Director Server. The only difference we have seen after this modified installation is that any account with local administrator rights on the management server has what amounts to super-user rights for management server access, even though it is not a member of the DirSuper group.
4.2 SteelEye LifeKeeper for high availability

SteelEye offers a high-availability toolkit for IBM Director Server called LifeKeeper Protection Suite for IBM Director. Any true (that is, production) high-availability IBM Director solution should be based on one of the supported external databases. However, you can download the SteelEye solution and use it for no charge on an Apache Derby-based management server for the purpose of proof-of-concept.

At the time of this writing, LifeKeeper supports IBM Director Server installed on a Windows server and using the Apache Derby, Microsoft SQL Server, or Oracle databases.

It is important to decide whether you will implement a highly available management server before installing IBM Director Server, since the cluster environment and data replication must be installed and configured prior to IBM Director Server installation.

4.2.1 LifeKeeper overview

LifeKeeper constantly monitors IBM Director Server processes and the database to ensure that all components are properly working. If a failure is detected, LifeKeeper performs the necessary actions to return the management server to operation. LifeKeeper also supports manual switchover of IBM Director Server processes to and from the standby system, so that planned maintenance can be performed without downtime.

Using the LifeKeeper Protection Suite for IBM Director provides the following benefits:

- Eliminates IBM Director Server as a potential single-point-of-failure
- Ensures that appropriate alerts continue to be sent on hardware health issues
- Allows any needed hardware maintenance of the IBM Director Server without losing access to important management tasks
- Continues proactive management through event action plans
- Provides the highest levels of availability possible for your IT management infrastructure

The LifeKeeper IBM Director Recovery Kit software makes IBM Director Server services highly available through the clustering technology provided by LifeKeeper for Windows. LifeKeeper monitors the IBM Director Server service and the associated IP communication resource.
Making IBM Director Server highly available is accomplished by configuring the IBM Director Server service and its clients to use a virtual server name and a protected IP address rather than the name of any specific server it is installed on. Using this approach, IBM Director Server can be run on either a primary or a backup server while using the same database. Figure 4-16 illustrates a LifeKeeper protected management server.

![Figure 4-16 SteelEye LifeKeeper Protection Suite for IBM Director](image)

LifeKeeper protects the disk resources used by IBM Director Server, as well as the IP addresses used to access them. In addition, the LifeKeeper IBM Director Recovery Kit monitors and protects the following services:

- TWGIPC (IBM Director Support Program)
- TWGSERVER (IBM Director Server)

Should these services stop unexpectedly, or if the system experiences a catastrophic failure, they will be restarted locally or restarted on another server in the cluster in the order and priority selected by the administrator. The recovery kit also runs an IBM Director command periodically to check whether IBM Director Server service is running. If this check fails, LifeKeeper will restart all IBM Director services locally or fail over the complete resource hierarchy to another server in the cluster. Local recovery is an optional setting for each resource instance.
4.2.2 LifeKeeper GUI

The LifeKeeper GUI allows you to create a complete IBM Director Server resource hierarchy and monitor the state of all components of the highly available environment. The GUI can be accessed natively (as in Figure 4-17), or through a browser (as in Figure 4-18 on page 169).

Figure 4-17  SteelEye LifeKeeper GUI-based interface
As you can see, both user interfaces are identical, providing familiar controls and configuration options regardless of your method of launching the tool.

![SteelEye LifeKeeper browser-based interface](image)

Figure 4-18  SteelEye LifeKeeper browser-based interface

### 4.2.3 HA setting

After installation and configuration of LifeKeeper components and IBM Director Server, you should enable the HA setting for the management server, which is a new option, beginning with IBM Director 5.20.

Normally, the default IBM Director Server configuration provides an acceptable balance between reliability and performance. In some situations, some intermediate data might be lost, but performance is not adversely affected by near-constant logging of events to disk. However, you can choose to improve reliability in high-availability environments, at the cost of decreased performance, particularly with regard to event processing.
With IBM Director configured for high-availability environments, very little data is likely to be lost because of unexpected failovers, but performance might be negatively impacted by logging events to disk and increased redundancy in disk write operations. Enabling the high-availability configuration also enables some tasks, such as inventory collection, to save checkpoints while they are running. If a failover occurs, the task continues from the last saved checkpoint rather than starting from the beginning.

To enable the high-availability configuration for IBM Director Server, add the following line to the TWGServer.prop file:

```
HA.enabled = true
```

Restart IBM Director Server after making this change.

For more information about IBM Director Server high-availability configuration, see Chapter 3 in the *IBM Director Planning, Installation, and Configuration Guide*.

### 4.2.4 Automated failover

In our lab, we installed LifeKeeper Protection Suite for IBM Director, using Apache Derby as the systems management database. In our testing, all IBM Director Server services and connectivity failed over successfully to the standby server in the event of system or network failure.
Figure 4-19 shows an active LifeKeeper cluster in its normal state of operation. Argon is our primary IBM Director Server and is marked *Active*. Potassium is the backup server and is marked *Standby*. Calcium is the virtual system name given to the pair and registered with DNS. All management consoles target Calcium for login. Replicated is the tag given to the replicated volume on which IBM Director Server is installed.

*Figure 4-19  LifeKeeper GUI shows normal operation and status of IBM Director Server*
When we unplug the network cable from the primary management server (Argon) and LifeKeeper can no longer communicate with it, its status is marked *Unknown*, as shown in Figure 4-20.

*Figure 4-20  LifeKeeper has lost communication with the primary management server*
After a specified amount of time, LifeKeeper begins the failover process. First, ownership of the replicated volume is transferred to our backup management server. This replicated volume includes the installation directory for the single IBM Director Server installation that is shared between the two management servers. Once ownership of the replicated volume is changed, it is marked *Active* under the owning system, as shown in Figure 4-21.

*Figure 4-21  LifeKeeper begins failover by transferring ownership of replicated volume*
Next, the IP address and virtual system name are moved to Potassium, the backup management server. Figure 4-22 shows completion of this step in the failover process. The virtual system name of our management server, Calcium, is marked as *Active* under the backup server.

*Figure 4-22  LifeKeeper transfers ownership of virtual server name and IP address*
At this point LifeKeeper starts IBM Director Server services on our backup server, as seen in Figure 4-23. As usual, it takes a few minutes to start all of the processes. LifeKeeper waits for IBM Director Server to become fully available, sending an IBM Director command periodically to check whether all services are running.

![Figure 4-23  LifeKeeper starts IBM Director services on backup server](image)

The screenshot shows the process of bringing IBM Director services into service, with successful starts for various services.

Figure 4-23  LifeKeeper starts IBM Director services on backup server
Once LifeKeeper receives confirmation from Potassium that all IBM Director services are running, it marks Potassium as *Active*, as seen in Figure 4-24. We can once again open IBM Director Console against Calcium. Notice that the management server is still marked *Unprotected*, since LifeKeeper still cannot communicate with Argon.

*Figure 4-24  LifeKeeper marks backup server as Active*
When we plug the network cable back into Argon, LifeKeeper reestablishes communication and marks our environment *Active Protected*, as shown in Figure 4-25. Notice that Argon is now our Standby server. We can leave the configuration this way, or we can bring our primary management server *In-Service* through a simple right-click operation. We also could have configured LifeKeeper to automatically fail back to Argon when communication was restored.

![LifeKeeper GUI](image)

*Figure 4-25  Communication with primary server restored, active protection initiated*

### 4.2.5 More information

For more information about SteelEye LifeKeeper Protection Suite for IBM Director or to download this solution, see SteelEye’s site at:

http://www.steeleye.com/partners/technology/ibm/director.html

### 4.3 Server Plus Pack considerations

If you intend to upgrade IBM Director 4.x that includes Server Plus Pack to version 5.x, it is important to read and understand this section.
Version 4.x of IBM Director supported a fee-based group of extensions called the Server Plus Pack (SPP), which has now been discontinued. There were five extensions in the Server Plus Pack:

- Rack Manager is now part of the base IBM Director product.
- Active PCI Manager has been discontinued and is no longer available.
- Software Rejuvenation has been discontinued and is no longer available.
- System Availability is now a free downloadable extension, downloadable from:
  

- Capacity Manager is now a fee-based extension that can be added to a base IBM Director installation.

See 1.5.2, “IBM Director Extensions” on page 14, for more information about System Availability and Capacity Manager.

The actions you perform to ensure a successful upgrade depend on the operating system and IBM Director 4.x component that is installed:

- Under Linux, if you use the dirinstall scripts to install IBM Director 5.x, SPP extensions are removed prior to the new version being installed. The proper uninstall commands are already in place in the various dirinstall scripts.

  On the other hand, if you use standard RPM commands, you bypass the automatic removal of the SPP extensions. These would have to be manually removed using the `rpm -e <pakage_name>` RPM command after installation.

- Under Windows installations of IBM Director Server and Console 4.x, SPP extensions were built into the product (there were no separate SPP installers to run on the Server or Console). When you uninstall Server or Console Version 4.x, SPP extensions are uninstalled as well. Therefore, there is no need to take special action.

- Under Windows installations of IBM Director Agent 4.x, SPP extensions were installed separately from the Agent, resulting in separate uninstall routines for each installed extension. Therefore, the upgrade installer is not able to remove them. They remain on the system but do not work. Tests have confirmed that these orphaned extensions do not interfere with the operation of IBM Director 5.x, but we recommend that you remove these obsolete tools.

  The simplest way to do this is to manually uninstall each of the SPP extensions before proceeding with IBM Director Agent 5.x upgrade.

  If you have already upgraded without uninstalling the SPP extensions manually, they can be removed by running the following command:

  `msiexec /qb /x product_code`
Where *product_code* is found in Table 4-2.

The { }’s are part of the *product_code*. The /qb tells the uninstaller to run in an unattended fashion, but display progress and any errors. If you want the uninstaller to run silently (where errors are just logged), use /qn instead of /qb. If you have many agents that are affected, we recommend creating a process task in IBM Director with each of the uninstall commands. This process task can be executed against a group of target systems in the normal fashion, effectively automating this process. Perform the uninstallation before or after the upgrade to IBM Director Agent 5.x.

**Table 4-2  Product codes for obsolete Server Plus Pack Agent extensions**

<table>
<thead>
<tr>
<th>SPP component</th>
<th>Product code</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1x Capacity Manager</td>
<td>{09BF50B0-32DA-4CCA-A8E9-14A88E008A4A}</td>
</tr>
<tr>
<td>4.1x Software Rejuvenation</td>
<td>{44F3E63B-D6DE-4264-8F4B-027DED9FCFAD}</td>
</tr>
<tr>
<td>4.1x System Availability</td>
<td>{E73049CD-AC54-42AA-BC97-F515129DFC52}</td>
</tr>
<tr>
<td>4.1x Active PCI Manager</td>
<td>{6DC6B56A-091B-467A-AF71-A9C8427A8541}</td>
</tr>
<tr>
<td>4.2x Capacity Manager</td>
<td>{2BB5F893-5990-4DB3-9883-127A7058B679}</td>
</tr>
<tr>
<td>4.2x Software Rejuvenation</td>
<td>{CD06DFFA-65FA-447E-8F28-680B151AD383}</td>
</tr>
<tr>
<td>4.2x System Availability</td>
<td>{386A7A61-3B95-423D-A0D0-9CB0156697F1}</td>
</tr>
<tr>
<td>4.2x Active PCI Manager</td>
<td>{84924454-DE12-4494-AAB6-5C9B342D0FBF}</td>
</tr>
</tbody>
</table>

### 4.4 System x service processors

Most IBM System x servers ship with a service processor. Current service processors are:

- **Baseboard Management Controller (BMC)**

  The BMC in System x servers provides the environmental monitoring for the server. If environmental conditions exceed thresholds or if system components fail, the baseboard management controller lights LEDs to help you diagnose the problem, and records the error in the BMC System Event/Error log. The BMC can also be used to remotely control power to the server, and offers text-based console redirection with the system Ethernet port using Serial over LAN (SOL).

- **Remote Supervisor Adapter II (either the PCI or SlimLine versions)**

  The Remote Supervisor Adapter II (RSA II) is the top-of-the-line systems management adapter for System x servers. It provides many options for
alerting, monitoring, and remote management of System x servers. There are three versions of the RSA II that provide similar functionality:

- Remote Supervisor Adapter II
- Remote Supervisor Adapter II-EXA
- Remote Supervisor Adapter II SlimLine

The RSA II offers high-performance remote control capabilities including to map a CD or diskette drive to the remote server for software installation, including remote installation of a complete operating system. The RSA II is remotely managed and configured using its built-in Web interface and provides comprehensive alerting to IBM Director.

In addition, the IBM BladeCenter also comes with a management module that provides similar functions to the RSA II and communicates with the BMCs found on the individual blade servers.

For a list of which System x servers support these service processors, see the technote *Service Processors Supported in IBM System x Servers*, TIPS0146: http://www.redbooks.ibm.com/abstracts/tips0146.html

**Note:** These service processors provide strong management capabilities on their own. These functions are discussed in *IBM eServer xSeries and BladeCenter Server Management*, SG24-6495, available from: http://www.redbooks.ibm.com/abstracts/sg246495.html

Discussing the use of the service processors by themselves is beyond the scope of this book, and we refer readers to the above Server Management book.

In this section we discuss the BMC service processor and Remote Supervisor Adapter II and device driver installation (including the correct installation order).

### 4.4.1 Interaction with IBM Director

Service processors such as the RSA II and BMC can provide important information to IBM Director about the current state of your System x server.

We strongly recommend that you configure your systems so that all alerting information is properly routed to IBM Director for processing and event management. The primary method of achieving this integration is by installing the appropriate service processor device driver before installing IBM Director Agent. This is known as in-band communication.
After the device driver and IBM Director is installed, the service processor should be automatically discovered by IBM Director Server. IBM Director considers service processors to be Physical Platform Managed Objects (PPMOs). When discovery is successful, by default, any events generated by the service processor are automatically sent to the management server. You can then create event action plans, as described in Chapter 12, “Event management” on page 675, to perform actions based on these events.

### 4.4.2 Out-of-band versus in-band communications

Most System x service processors support two methods of communication:

- **In-band communication**
  
  This is the normal method of communication and involves the operating system running on the server and the service processor device driver. If IBM Director Agent is installed on the server, then IBM Director also communicates with the service processor with in-band. With in-band communication, you can also control power with the additional feature of being able to do a graceful shutdown using the operating system.

- **Out-of-band communication**
  
  Most System x servers have the capability to be addressed over TCP/IP, and this form of communication bypasses the software stack running on the server (Director Agent, operating system, driver). As a result, this method of communication can be used even when the operating system is not running.

  Because you are communicating directly with the service processor, the functions available are very much dependant on the device. However, at the very least, you can control power (on/off/restart), controlling the blue information LED and getting hardware status.

  Events detected by the BMC are sent out-of-band as PET events to the IBM Director Server or other PET listener (provided that you have alert forwarding configured). Events detected by the RSA II are sent out-of-band as SNMP events to IBM Director Server (also provided that you have alert forwarding configured).

### 4.4.3 Driver installation

The service processor device lets IBM Director communicate with the service processor in-band, for both alerting from the service processor to IBM Director and control of the service processor by IBM Director. The device driver also enables specific functions such as facilitating the graceful shutdown of the operating system.
Service processor drivers are available for VMware ESX Server, beginning with Version 3.0, and should be installed if IBM Director is used to manage the environment, particularly if the Virtualization Manager extension is used. Details on installing the RSA II driver in this situation can be found in 4.5.1, “RSA II driver installation for ESX Server 3.x” on page 194.

You should always install the service processor device driver before installing IBM Director Agent. If you do not have the driver installed, the IBM Director Agent installer will not install the in-band communication support. Beginning with IBM Director 5.20, the agent installer checks for service processor device drivers prior to installation and will alert you if it finds any issues.

To perform the check, the installer attempts to load the interface library and make a driver call to verify that the driver is properly installed on the system. The messages shown in Table 4-3 are simply warning messages and do not prevent the installation from continuing.

<table>
<thead>
<tr>
<th>OS</th>
<th>Driver</th>
<th>Message type</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>RSA</td>
<td>Popup</td>
<td>Detected system support for RSA, but encountered potential issue with the RSA driver stack. Check the dirinst.log for details.</td>
</tr>
<tr>
<td>Windows</td>
<td>RSA</td>
<td>Log</td>
<td>Detected potential issue with RSA driver. Check for driver updates on IBM Web site.</td>
</tr>
<tr>
<td>Windows</td>
<td>IPMI</td>
<td>Popup</td>
<td>Detected system support for IPMI, but encountered potential issue with the IPMI driver stack. Check the dirinst.log for details.</td>
</tr>
<tr>
<td>Windows</td>
<td>IPMI</td>
<td>Log</td>
<td>Failed to load libibmsp6.so. Ensure that the system has the IBM IPMI driver and library packages.</td>
</tr>
<tr>
<td>Windows</td>
<td>IPMI</td>
<td>Log</td>
<td>Encountered BMC error.</td>
</tr>
<tr>
<td>Windows</td>
<td>IPMI</td>
<td>Log</td>
<td>Failed to load IPMI driver. Check IBM Web site for IPMI driver update package.</td>
</tr>
<tr>
<td>Linux</td>
<td>RSA</td>
<td>Popup</td>
<td>Detected RSA support and successfully loaded driver.</td>
</tr>
<tr>
<td>Linux</td>
<td>RSA</td>
<td>Popup</td>
<td>IBM WARNING — Detected system support for RSA, but encountered potential issue with the RSA driver stack. Check for RSA driver package updates on the IBM Web site.</td>
</tr>
</tbody>
</table>

Note: Some service processor device drivers are in fact operating system services or daemons. For ease of discussion, we collectively refer to them as device drivers.
Chapter 4. IBM Director installation

If you install IBM Director Agent on a system that does not have service processor drivers installed and you later decide to make use of the in-band communication between the service processor and IBM Director Agent, you must uninstall IBM Director Agent, install the drivers, then reinstall IBM Director Agent.

Device drivers are specific to each server and service processor. Support is available for the following operating systems:

- Windows
- Linux
- VMware ESX Server 3.x
- Novell NetWare

**Important:** Ensure that you have service processor drivers installed on System x and BladeCenter servers before you install IBM Director Agent. If this is not the case, we recommend that you uninstall IBM Director Agent, install the drivers, then reinstall IBM Director Agent.

### 4.4.4 Integrating the service processor without the driver

Both the RSA II and the BMC support out-of-band communications with IBM Director. We define *out-of-band* communication as outside of the software stack.

<table>
<thead>
<tr>
<th>OS</th>
<th>Driver</th>
<th>Message type</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>IPMI</td>
<td>Popup</td>
<td>Detected system support for IPMI and successfully loaded driver.</td>
</tr>
</tbody>
</table>
| Linux   | IPMI   | Popup        | IBM WARNING — Detected system support for IPMI, but failed to load libibmsp6.so.
| Linux   | IPMI   | Popup        | IBM WARNING — Detected system support for IPMI, but encountered BMC communication error. |
| Linux   | IPMI   | Popup        | IBM WARNING — Detected system support for IPMI, but encountered potential issue with the IPMI driver stack. |
| Linux   | OpenIPMI | Popup       | IBM WARNING — Detected system support for OpenIPMI, but encountered potential issue with the OpenIPMI driver stack. |

**Note:** In Linux, the messages displayed on the window during installation are also captured in the /var/log/dirinst.log file. The warning messages are written to the syslog as well. In Windows, the *Display* messages are written to the Windows Application Event log.
and through some external interface. For the RSA II, this is typically through the adapter’s Ethernet interface (although the serial port and ASM interconnect network ports are also suitable). For the BMC, this is through the system Gigabit Ethernet port that is assigned to the BMC (usually port 1).

To send alerts from the service processor to IBM Director, alert forwarding must be enabled and configured on the service processor.

- For the RSA II, alert forwarding can be configured using the RSA II Web interface, the MPCLI utility, or the command-line interface of the Management Processor Assistant in IBM Director (use the Alert dial-out entry configuration commands).
- For the BMC, alert forwarding can be configured using the command-line interface of the Management Processor Assistant in IBM Director or the bmc_cfg utility.

Information about how to use these utilities can be found in *IBM eServer xSeries and BladeCenter Server Management*, SG24-6495.

You can manage service processors out-of-band with IBM Director by working with the physical platform object. Adding this object to IBM Director Console is discussed in the next section.

### 4.4.5 Adding a service processor to IBM Director Console

The service processors are referred to as *physical platforms* by IBM Director Console.

If you have correctly installed the service processor device drivers and IBM Director Agent, then when your server is discovered by IBM Director, the service processor will be automatically discovered and added to the console as a physical platform, as follows:

- If only a BMC is installed, the BMC is added to the console as a physical platform.
- If only a RSA II is installed, or if an RSA II and a BMC is installed but the BMC’s IP address is not valid, only the RSA II is added to the console as a physical platform.
- If both a BMC and an RSA II are installed and drivers are loaded properly, then only the RSA II is added as a physical platform. The BMC is not added to the console.

You can also add the service processor manually if you want or if you do not have the device driver installed. To do this, select **Console** → **New** → **Managed Object** → **Physical Platforms** to display the Add Physical Platform dialog box.
Give the physical platform a meaningful name and enter the IP address. This adds a physical platform object.

You can change the IP address of the RSA II or BMC with the Advanced menu in BIOS (Figure 4-26).

Both the RSA II and the BMC have default IP addresses:

- **BMC**: A static address of 10.1.1.97 (some servers have a default of 0.0.0.0). DHCP is not supported.

- **RSA II**: By default, the RSA II adapter is configured to look for a DHCP server to obtain an IP address, and if none is available, to use the IP address 192.168.70.125.

You can change these settings in the appropriate submenu from the Advanced Setup menu (Figure 4-26). You can also change the IP addresses used by service processors using the Server Configuration Manager, as described in 6.3.17, “Server Configuration Manager” on page 335.

**Note**: IBM Director does not permit you to add both the BMC and the RSA II to the console. If one has already been added and discovered and you attempt to manually add the other, you get an error message:

An error occurred while attempting to add the Physical Platform. Unable to establish a connection with the System.

If you have changed the default USERID/PASSWORD combination when you added the physical platform, you get the padlock icon next to the new entry.
You need to request access to the object. To do this, right-click the object and select **Request Access**.

Figure 4-27 shows the attributes page of a BMC object.
Figure 4-28 shows the attributes page of an RSA II object.

![Display System Attributes: x236rsa00b](image)

<table>
<thead>
<tr>
<th>General Attributes</th>
<th>System Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>x236rsa00b</td>
</tr>
<tr>
<td>System Factory ID</td>
<td>Physical Platforms</td>
</tr>
<tr>
<td>System State</td>
<td>Online</td>
</tr>
<tr>
<td>System Presence Check Setting (minutes)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Secure/Unsecure supported</td>
<td>false</td>
</tr>
<tr>
<td>Access Denied</td>
<td>false</td>
</tr>
<tr>
<td>Encryption Enabled</td>
<td>false</td>
</tr>
<tr>
<td>System UUID</td>
<td>8A3C2EBCD21DB211AC2182F29255B05B</td>
</tr>
<tr>
<td>Machine Type and Model</td>
<td>364141U</td>
</tr>
<tr>
<td>Machine Serial Number</td>
<td>KPXV612</td>
</tr>
<tr>
<td>MAC Addresses</td>
<td>()</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>{&quot;192.171.157}&quot;</td>
</tr>
<tr>
<td>Platform FRU</td>
<td>32R1053</td>
</tr>
<tr>
<td>Management Processor Text ID</td>
<td>KPXV612rsr</td>
</tr>
<tr>
<td>Management Processor IP Address</td>
<td>192.171.157</td>
</tr>
<tr>
<td>Management Processor Hostname</td>
<td>KPXV612rsr</td>
</tr>
<tr>
<td>Connection status</td>
<td>Connected</td>
</tr>
</tbody>
</table>

| Service processor type                  | Remote Supervisor Adapter II        |

**Tip:** When the IBM Director Agent is installed, it matches the system unique ID from the server and the management processor and pairs the two, so the association exists between a server and a physical platform.
In IBM Director Console you can display the service processors as child objects to the managed systems they are installed in. To do so, click **Associations → System Membership**. The group contents pane in the console looks similar to Figure 4-29.

**Figure 4-29 Using the system membership association**

**Note:** You can configure the naming of service processors (physical platforms) using templates, as described in 4.4.6, “Naming the physical platforms” on page 189.

**Resolving problems**

If you are still having problems, you can turn on a debug log file TWGRas.log. To do so, edit the TWGRas.properties file in the data folder, and remove the comment character at the beginning of each line. See 4.7.3, “TWGRas log file” on page 218, for more details.

Stop and restart the director server to have this change take effect. Then, after you have reproduced the problem, you should see a TWGRas.log file in the log folder. This can indicate the problem that you have.

**Tip:** There is a known problem with adding the RSA II SL card in an x366, x460, or x260 to IBM Director. In the TWGRas.log you see the message:

```
ERROR: Enclosure Machine Type Model not valid: ""
```

This is a problem with RSA II firmware Version 26A or earlier. It has been fixed with firmware 27A.
4.4.6 Naming the physical platforms

By default, when a new physical platform is discovered, it is named using the following template:

```
IBM %SERVER_MACHINE_TYPE_MODEL% %SERVER_SERIAL_NUMBER%
```

You can change this template with **Options → Discovery Preferences** and then click the **Physical Platforms** tab, as shown in Figure 4-30.

![Discovery Preferences - Physical Platforms](image)

You can change the template by highlighting variables from the left-hand list and clicking **Add**, or highlighting existing variables from the right-hand list and clicking **Remove**. You can also add spaces or any other character as well.
For example, you might want to use something more useful, such as:

%SP_TEXT_ID% (%DIR_AGENT_NAME%)

We recommend that you experiment with a template that is suitable for your use.

After you have saved the template, you can update all previously discovered physical platforms as follows:

1. Select all physical platform objects by changing the displayed group to Physical Platforms, then pressing Ctrl+A to select them all.
2. Right-click any one of them and click **Auto Rename**.
3. Click **Execute Now** to perform the function immediately.

In addition, if you check the box **Use during discovery**, then any Physical Platforms that are discovered will be automatically renamed using this template.

**Tip:** Our experience in the lab has been that you sometimes have to run Auto Rename more than once to make it rename a group of systems, and even then some do not rename properly.

### 4.4.7 Management interfaces

When you have added the service processor to IBM Director Console, you can now manage the devices. IBM Director provides the following tasks, either by right-clicking the physical platform object or from the Tasks pane, or both:

- **Server Configuration Manager**

  Server Configuration Manager provides a way to configure networking and user accounts across multiple service processors (physical platforms). You create a profile with the required configuration information, then apply that to multiple service processors or groups. You can also configure Server Configuration Manager to automatically apply a profile to any newly discovered or added physical platforms. See 6.3.17, “Server Configuration Manager” on page 335.

- **Management Processor Assistant: Web interface**

  This function is for the RSA II only and launches the Web interface to that service processor. The BMC does not support this function.

  This function differs from directly connecting to the RSA Web interface in that IBM Director Server acts as a proxy between the management workstation (where you are running IBM Director Console) and the service processor. This means that you can use this function even if the service processor is on
a private management network not normally accessible by the management workstation.

- **Management Processor Assistant: command-line interface**

  This is the equivalent of the MPCLI, but is an updated version that works with both the RSA II and the BMC service processors. The MPCLI is a comprehensive command-line interface.

  Similar to the MPA Web interface, IBM Director Server acts as a proxy between the management workstation and the service processor. The MPCLI command is actually run from the management server. The session is run in an IBM Director Remote Console window.

  This function issues the following commands on the server using a Remote Console session. If you prefer, you can run these commands directly from the server:
  - RSA II:
    ```
    MPCLI logonip -hostname 9.42.171.149 -u USERID -p PASSWORD
    ```
  - BMC:
    ```
    MPCLI logonip -hostname 9.42.171.149 -u USERID -p PASSWORD -t ipmi
    ```

  **Note:** The standalone MPCLI Version 3.0 utility does not support the BMC. Future versions are likely to include this support.

- **Power control**

  This function allows you to power off the server, restart the server, or power on the server.

  - Without a service processor installed but with IBM Director Agent installed, you can gracefully shut down or restart the server.
  - With a service processor, you can power on the server when it is off, as well as immediately power off or restart the server.

- **System identification**

  This function lets you turn on or off the blue indicator LED on the front of the server.

### 4.4.8 Out-of-band alert forwarding

When you have IBM Director Agent and the service processor device driver installed, then all alerting from the service processor can be handled in-band to IBM Director Agent and then to IBM Director Server.
However, if you do not have IBM Director Agent installed, you need to configure out-of-band alert forwarding. For the RSA II, you can use the Web interface or MPCLI. For the BMC, you can use MPCLI or bmc_cfg.

Because the common method is MPCLI, we describe that here. The use of bmc_cfg is described in detail in *IBM eServer xSeries and BladeCenter Server Management*, SG24-6495.

To set alert forwarding on the service processor so that alerts are forwarded to IBM Director Server at IP address 9.42.171.229, issue the commands shown in Example 4-1.

*Example 4-1  MPCLI commands to enable alert forwarding (BMC)*

```
mp> logonip -hostname 9.42.171.53 -u USERID -p PASSW0RD -t ipmi
SUCCESS: logonip -hostname 9.42.171.53 -u USERID -p PASSW0RD -t ipmi
logged on ip=9.42.171.53>
getalertentry -index 1
Alert Entry:
   Index: 1
   Enabled: true
   Critical Events Only: false
   Description: null
   Type: director.all
   Number: null
   IP Address: 192.168.128.51
   PIN: null
   Email address: null
   PPP Login Id: null
   PPP Password: null
logged on ip=9.42.171.53>
deletealertentry -index 1
true
logged on ip=9.42.171.53>
getalertentry -index 1
Alert Entry:
   Index: 1
   Status: 0 (Invalid)
logged on ip=9.42.171.53>
setalertentry -index 1 -enabled true -type director.all -ipaddress 9.42.171.229
SUCCESS: setalertentry -index 1 -enabled true -type director.all -ipaddress 9.42.171.229 -enabled true
SUCCESS: setalertentry -enabled true
true
FAILURE: setalertentry -type director.all failed
SUCCESS: setalertentry -ipaddress 9.42.171.229 true
SUCCESS: setalertentry -enabled true
true
```
logged on ip=9.42.171.53>getalertentry -index 1
Alert Entry:
  Index: 1
  Enabled: true
  Critical Events Only: false
  Description: null
  Type: director.all
  Number: null
  IP Address: 9.42.171.229
  PIN: null
  Email address: null
  PPP Login Id: null
  PPP Password: null

Note the following about this procedure:

► All alert forwarding entries are numbered. You need to specify which entry
  with which you are working. The number is not important, however. All
  enabled entries are processed.

► We first display the entry using getalertentry, then delete it using
  deletealertentry. These steps are not necessary, but are recommended to
  see the values prior to setting them and to delete the entry back to a known
  state.

► The single setalertentry command actually performs three commands
  (enable, connection type, and destination address). We could have also
  issued these three commands separately. In fact, you can see from the output
  that all three commands are indeed processed separately.

► The -type director.all command failed. This is because the service
  processor we issued these on is a BMC, which only supports connection type
  director.all, and this cannot be changed. If we were to run this command on
  an RSA II, then it would return with SUCCESS.

► If you need to issue these commands against multiple service processors you
  could add them to a text file on the management server and use the
  inputfile filename MPCLI command to read the commands from the text
  file.

See the Management Processor Command-Line Interface User's Guide for more
information about commands and scripting, available from:

http://www.ibm.com/systems/management/director/resources

Look under IBM Director Extensions.
4.5 Installing service processor drivers for ESX Server

The process of installing service processor drivers on various IBM server hardware running various operating systems is covered in multiple documents. However, we were not able to find a satisfactory guide to installing these drivers for VMware ESX Server. Since there are now supported service processor drivers available for VMware ESX Server (beginning with Version 3.0), we cover the installation steps here.

We cover two basic options for providing in-band communication between VMware ESX Server and IBM Director Agent. For systems with an RSA II card, follow the instructions in 4.5.1, “RSA II driver installation for ESX Server 3.x” on page 194. For an ESX Server host without an RSA card installed, refer to 4.5.2, “Enabling OpenIPMI driver for BMC” on page 199, for details about establishing in-band communication with the BMC.

4.5.1 RSA II driver installation for ESX Server 3.x

If you have an RSA II or RSA II SlimLine installed in your server, you should install the RSA II daemon before installing IBM Director Agent. VMware ESX Server 3.x now supports the use of the RSA II daemon for in-band alerting for hardware events to IBM Director Agent.

At the time of writing, however, there was no compiled RSA II daemon for use in ESX Server 3.0. This section describes how to compile the daemon and install it. You will need to install the daemon before installing IBM Director Core Services or IBM Director Agent and the VMM agent on the ESX Server console OS.

**Note:** Compiling the daemon requires files from ESX 3.0.x CD or the Red Hat distribution or from rpmfind.net.

Prior to installing the RSAII daemon, you need to get the following rpm files:

- libusb-0.1.6-3.i386.rpm
- libusb-devel-0.1.6-3.i386.rpm

You can get them from any of the following sources:

- ESX 3.0.x CD
- RHEL 3 Update 6 CD
- rpmfind.net web site
Table 4-4 summarizes the rpm files needed and the alternative methods to get them.

Table 4-4  RPMs required to compile the RSA device driver

<table>
<thead>
<tr>
<th>RPM file name</th>
<th>Location on ESX 3.0.x CD</th>
<th>Link</th>
<th>Location on RHEL CD</th>
</tr>
</thead>
<tbody>
<tr>
<td>libusb-0.1.6-3.i386.rpm</td>
<td>/VMware/RPMS</td>
<td>rpmfind.net(^a)</td>
<td>RHEL 3 CD #2 /RedHat/RPMS</td>
</tr>
<tr>
<td>libusb-devel-0.1.6-3.i386.rpm</td>
<td>/VMware/RPMS</td>
<td>rpmfind.net(^b)</td>
<td>RHEL 3 CD #3 /RedHat/RPMS</td>
</tr>
</tbody>
</table>

\(^a\) [http://rpmfind.net/linux/RPM/sourceforge/a/ac/accessrunner/libusb-0.1.6-3.i386.html](http://rpmfind.net/linux/RPM/sourceforge/a/ac/accessrunner/libusb-0.1.6-3.i386.html)

\(^b\) [http://rpmfind.net/linux/RPM/sourceforge/c/cp/cp4218/libusb-devel-0.1.6-3.i386.html](http://rpmfind.net/linux/RPM/sourceforge/c/cp/cp4218/libusb-devel-0.1.6-3.i386.html)

To install the RSAII daemon:

1. Log into the ESX Server console OS as root.
2. Copy the rpm files required to a temporary directory.
3. Log in to the ESX Server service console and change to the temp directory where all of the RPMs have been copied to and install the RPMs using the following command:
   
   ```bash
   rpm -ivh *.rpm
   ```

   The output is shown in Example 4-2.

**Example 4-2  Install RPMs on ESX console**

```
[root@esx3demo2 redhat]# ls *libusb*
libusb-0.1.6-3.i386.rpm  libusb-devel-0.1.6-3.i386.rpm
[root@esx3demo2 redhat]# rpm -ivh libusb*.rpm
warning: libusb-0.1.6-3.i386.rpm: V3 DSA signature: NOKEY, key ID db42a60e
Preparing...
#................................................ [100%]
1:libusb
#................................................ [ 50%]
2:libusb-devel
#................................................ [100%]
[root@esx3demo2 redhat]#
```
4. Download and copy the source RPM for the latest USB daemon for Linux to the ESX console. The latest code is available from support document MIGR-64585:

http://www.ibm.com/support/docview.wss?uid=psg1MIGR-64585

At the time of writing, the downloaded file is named ibmusbasm-1.22-2.src.rpm.

5. Log in to the ESX Server service console and enter the directory where you copied the drivers. Use the following command to compile and build the driver:

```
rpmbuild --rebuild ibmusbasm-1.22-2.src.rpm
```

The output is shown in Example 4-3.

Example 4-3  Build RSA II driver using rpmbuild

```
[root@esx3demo2 RSA]# rpmbuild --rebuild ibmusbasm-1.22-2.src.rpm
Installing ibmusbasm-1.22-2.src.rpm
Executing(%prep): /bin/sh -e /var/tmp/rpm-tmp.89307
+ umask 022
+ cd /usr/src/redhat/BUILD
+ cd /usr/src/redhat/BUILD
+ rm -rf ibmusbasm-src
+ /usr/bin/gzip -dc /usr/src/redhat/SOURCES/ibmusbasm-src.tgz
+ tar -xvfv -

drwxrwxr-x root/root 0 2006-05-10 19:36:30 ibmusbasm-src/
-rw------- root/root 7256 2006-05-10 19:36:30 ibmusbasm-src/README.TXT
-r-xr-xr-x root/root 5133 2006-05-10 19:36:30 ibmusbasm-src/ibmusbasm.spec
-r-xr-xr-x root/root 2591 2006-05-10 19:36:30 ibmusbasm-src/ibmasm.initscript
drw-rw-r-- root/root 0 2006-05-10 19:36:30 ibmusbasm-src/src/
-rw------- root/root 312 2006-05-10 19:36:30 ibmusbasm-src/src/Makefile
-rw------- root/root 14580 2006-05-10 19:36:30 ibmusbasm-src/src/ibmasm.h
-rw------- root/root 122197 2006-05-10 19:36:30 ibmusbasm-src/src/ibmasm.c
-r-xr-xr-x root/root 221 2006-05-10 19:36:30 ibmusbasm-src/ibmspdown
drw-rw-r-- root/root 0 2006-05-10 19:36:30 ibmusbasm-src/src/exe/
```
执行(%build): /bin/sh -e /var/tmp/rpm-tmp.89307
   + umask 022
   + cd /usr/src/redhat/BUILD
   + cd ibmusbasm-src
   + cd shlib
   + gcc -D__IBMLINUX__ -fPIC -shared -I ../src -o libsysSp.so.1
   uwiapi.c
   + cd ../exe
   + gcc -I ../src -o ibmasm ../src/ibmasm.c -ldl
   ../src/ibmasm.c: In function `InitNode':
   ../src/ibmasm.c:2552: warning: comparison between pointer and
   integer
   ../src/ibmasm.c:2552: warning: comparison between pointer and
   integer
   .../src/ibmasm.c: In function `InitDynamicLinks':
   .../src/ibmasm.c:3189: warning: assignment makes pointer from integer
   without a cast
   + exit 0
执行(%install): /bin/sh -e /var/tmp/rpm-tmp.89307
   + umask 022
   + cd /usr/src/redhat/BUILD
   + cd ibmusbasm-src
   + rm -rf /var/tmp/ibmusbasm-1.22-build
   + mkdir /var/tmp/ibmusbasm-1.22-build
   + mkdir /var/tmp/ibmusbasm-1.22-build/lib
   + mkdir /var/tmp/ibmusbasm-1.22-build/sbin
   + mkdir /var/tmp/ibmusbasm-1.22-build/etc
+ mkdir /var/tmp/ibmusbasm-1.22-build/etc/init.d
+ install -m 755 shlib/libsysSp.so.1
/var/tmp/ibmusbasm-1.22-built/lib
+ install -m 700 exe/ibmasm /var/tmp/ibmusbasm-1.22-built/sbin
+ install -m 700 ibmsspup ibmsspdown
/var/tmp/ibmusbasm-1.22-built/sbin
+ install -m 700 /usr/src/redhat/SOURCES/ibmasm.initscript
/var/tmp/ibmusbasm-1.22-built/etc/init.d/ibmasm
+ ln -sf /lib/libsysSp.so.1
/var/tmp/ibmusbasm-1.22-built/lib/libsysSp.so
+ /usr/lib/rpm/brp-compress
+ /usr/lib/rpm/brp-strip
+ /usr/lib/rpm/brp-strip-static-archive
+ /usr/lib/rpm/brp-strip-comment-note
Processing files: ibmusbasm-1.22-2
Executing(%doc): /bin/sh -e /var/tmp/rpm-tmp.89307
+ umask 022
+ cd /usr/src/redhat/BUILD
+ cd ibmusbasm-src
+ DOCDIR=/var/tmp/ibmusbasm-1.22-built/usr/share/doc/ibmusbasm-1.22
+ export DOCDIR
+ rm -rf /var/tmp/ibmusbasm-1.22-built/usr/share/doc/ibmusbasm-1.22
+ /bin/mkdir -p
/var/tmp/ibmusbasm-1.22-built/usr/share/doc/ibmusbasm-1.22
+ cp -pr README.TXT
/var/tmp/ibmusbasm-1.22-built/usr/share/doc/ibmusbasm-1.22
+ exit 0
Provides: config(ibmusbasm) = 1.22-2 libsysSp.so.1
Requires(interp): /bin/sh /bin/sh /bin/sh /bin/sh
Requires(rpmlib): rpmlib(CompressedFileNames) <= 3.0.4-1
rpmlib(PayloadFilesHavePrefix) <= 4.0-1
Requires(pre): /bin/sh
Requires(post): /bin/sh
Requires(preun): /bin/sh
Requires(postun): /bin/sh
Requires(%clean): /bin/sh -e /usr/src/redhat/RPMS/i386/ibmusbasm-1.22-2.i386.rpm
Executing(%clean): /bin/sh -e /var/tmp/rpm-tmp.89307
+ umask 022
+ cd /usr/src/redhat/BUILD
+ cd ibmusbasm-src
6. Install the RSAII daemon using the following rpm command from the /usr/src/redhat/RPMS/i386™ directory:

```
 rpm -ivh ibmusbasm-1.22-2.i386.rpm
```

The output is shown in Example 4-4.

**Example 4-4  Install the RSAII daemon using rpm**

```
[root@esx3demo2 i386]# pwd
/usr/src/redhat/RPMS/i386
[root@esx3demo2 i386]# rpm -ivh ibmusbasm-1.22-2.i386.rpm
Preparing...
##################################################### [100%]
  Found IBM Remote Supervisor Adaptor II.
  1:ibmusbasm
##################################################### [100%]
  Removing previous Start/Kill ibmasm run levels.
  Starting IBM RSA II daemon
  Calling chkconfig ibmasm on
[root@esx3demo2 i386]#
```

**Note:** The package adds an init script called ibmasm and sets it to start up automatically at all run levels.

### 4.5.2 Enabling OpenIPMI driver for BMC

If your system has a BMC and does not have an RSA II card installed, you can enable in-band communication with IBM Director Agent through the OpenIPMI device driver. The following instructions apply whether you intend to install IBM Director Core Services (Level-1) or IBM Director Agent (Level-2) on the VMware host.

IPMI is an open standard describing a hardware manageability interface. This includes how to monitor systems hardware, sensors, logs, and so on. OpenIPMI
Implementing IBM Director 5.20 is the open source implementation of the IPMI standard, as opposed to other implementations, such as the one provided by a company called OSA Technologies.

**Important:** IBM does not support the OSA IPMI mapping layer on ESX Server, so you should not install this code.

Starting with ESX Server 3.0, VMware supports the OpenIPMI implementation on ESX Server. On Version 3.0 you must install patch 8005537, which can be found on the VMware Web site:


This patch installs the OpenIPMI init script, which is used to automatically start the daemon at system startup. Install this patch if required before proceeding with these instructions.

If you are running ESX Server 3.0.1, you do not need the patch.

Whether or not you need the patch, you should check the configuration of the init script. To verify that the init script has been activated, open a shell to the ESX Server host, logging on as root, and run the following command:

chkconfig --list | grep ipmi

If no output is returned from the `--list` command, the IPMI init script is not registered. To correct this, run the following commands:

chkconfig --add ipmi
chkconfig ipmi on

The `--add` command registers the IPMI init script, while the second command enables it for automatic startup.

If the output returned by the `--list` command is in the following format, the IPMI init script has been registered and its startup type is listed for all run levels:

```
ipmi 0:off 1:off 2:off 3:off 4:off 5:on 6:off
```

It is important to check the status of run level 3, since this is the run level used by ESX Server. If it is set to `off`, as in our example, you must enable it by issuing the following command:

chkconfig ipmi on

This will ensure that OpenIPMI will start automatically at system startup. To start OpenIPMI in the current session, issue the following command:

service ipmi start
Refer to the following VMware knowledge base article for more details:
http://kb.vmware.com/vmtnkb/search.do?cmd=displayKC&docType=kc&externalId=8005537&sliceId=SAL_Public

Once the OpenIPMI device driver is started, you can proceed with IBM Director Agent installation. The Agent installer should recognize the daemon and establish communication with the BMC.

4.6 Automating the installation process

This section describes how to automate the following procedures:

- Unattended installation of IBM Director Agent (page 201)
- Using cloning to deploy IBM Director Agent (page 206)
- Deploying driver updates using software distribution (page 209)

4.6.1 Unattended installation of IBM Director Agent for Windows

All parts of IBM Director now support unattended installation. This means that each and every package of the IBM Director can be scripted and installed with a response file, including components such as ServeRAID Manager, System Availability, and Capacity Manager.

When customers install IBM Director Agent on a large number of Windows systems, the typical methods are cloning and unattended installation. Cloning only works on systems without an operating system installed. Unattended installation works if you already have the operating system loaded.

**Tip:** For information about using IBM Director Software Distribution to install IBM Director Agent remotely, see 13.2, “Automated IBM Director Agent promotion” on page 776.

To perform an unattended installation of IBM Director Agent, modify the DIRAGENT.RSP file located in the agent subdirectory on the IBM Director CD. The full path is `\director\agent\windows\i386\FILES\diragent.rsp`.

After you modify this file, you can start a silent installation of the IBM Director Agent using these methods:

- Command line
- Batch file
- A RunOnce statement in the Windows registry
- Scheduled task
Remote installation service

There are a number of different parameters you can use when starting the installation. Look at the response file that accompanies the executable for details.

To launch a silent or unattended installation, you can use the following commands:

- `dir5.20_agent_windows.exe -a unattended`
  
  This command displays the built-in models’ dialog boxes that show progress messages and uses the Diragent.rsp response file located in the installation source directory.

- `dir5.20_agent_windows.exe -a silent`
  
  This command performs a silent installation that does not display an interface, and uses the Diragent.rsp response file located in the installation source directory.

- `dir5.20_agent_windows.exe -a RSP="filename"`
  
  This command is used with unattended or silent parameters. It specifies the name and location of the response file.

- `dir5.20_agent_windows.exe -a waitforme`
  
  This command is used with unattended or silent parameters and ensures that the ibmsetup.exe process will not end until the installation of IBM Director Agent is complete.

DIRAGENT.RSP contents

This section describes the entries in the response file (Example 4-5). For a detailed deployment scenario, see 13.2, “Automated IBM Director Agent promotion” on page 776.

Example 4-5  The diragent.rsp response file for unattended installs

```
[Agent]=Y
UseExistingTarget = Y
TargetDrive = C
TargetFolder = Program Files\IBM\Director
RemoteControl = N
EncryptCommunication = Y
SecureAgent = Y
Driver.TCPIP = 1
Driver.NETBIOS = 1
Driver.NETBIOS2 = 0
Driver.NETBIOS3 = 0
```
Driver.NETBIOS4 = 0
Driver.IPX = 0
Parm1.NETBIOS = MACHINE1 (network_id)
Parm1.NETBIOS2 = MACHINE2
NetTimeout = 15
SystemName=user friendly name
WakeOnLan = 0
ReqUserAuthToScreen = 0
DisableScreenSaver = 0
DisableWallpaper = 0
AddKnownServerAddress=TCPIP::146.84.167.121
ShutdownDoesPoweroff = 0
RebootIfRequired = Y

The meaning of each entry is as follows:

- **UseExistingTarget**
  This command is useful in upgrading an older client. If set to Y (yes), the installation always uses the previously installed directory.
  If set to N (no), the agent uninstalls the previous agent and installs the new agent in the directory specified in the next lines.
  Be careful that if you specify different locations for IBM Director Agent and use that response file to upgrade core services, the installation will fail. The full agent must reside in the same directory where core services is installed. We recommend setting this to the default value.

- **TargetDrive and TargetFolder**
  These commands set the preferred path to where the package will be installed. Note that if you are installing the same version, it is not considered an upgrade, and this parameter is ignored. This means that you cannot have Level-1 and Level-2 agent files on separate drives.

- **RemoteControl**
  Remote control refers to the built-in remote control functionality in IBM Director, which enables you to take control of the managed system’s window, mouse, and keyboard from your IBM Director Console. If you want to install this feature set the value to Y. Otherwise, set the value to N.

- **EncryptCommunication**
  The encrypting option selects whether to encrypt or not encrypt the communication between IBM Director Agent and IBM Director Server. If you will be transmitting confidential data, you might want to enable this function. The encryption method is the one chosen by the Server, so if the server has
no encryption enabled, it cannot talk to the agent. A server with encryption enabled can talk to the agent with no encryption selected.

- **SecureAgent**
  When SecureAgent is set to Y, all system management servers who want to communicate with this server need to be authorized first.

  When not secured, it means that the agent shows up on management servers without any padlocks, and can be managed by any IBM Director management server. For security reasons, we always recommend setting this to Y.

- **Driver.**
  With this parameter, you can specify the network protocols used by IBM Director Agent. We suggest that you enable pure TCP/IP without the use of NetBIOS, unless you have special requirements such as IPX.

- **ParmN.x**
  This option is used only by NetBIOS. If you plan to use NetBIOS as a protocol, then use the system name as its NetBIOS name for IBM Director Agent. We suggest that you do not change these settings.

- **NetTimeout**
  The network timeout option can be a useful feature if you operate IBM Director in a complex network environment with possible high network latency. The default is 15 seconds, which is the time IBM Director Agent will wait for a reply from IBM Director Server.

- **SystemName**
  SystemName refers to the name of the managed system as it appears on IBM Director Console. By default, this will be the system’s host name. We suggest that you leave this default setting, because it turns out to be very efficient in production environments. You can also use a combination for easier grouping, for example, prefix NC_\$M for all systems in North Carolina. The variables you can use are:
  - $M substitutes the computer name of the system.
  - $U substitutes the system’s owner (not suggested in an enterprise).
  - $O substitutes the organization name.
  - $$ substitutes the $ symbol.

- **WakeOnLan**
  This entry lets you enable Wake on LAN® if it is supported by the network card. Wake on LAN lets you power on a remote client over the network card’s MAC address, and it is supported by most current System x servers, NetVista desktops, IntelliStation workstations, and ThinkPad notebooks.
In general, this setting should be enabled and set to 1. Systems that do not support Wake on LAN are unaffected by this setting.

- **ReqUserAuthToScreen**
  This section enables or disables user authorization for the remote control function of IBM Director. This setting can vary depending on the type of system on which you are installing IBM Director Agent. For client systems, generally we suggest that you enable user prompting. In some countries, this might even be necessary based on the local privacy laws.

  On servers, we recommend that you set this option to N, because most servers are unattended.

- **DisableScreenSaver**
  Disabling the screen saver for remote control is a highly useful option. By enabling it, possible screen saver data is not transmitted through IBM Director remote control software. Transmitting screen saver data can cause high network traffic and might slow down the connection to the managed system.

- **DisableWallpaper**
  Disabling the wallpaper can be compared to disabling the screen saver during a remote control session. No changes are made on the managed system’s desktop. Instead of transmitting the wallpaper over the remote control session, a blank background is presented.

- **AddKnownServerAddress**
  Adding the address or the host name of a system running IBM Director Server causes IBM Director Agent to contact this server the first time IBM Director Agent starts. As a result, the managed systems report themselves to the management server, rather than having the management server search for those systems.

  We strongly suggest that you make use of this feature. We also suggest that you use host names rather than IP addresses, as IP addresses can be subject to change. You can use multiple AddKnownServerAddress statements if you want your managed system to report to multiple management servers. The syntax for specifying management servers is:

  AddKnownServerAddress=<protocol>::<address>

  For example:

  AddKnownServerAddress=TCPIP::directorserver.fqdn.local

- **ShutdownDoesPoweroff**
  Enabling this setting using a 1 maps the shutdown command of a management server with a physical power-off of the respective managed system. For this feature to work, the managed system must support a
physical power-off from the operating system level, which requires an Advanced Power Management™ Interface (APMI) to be installed. Because this setting does not harm systems that do not support APMI, we suggest that you leave this option as the default 0, meaning enabled.

- RebootIfRequired

This option enables or disables a reboot after the installation of IBM Director Agent. The default is Y. Depending on your deployment mechanism, you might want to disable the rebooting of the managed system. However, in order to register the Windows Installer 3.0 package, the operating system must be rebooted. IBM Director itself does not require a reboot before it can be started.

### 4.6.2 IBM Director Agent and cloning

A popular method of mass deployment of operating systems is cloning an image or donor system. Cloning has been very popular for Windows-based systems, which include specialized tools to remove unique identifiers. However, cloning of Linux systems is also becoming popular as speed of deployment becomes increasingly important.

Tools such as Microsoft Sysprep ensure that all Microsoft unique identifiers of the donor system are removed, making sure that all clones are unique in the network. Unlike Windows-based systems, Linux does not use Security Identifiers (SIDs) or registry keys, which makes cloning of systems easier.

However, the IBM Director Agent software also uses unique identifiers, which Sysprep and Linux do not handle. In a usual cloning procedure, these identifiers remain untouched, resulting in identifiers that are no longer unique between the donor system and its clones. When this occurs, the management server is not able to distinguish between these managed systems.

For a discussion of how to automate the repair of a cloned Windows system, see 13.1, “IBM Director Agent on a cloned Windows system” on page 764.

**Option 1: preparing the donor before cloning**

The most effective way to solve a problem is to make sure it never occurs.

**Windows systems**

Three critical settings are stored on the hard drive and in the Windows Registry. Before making an image of the donor system, these settings must be removed. After restarting IBM Director Agent on the cloned system, these settings are
regenerated. To ensure that each cloned system appears as a unique entity to
the management server, follow these steps:

1. Install IBM Director Agent on the system and reboot.

2. Stop IBM Director Agent using the `net stop twgipc` command.

3. Delete the `twgmach.id` file, found in `C:\Program Files\IBM\Director\data`
   (assuming a default installation directory).

4. Delete the Windows Registry key `TWGMachineID`, which is found in
   `HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName`.

5. Delete the `netdrvr.ini` file, found in `C:\Program Files\IBM\Director\data`
   (assuming default installation directory).

The donor system is now ready for normal Sysprep preparation and cloning. It is
important that you do not reboot the donor system after you make the specified
changes. If you reboot before creating the source image, these two settings are
recreated and you need to start over.

These steps ensure that every system cloned from that donor system will be
seen as a unique entity within the management server. In addition, by deleting
`netdrvr.ini`, you ensure that the system name displayed in the management
console matches the Windows computer name.

The problem with deleting `netdrvr.ini` in this manner is that when this file is
recreated when IBM Director Agent starts for the first time on the cloned
systems, the other parameters stored in `netdrvr.ini` are reset to default. These
include which network drivers to use, the network timeout value, whether to
enable Wake-on-LAN functionality, and other settings related to IBM Director
Remote Control. In many installations, default values are acceptable. If this is the
case, no further consideration is necessary. However, if you prefer to configure
nondefault settings for `netdrvr.ini`, see 13.1, “IBM Director Agent on a cloned
Windows system” on page 764, for a way to configure all cloned systems to
automatically recreate `netdrvr.ini` with your customized values.

**AIX, i5/OS and Linux systems**

Two critical settings are stored on the hard drive. Before making an image of the
donor system, these settings must be removed. After restarting IBM Director
Agent on the cloned system, these settings are regenerated. To ensure that each
cloned system appears as a unique entity to the management server, follow
these steps:

1. Install IBM Director Agent.

2. Stop the IBM Director Agent using the `twgstop` command.

3. Delete the file `/etc.ibm/director/twgagent/twgagent.uid`. 
4. Open the file install_root/data/ServiceNodeLocal.properties and remove the line starting with:

        ipc.uid=

The donor system is now ready for cloning. It is important that you do not reboot the donor system after you make the specified changes restart the IBM Director service. If you reboot or restart the services before creating the source image, these two settings are recreated and you need start over.

These steps ensure that every system cloned from that donor system will be seen as a unique entity within the management server.

Option 2: repairing a cloned system after rollout

This section describes how to fix IBM Director Agent settings on systems that have been cloned without preparing the donor system, as described in the previous section.

If you attempt to manage multiple systems that have been cloned from a donor that was running IBM Director Agent without first preparing the donor as discussed in “Option 1: preparing the donor before cloning” on page 206, you will only see one system, the name of the original donor system.

This is due to duplication of the unique identifiers used by IBM Director during the cloning process, resulting in the management server being unable to distinguish between the cloned systems. Only the first managed system the management server discovers is added to the management console.

Windows systems

To fix this problem, you must manually remove all unique identifiers and pointers that identify each cloned system. Follow these steps:

1. Stop IBM Director Agent using the net stop twgipc command.

2. Delete the twgmach.id file, found in C:\Program Files\IBM\Director\data (assuming default installation directory).

3. Delete the Windows Registry key TWGMachineID, which is found in HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName.

4. Change the netdrvr.ini settings using the twgipccf command to start the GUI-based configuration utility. Make any desired changes and click OK.

5. Restart the IBM Director Agent using the net start twgipc command.
**4.6.3 Setting up a file distribution architecture**

With IBM Director you can distribute firmware and drivers to managed IBM System x and BladeCenter servers using the base Software Distribution task rather than manually updating those systems. With the addition of the fee-based extensions Remote Deployment Manager and Software Distribution Premium Edition, IBM Director can be used to install operating systems and distribute any kind of software.

However, with the advent of these very powerful capabilities comes the need for a proper file distribution configuration. Distributing drivers or fixes over slow WAN links can saturate some networks. To respond to this problem, IBM Director offers two ways of distributing software: streaming and redirection.

**Streamed installations**

The architecture underlying streamed installations is straightforward: when you drag and drop a driver update or a software package onto a managed system, the package is sent directly from the management server to the managed system.

This feature is very useful in fast local LANs where the file packages do not have to be sent over WAN connections. A big advantage of streamed installations is that interrupted file transfers can be continued where they stopped, while redirected installations have to resend the whole package. Redirected installations are enabled by default for all managed systems. You can, however, configure the properties of the streaming server in order to grant a certain network bandwidth for streamed installations.

**Redirected installations**

Redirected installations, as the name suggests, do not send the file packages directly from the management server to a managed system. Instead, the file packages are sent to a staging system, then distributed to the managed systems.

Redirected installations are highly efficient for isolated networks with a single or slow connection. A typical example of an isolated network with a single
connection is a branch office. Even though systems in the branch office are centrally managed by the management server in the main location, sending software packages for multiple systems over a single WAN connection is not recommended.

Instead, the management server uses one of the managed systems in the remote location as a cache. Files can be transferred either with FTP (provided it has an FTP server installed) or with a standard network share. As a result, the management server transmits the file package once to the redirection server at the remote location. This server then distributes the file package to all managed systems in the remote location. In this way, the bandwidth of the WAN connection consumed by software distribution is much less compared to the streamed installation method.

1. To configure redirected installations, click **Options → Server Preferences**. Click the **File Distribution Servers** tab, and click **Add** to add a new file distribution server. You need to know this information:

   - The address of an FTP server on the remote site you want to use for redirected installations.
   - The DNS name and the FTP folder to be used by IBM Director.
   - A valid user ID that has the right to create files in the specified directory.
   - Whether you want to limit the space used by the file distribution server. As a default, IBM Director will use 500 MB on the specified FTP server. You can limit or expand this value according to your needs and the limitations of the specified FTP server.
   - The maximum number of managed systems that can receive their software packages by the specified FTP server at one time. Depending on the limitations of the FTP server and the network, you might have to specify fewer than the maximum. Otherwise, these default values should be sufficient in most environments.
   - A limit on bandwidth you want to impose on file distribution. This limits the network bandwidth that the management server uses to stream the source packages to the remote file distribution server.
For example, the configuration window might look similar to Figure 4-31.

![Figure 4-31 Configuring a file distribution server](image)

2. Click **OK**, and the new server appears in the list (Figure 4-32).

![Figure 4-32 New distribution server added](image)

3. Add other distribution servers as necessary for your network.

   After file distribution has been configured on the management server, the next task is to specify which managed systems use which file distribution server.

   The easiest way to do this is by using groups in IBM Director that correspond to the remote sites. The simplest kind of group you can create is a static
group that you populate with the managed systems of each remote site. Such groups should reflect the remote site and should be named accordingly, for example, *Systems in Geneva* or *Systems in Seattle*.

If you do not assign a file distribution server to a group, all systems use all available file distribution servers. This could lead to a situation where managed systems in Geneva access a file distribution server in Seattle, with potentially major network problems as a result.

4. If you have created groups reflecting sites connected with a WAN, right-click a group, and click **Distribution Preferences**. This opens a window similar to Figure 4-33.

![Set Managed System Distribution Preferences](image)

*Figure 4-33  Group preferences for file distribution*

By default, all file distribution servers are a valid source. You identify this by the single entry (`\"\``) under Share Names. This entry states that all configured file distribution servers are valid sources for distribution.

5. Either remove this entry and add a new one, or edit this entry with corresponding values for your distribution server. In our example, the share is
local to the managed systems, so we use a share name, \zurich\upload\, rather than an FTP server. See Figure 4-34.

![Add Share Name](image)

**Figure 4-34 Configuring the file distribution server for a specific site**

After you complete this step for each of your remote sites, file distribution is set up and ready to use.

If a file distribution server becomes inaccessible (for example, if the defined file distribution server is down while you start a file distribution task), the managed systems stream the software packages directly from the management server. This feature is useful if it is essential to guarantee a successful software distribution. However, there might be situations in which you want to prohibit the use of WAN links for file distribution tasks, such as in case of an unavailable file distribution server.
To prevent WAN links from being used as a backup when the file distribution server is unavailable, click **Options → Server Preferences**, click the **Software Distribution** tab, and check **Do not stream distribution if redirected distribution fails**, as shown in Figure 4-35.

![Server Preferences](image)

**Figure 4-35  Preventing streaming even if the file distribution server is down**

### 4.6.4 Silent install of the ServeRAID agent

In addition to pushing out the ServeRAID agent to managed systems using software distribution and IBM Update Assistant, you can also run the ServeRAID agent installer locally with parameters that allow a silent install.

Here are four examples of different ways to install the ServeRAID Manager agent silently on a Windows system. Note that the quotation marks are required after the `/v` because the parameters between quotation marks are passed onto msiexec, the Microsoft Installer utility.

**Note:** In the examples here, the ServeRAID agent installer is `serveraid_agent_windows.exe`. The file name you use might be different.

Use the following command for the basic silent installation:

```
serveraid_agent_windows.exe /s /v"/qn"
```
To install silently and suppress the reboot, use this command:
serveraid_agent_windows.exe /s /v"/qn REBOOT=ReallySupress"

To install silently with logging, use this command:
serveraid_agent_windows.exe /s /v"/qn /L*v install.log"

To install silently with logging and suppress the reboot, use this command:
serveraid_agent_windows.exe /s /v"/qn /L*v install.log REBOOT=ReallySupress"

**Note:** Even though you can suppress the reboot after the install, a reboot is required for the ServeRAID extension to work properly.

In addition, you can add `start /wait` and the `/w` parameter to the command line. This command causes the installation to wait until the installation finishes before exiting or returning you to a command prompt:

```
start /wait serveraid_agent_windows.exe /w /s /v"/qn /L*v install.log REBOOT=ReallySupress"
```

This wait mechanism is especially useful if you are doing the silent install at the command prompt. It will be obvious that the installation is complete because you are returned to the command prompt.

For information about these and other InstallShield parameters, see:

### 4.7 Troubleshooting IBM Director Agent installation

This section gives you information about common problems that can occur during or after IBM Director Agent installation. However, we provide only guidelines for identifying the problem. It is beyond the scope of this book to provide a troubleshooting guide for IBM Director.

For further troubleshooting information refer to the *IBM Director Planning, Installation, and Configuration Guide* and the *IBM Director Systems Management Guide*, which are included on the IBM Director CD-ROM or available for download from:
http://www.ibm.com/systems/management/director/resources
The publications are also available online in the IBM InfoCenter:

http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/dircinfo_5.20/fqm0_main.html

The IBM support side is useful to search for possible eFixes, service packs, and other valuable information:

http://www.ibm.com/servers/eserver/support/xseries/

There is also an IBM Director discussion forum that provides a good source of real-life experience:


We encourage you to participate in the discussion forum and take part in the global IBM Director community. If your problem was not solved by the information provided or if you would like to report a bug in IBM Director, use the IBM Director support queue or call your local IBM HelpCenter®.
4.7.1 Installing patches

Some IBM Director patches, such as IBM Director 5.10.1 (also known as patch 1 or update 1) do not update the Product Information window. For example, Figure 4-36 is taken from an IBM Director 5.10.1 system.

![Figure 4-36 Product Information window on a 5.10.1 system](image)

The best way to confirm the installed product level is to check the version.key file in the main director folder (in Windows, c:\Program Files\IBM\Director). This text file shows the installed patch level, as shown in Example 4-6.

Example 4-6 Contents of the version.key file

```
510160120 510010000 BASE
component=IBM Director Agent
version=5.10.1
builddate=2006-01-20
buildnum=d0034
codebase_version=5.10
prodversion=BASE
```
4.7.2 Log files

Troublesome installations can happen for any number of reasons, such as defective media or bad installation choices. Often a problem within IBM Director can be tracked back to problems with the installation.

To identify the problems that have occurred, start by looking at the log files IBM Director creates. Depending on the installed options, you can find several log files in the /log subdirectory where you installed IBM Director:

- Linux: /opt/IBM/director/log
- NetWare: SYS:\IBM\Director
- Windows c:\Program Files\IBM\Director\log

4.7.3 TWGRas log file

Another problem determination tool is to enable a debug log file TWGRas.log in the data directory. By default, the RAS log only shows errors. To enable all logging, edit the TWGRas.properties file in the Director\data folder, and remove the comment character from the beginning of each line.

| Example 4-7   TWGRas.properties file with debug logging disabled |
|---------------|----------------------------------------------------------------|
| #twg.ras.comps=-1 |
| #twg.ras.types=-1 |
| #twg.ras.size=16384 |
| #twg.ras.high=1 |
| #twg.sysout=1 |

Stop and restart the director server to have this take effect. Then after you have reproduced the problem, you should see a TWGRas.log file in the Director\log folder.

The TWGRas.log file is largely text. However, a better way to read the contents of the file is to use the rasdump command to covert it to plain text. Run the command from the log directory and pipe the output to a text file:

C:\Program Files\IBM\Director\log>rasdump > twgras.txt

4.7.4 Installation log file

In particular, to verify that IBM Director installation went well on Windows-based systems, check the log file, dirinst.log, placed in the administrative share on the system (\servername\admin$ or c:\winnt).
To help find lines that contain details of interest, the `find` command can be used as follows:

```
find "xxxx" \servername\admin$\dirinst.log
```

Where `xxxx` is any text you want to find in the file. This command returns all lines that include “`xxxx`”.

Searching for the text “MSI” in one of our systems yields the output shown in Example 4-8.

**Example 4-8  Result of a search for “MSI” in dirinst.log**

```
-------- \SKAGIT\ADMIN$\DIRINST.LOG
MSI (s) (BC:EC) [09:46:36:222]: Product: IBM Director Agent -- Installation operation completed successfully.
MSI (s) (EC:74) [14:17:35:125]: Product: IBM Director Console. The file C:\Program Files\IBM\Director\bin\twgipc32.dll is being held in use by the following process
Name: twgipc , Id 2176.
MSI (s) (EC:74) [14:17:35:141]: Product: IBM Director Console. The file C:\Program Files\IBM\Director\bin\twgipc32.dll is being held in use by the following process
Name: twgescli , Id 640.
MSI (s) (EC:74) [14:17:35:141]: Product: IBM Director Console. The file C:\Program Files\IBM\Director\bin\twgipc32.dll is being held in use by the following process
Name: twgmonit , Id 1108.
MSI (s) (EC:74) [14:17:35:141]: Product: IBM Director Console. The file C:\Program Files\IBM\Director\bin\twgipc32.dll is being held in use by the following process
Name: nfUMSagent , Id 2944.
MSI (s) (EC:74) [14:17:35:625]: Product: IBM Director Console. The file C:\Program Files\IBM\Director\bin\twgucd32.dll is being held in use by the following process
Name: twgipc , Id 2176.
MSI (s) (EC:74) [14:17:35:625]: Product: IBM Director Console. The file C:\Program Files\IBM\Director\bin\twgucd32.dll is being held in use by the following process
Name: twgescli , Id 640.
MSI (s) (EC:74) [14:17:35:625]: Product: IBM Director Console. The file C:\Program Files\IBM\Director\bin\twgucd32.dll is being held in use by the following process
Name: twgmonit , Id 1108.
MSI (s) (EC:74) [14:17:35:625]: Product: IBM Director Console. The file C:\Program Files\IBM\Director\bin\twgucd32.dll is being held in use by the following process
Name: nfUMSagent , Id 2944.
MSI (c) (34:D0) [14:20:50:198]: Product: IBM Director Console -- Installation operation completed successfully.
MSI (c) (34:D0) [14:20:50:213]: The Windows Installer initiated a system restart to complete or continue the configuration of 'IBM Director Console'.
MSI (s) (B8:0C) [15:54:48:091]: Product: IBM Director Agent -- Configuration completed successfully.
```
4.7.5 Checking the communication using genevent

Most problematic situations occur due to communication issues. The most common problem is that you cannot see a managed system in the management console. To ensure that there is a connection between the management server and the managed system, we suggest that you check the connection using the genevent tool. genevent (case sensitive in Linux) is a small command-line-based tool that generates a custom event and contacts a management server. The genevent syntax is as follows:

Genevent /type:"<event type>" /text:"<event description>" /dest:<interface>::<address of a management server> /sev:<severity>
For example:
Genevent /type:"Test.Event" /text:"Checking communication..." /dest:TCPIP::ZURICH.IBM.COM

If the event was sent successfully, you see:
The event was sent successfully to the given destination.

When you receive this output, you know that the communication between the managed system and the management server is working. If you receive an error message, make sure that it is not related to a syntax error.

On Windows agents, if the send was not successful, check the configuration of the IBM Director Agent network driver using the TGIPCCF command to open the window shown in Figure 4-37.

![Network driver configuration](image)

*Figure 4-37  IBM Director network driver configuration utility*

Make sure that at least one network interface is enabled for IBM Director communication. Also make sure that you used the corresponding interface in your `genevent` command.
For example, if you have two network cards in your system, the destination parameter used with `genevent` must reflect the correct interface. If you use the second network interface, add a parameter to your `genevent` command, such as:

```
Genevent /type:"Test.Event" /text:"Checking communication..." /dest:TCPIP2::ZURICH.IBM.COM
```

### 4.7.6 Listing the authorized servers

At a command prompt on the managed system running IBM Director Agent, you can issue the list servers command `twglstsr` to show details about each server that is or was authorized to access the Agent. Sample output is shown in Example 4-9.

---

**Example 4-9  Output from the twglstsr command**

```
C:\>twglstsr
{ UID=2F7C756F26B00121, NAME='Director 5', PATH='TCPIP::9.42.171.229',
LASTUPDATE='Thu Dec 15 03:10:31 2005' }
{ UID=7F6E6DA36B2E35E5, NAME='FS2-ID510', PATH='TCPIP::169.254.44.105',
LASTUPDATE='Mon Jan 16 12:43:38 2006' }
{ UID=A13A7A6EE0D0DD4F, NAME='m106958f.itso.ral.ibm.com', PATH='TCPIP::9.42.171.83',
LASTUPDATE='Thu Dec 15 03:17:15 2005' }
{ UID=7F9E973B9A3C5442, NAME='Baker.Director.ITSO.Raleigh.IBM.com',
PATH='TCPIP::9.42.171.212', LASTUPDATE='Mon Nov 14 12:02:17 2005' }
```
---

In this example you can see that four IBM Director Server systems are authorized to connect to this client, but at the time the command was issued (January 16, 2006), only one server was in communication with it. In our example, the other management servers are offline.

If you want to delete all entries and recreate this list, follow these steps:

1. Stop IBM Director Agent (on Windows, use `net stop twgipc`).
2. Delete the file `netdrvr.ini` from directory `Director\data`.
3. Run `twgipccf` and click **OK** to recreate `netdrvr.ini`.
4. Restart IBM Director Agent (on Windows, use `net start twgipc`).
5. Initiate Agent <> Server communications by one of these methods:
   - Wait for the next automated discovery from the server, or force a discovery from the console.
   - Issue a `genevent` command from the client to send an event to the server, which will result in the client being discovered.
Create a .rsp response file that includes the AddKnownServerAddress parameter, put the RSP file in the Director\bin directory, and run the command `twgipccf /r:file.rsp`. See “DIRAGENT.RSP contents” on page 202 for details of the response file.

### 4.7.7 Discovery problems: resetting IBM Director Agent

If you are having trouble getting a managed client added to IBM Director Console, follow these steps to reset IBM Director Agent and force it to get a new machine ID:

1. Stop the director support program (on Windows, `net stop twgipc`).
2. Delete the file TWGMACH.ID from Director\data.
3. Delete the file NETDRVR.INI from Director\data.
4. Delete all server public keys DSA*.PUB from Director\data.
5. Delete the machine ID from the Windows registry HKLM\System\CurrentControlSet\Control\ComputerName\ComputerName\TWGMachineID.
6. Run TWGIPCCF and enable all appropriate adapters and protocols. This recreates NETDRVR.INI.
7. Start the Director Support Program (on Windows, `net start twgipc`). This recreates the machine ID.
8. Rediscover the client.

### 4.7.8 Clients no longer send events to the management server

When events occur on managed systems, the alerts are sent to the one or more management servers that are authorized to access that managed system. This is achieved because upon discovery, IBM Director Agent stores the IP address of each system running IBM Director Server. It is for this reason that your IBM Director Server should use a static IP address.

If the IP address of your management server has changed, you will need to issue various `cimsubscribe` commands on each agent to reestablish communications. This command is discussed in detail in 5.5, “Using cimsubscribe to process local events” on page 254.

1. Determine the UID of your management server. You can get the UID by double-clicking the management server in IBM Director Console to display system attributes. In the commands here, our server UID is 2f7c756f26b00121.
2. Delete the CIM subscription associated with the management server:
   cimsubscribe -ds -fn 2f7c756f26b00121 -hn 2f7c756f26b00121
3. Delete the filter with the name of the management server UID:
   cimsubscribe -df -fn 2f7c756f26b00121
4. Delete the handler with the name of the management server UID:
   cimsubscribe -dh -hn 2f7c756f26b00121
5. Delete the managed system from IBM Director Console.
6. Rediscover the managed system.

### 4.8 Uninstall

This section describes various aspects of uninstalling IBM Director.

#### 4.8.1 Silent uninstall

By using psexec.exe, you can remotely start an uninstallation of IBM Director Agent using the following syntax:

```
psexec \systemname -u userid -p password dirunins.exe agent deletedata silent
```

Psexec is a tool available for download from:

http://www.sysinternals.com/Utilities/psexec.html

#### 4.8.2 Uninstalling old versions of IBM Director

If you have trouble uninstalling older versions of IBM Director, try using the DirClean tool that is part of the IBM Director Support Tools, available from:


Tools in this package are as follows:

- **DirClean** assists with the uninstallation of IBM Director by removing registry data and files left behind by the Director uninstaller.
- **Filechek** identifies files associated with IBM Director that may not be properly replaced during a patch (minor) upgrade.
- **Twgrepair** fixes problems related to Windows installer and locked files, and with TWGIPC not stopping and hotfix 890859.
- *DirGather* captures information and files pertinent to debugging issues with IBM Director configurations.
- *DirStop* aids with stopping all Director-related services and processes.
IBM Director configuration

This chapter builds on the information presented in the product publication *IBM Director Systems Management Guide* and focuses on areas of customization that might need special consideration, particularly in more-complex IT environments. In particular, we will look at areas that are new to IBM Director 5.10 and may not be covered in detail elsewhere.

This chapter includes discussion of the following topics:

- 5.1, “AutoLogon shortcut” on page 228
- 5.2, “IBM Director discovery” on page 229
- 5.3, “IBM Director groups” on page 243
- 5.4, “SNMP configuration” on page 250
- 5.5, “Using cimsubscribe to process local events” on page 254
- 5.6, “Management server backup and restore” on page 265
5.1 AutoLogon shortcut

Before we get into configuration of IBM Director itself, here is a tip that can save a few keystrokes every time you need to log on to IBM Director Console. The management console can be launched from the command line using the following syntax:

"C:\Program Files\IBM\Director\bin\twgconw.exe" [-s] server user password

Where elements have the following definitions:

- -s is a switch to enable SSL security for the session.
- server is the name or IP address of the target IBM Director Server.
- user is the user account requesting logon.
- password is the password for the user account supplied.

Because Windows shortcuts can use command-line syntax, you can add logon information directly to the shortcut for IBM Director Console that gets added to the Windows Start menu during installation. To do this, follow these steps:

1. Locate the shortcut in the Start menu, or make a copy of it.
2. Right-click its icon and select Properties.
3. With the Shortcut tab selected, add the -s switch if you want to enable Console <> Server encryption.
4. Add the server, user name, and password parameters to the end of the Target field, as shown in Figure 5-1.

![Figure 5-1: Windows shortcut configured to automatically logon to IBM Director Console](image)

5. Click OK.

From now on, double-clicking the shortcut icon launches IBM Director Console and logs you in automatically.

**Important:** Creating such a shortcut has security implications. Anyone who has access to your system can look at the Properties page for the shortcut and see your user ID and password.

### 5.2 IBM Director discovery

Although the basic discovery process applies, in general, to all managed objects, we limit our discussion here to the discovery of managed systems. Discovery (more specifically, server-initiated discovery) is the process by which IBM Director Server identifies and establishes connections with managed systems.
The management server sends out a discovery request and waits for responses from managed systems. The managed systems listen for this request and respond to the management server that sent the request.

5.2.1 Firewalls

For a system to be discovered and managed by IBM Director Server, it must allow communication over specific ports using specific protocols. For a complete list of port requirements see 2.9, “Network ports” on page 57. If a system is running firewall software, this software must be configured to allow communication on the proper ports.

Because we believe that the vast majority of systems being managed by IBM Director are Windows-based systems, we provide specific guidelines here for configuring those systems to be managed. Although the details of firewall configuration vary, the concept of opening ports through a firewall is the same for any operating system.

Windows Firewall

An easily overlooked point of blockage is the Windows Firewall included in Microsoft Windows XP Service Pack 2. This personal firewall is enabled by default and prevents IBM Director Server from discovering any systems on which it is running.

Windows Firewall can be configured using multiple methods, including:

- Accessing the Windows Firewall Control Panel directly on each local computer
- Modifying the Windows Firewall Setup Information file (found in the Windows installation directory at %windir%\Inf\Netfw.inf) on each local computer
- Creating a Windows Computer Configuration Group Policy (Active Directory environments only) to configure Windows Firewall on all systems in the Domain
- Using netsh commands in scripts or at the command line

For more information about all the above methods, refer to the white paper titled Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2, available from Microsoft:


In addition, the white paper titled Using the Windows Firewall INF File in Microsoft Windows XP Service Pack 2 provides detailed information about using
the setup information file to configure Windows Firewall and can be downloaded from:


If you use Active Directory, we recommend that you consider using it combined with the Group Policy Object (GPO) Editor to simplify configuration of the Windows Firewall across an entire Active Directory domain.

While even a moderately detailed discussion of the Windows GPO Editor is outside the scope of this book, we present the steps we used in our lab to properly configure our Active Directory domain and Windows Firewall so that IBM Director can be used to effectively manage our Windows clients.

To complete the process outlined here, you must have the proper rights in the Windows domain to modify domain policy. To modify the Windows Firewall GPO settings on a domain-wide basis, log on to a domain controller and follow these steps:

1. Open the **Active Directory Users and Computers** Snap-In.
2. Right-click your Domain container and select **Properties**, as shown in Figure 5-2.

![Image of Active Directory Users and Computers](image-url)

**Figure 5-2**  Windows Active Directory Users and Groups Snap-In
3. In the Properties window, select the **Group Policy** tab. You see the Group Policy view, as shown in Figure 5-3.

![Figure 5-3 The Domain Properties window showing the Group Policy tab](image)

4. Although not strictly necessary, it is a good idea to ensure that the GPO you are configuring will not be overridden by another policy in the domain. To configure this setting, select **Default Domain Policy** and then click the **Options** button.
5. In the Default Domain Policy Options window, select the **No Override** check box, as shown in Figure 5-4.

![Figure 5-4 Default Domain Policy Options window with No Override option selected](image)

6. Click **OK** to return to the previous window.

7. With the Default Domain Policy still selected, click **Edit**. The GPO Editor window opens.
8. Navigate the GPO tree to **Administrative Templates → Network → Network Connections → Windows Firewall → Domain Policy**, as shown in Figure 5-5.

![Group Policy Object Editor window with Windows Firewall Domain Policy selected](image)

**Figure 5-5** Group Policy Object Editor window with Windows Firewall Domain Policy selected

**Tip:** If the Windows Firewall policy settings do not appear in your Group Policy Object Editor (**Computer Configuration → Administrative Templates → Network → Network Connections**), you must update your existing group policy objects with the new Windows Firewall policy settings. See the Microsoft white paper *Managing Windows XP Service Pack 2 Features Using Group Policy* for details:


9. To enable the GPO for Windows Firewall, double-click the **Windows Firewall: Protect all network connections** setting.
10. Click to select the **Enabled** radio button, as shown in Figure 5-6. There is nothing else to configure for this setting. This simply enables the GPO so that group policy now controls the settings that would otherwise be made in the Windows Firewall Control Panel on each domain member computer.

![Windows Firewall: Protect all network connections Properties](image)

*Figure 5-6  The Protect all network connections setting is used to enable Group Policy control of Windows Firewall*

Depending on which types of systems you intend to manage, you need to configure other GPO settings to open specific ports in Windows Firewall.

11. If you want to discover and manage Level-0 systems (systems on which there is no IBM Director Agent installed), open the **Windows Firewall: Allow file and printer sharing exception** setting by double-clicking this setting.

**Tip:** Level-0 system discovery and management of Windows systems uses DCOM on ports 137 UDP, 138 UDP, 139 TCP, and 445 TCP. Rather than entering each of these ports manually under the Define port exceptions setting, we use the “Allow file and printer sharing exception” because these are exactly the ports opened by this setting. Either method works.

12. Click the **Enabled** radio button.
13. In the “Allow unsolicited incoming messages from” field, enter the IP address of your management server. You can also enter multiple IP addresses if you have multiple management servers, or the wildcard character (*) to allow messages from any source, or “localsubnet” to allow messages only from the local subnet to reach your clients.

While a single IP address is obviously the most secure, this requires a static IP address for your management server (which is required anyway). Our configured setting for this GPO is shown in Figure 5-7.

![Windows Firewall: Allow file and printer sharing exception Properties](image)

*Figure 5-7* The Allow file and printer sharing exception setting is used to open multiple ports used by IBM Director to discover and manage Level-0 (Agentless) systems

14. If you intend to manage Level-1 systems (with IBM Director Core Services installed), open ports 5988 TCP and 5989 TCP. If you intend to manage Level-2 systems (with IBM Director Agent installed), open port 14247 UDP, 14247 TCP, and 14248 TCP. To do this, double-click the **Windows Firewall: Define port exceptions** setting to open its Properties window.
15. Click the **Enabled** radio button, as shown in Figure 5-8.

![Windows Firewall: Define port exceptions Properties](image)

*Figure 5-8  The Define port exceptions setting is used to open specific ports in Windows Firewall to allow IBM Director to discover and manage Windows XP systems*

16. Click the **Show** button to open the Show Contents window, where specific ports can be added.
17. Click the **Add** button and enter the required ports using the syntax described in the Properties window. Proper configuration for an environment managing both Level-1 and Level-2 systems is shown in Figure 5-9.

![Figure 5-9 The Show Contents window displaying a list of ports to open in Windows Firewall](image)

18. After all ports have been added, click **OK** to close the Show Contents window.

19. Click **OK** again to close the setting Properties window.

**Tip:** Although GPO settings are effective immediately, it might take some time for the new settings to be propagated to Domain systems. To test your settings, open a command prompt and issue the `gpupdate` command from any Domain member computer running Windows XP with Service Pack 2. When the update is complete, the new GPO settings should be reflected in the Windows Firewall Control Panel applet.

### 5.2.2 Types of discovery

After discovery occurs, several activities occur, depending on the level of the managed system and how the management server and managed system have been configured. These activities include authentication of the management server, determination of the secured status of the managed system, exchange of digital signature algorithm (DSA) key files, collection of hardware and software inventory data, transmission of process and resource monitors from the management server, and transmission of queued events from the managed system.
For more information about authentication and IBM Director Agent security see 3.4.5, “IBM Director Agent security” on page 133.

IBM Director supports four types of discovery:

- Broadcast
- Multicast
- Unicast
- Broadcast relay

The management server performs all four types of discovery simultaneously.

**Broadcast discovery**

Broadcast discovery sends out a general broadcast packet over the LAN. The destination address of this packet depends on the particular protocol used to communicate with the managed systems.

Broadcast discovery can also send out a broadcast packet to specific subnets. If you specify the IP address and subnet mask for a system (a discovery seed address), IBM Director sends a broadcast packet to that specific subnet and discovers all managed systems on that subnet.

This is the broadcast method of choice for smaller networks, especially those with a single subnet. Larger, more complicated networks, however, often do not allow broadcast packets to move between subnets. In this case, broadcast discovery only discovers those managed systems that reside on the same subnet as the management server.

**Multicast discovery**

Multicast discovery operates by sending a packet to the multicast address. By default, IBM Director uses 224.0.1.118 as the multicast address. Managed systems listen on port 14247 (default for Level-2 systems) at this address and respond to the multicast from the management server. Multicasts are defined with maximum time to live (TTL), which is the number of times a packet is passed between subnets. After the TTL expires, the packet is discarded.

The multicast address can be changed from the default value. You might need to do this if some other application is using the 224.0.1.118 address as its multicast group address. Note that you must change the multicast address on both the management server and the managed systems.
To do this on the management server, click **Options → Discovery Preferences**, then click the **Level 2: IBM Director Agents** tab and select the **System Discovery (IP)** radio button (Figure 5-10). Here you can configure the multicast group address, as well as specify whether to use TCP/IP general broadcasts.

![Discovery Preferences window, System Discovery (IP) tab](image)

If you change the multicast group address on the management server, you need to change it on the managed systems it is to manage as well. Otherwise, the management server will multicast on an IP address that is ignored by all managed systems. You can also change the port used for multicast discovery. To modify either of these settings on the managed system, follow the procedure outlined for the appropriate operating system.

**Note:** Multicast discovery is only available for TCP/IP.

For IBM Director Agent running under Windows:

1. Using a simple text editor such as Microsoft Notepad, create a TCPIP.INI file in the IBM Director Data directory. (c:\Program Files\IBM\Director\Data is the default.)
2. Specify the new multicast group address or multicast port number in this file using the following format:

```
MULTICASTADDR=xxx.xxx.xxx.xxx
PORT=xxxx
```

For IBM Director Agent running under Linux/AIX:

1. Locate the file TCPIP.NETExt in the /opt/IBM/Director/classes/extensions directory and open it with a text editor. Near or at the end of the file, find the following three lines (which are wrapped here):

```
# optional init string for TWGUDPSocket will override defaults - UDP port number (or *=default)
# followed by space followed by optional multicast group (or *=default)
#net.datagram.initstring=14249
```

2. To change the multicast group, uncomment the net.datagram.initstring line. For example, to set the multicast group UDP address to 224.0.1.119 using the default port (14247), type:

```
net.datagram.initstring=* 224.0.1.119
```

To set the multicast group UDP address to 224.0.1.119 and change the port number to 14250, use:

```
net.datagram.initstring=14250 224.0.1.119
```

**Note:** If you change the multicast port on the IBM Director Agent, you must match this change on any management servers that you want to manage this system. Because there is no way to change the port used by IBM Director Server in the Discovery Preferences window, you also need to follow one of the procedures above to change the multicast port number on a management server.

Multicasts are useful for networks that filter broadcasts, but that do not filter multicasts. Multicast discovery also can be used in a large IBM Director environment as a method to assign certain managed systems to specific management servers. If multicast discovery is the only discovery method employed (if all other discovery methods are disabled), only systems using the same multicast group address will see each other. Such a method can be used to segregate management servers and their clients without regard to subnet.

**Unicast discovery**

Unicast discovery sends a directed request to a specific address or range of addresses. This method can generate the most network traffic, as it sends a discovery request for each address in the ranges specified.
Unicast discovery is useful in large corporate networks where both broadcasts and multicasts are filtered. To discover certain types of managed systems (for example, dial-up systems), it might be necessary to use Unicast discovery.

This option also can be used effectively to limit the number of managed systems that are discovered. For example, you might want to discover only certain types of systems, such as your BladeCenter systems and chassis, which are located on a specific subnet. A specific management server (call it BladeMgr) can be configured to discover and manage only these systems, leaving other systems to be managed by other management servers. This approach might reduce network traffic associated with events generated by managed systems. Only the BladeCenter systems send events to BladeMgr. Because the other managed systems have never been discovered by BladeMgr, they do not send events to this management server.

Unicast discovery is only available for TCP/IP.

**Broadcast relay agents**

Broadcast relay allows the management server to discover TCP/IP and IPX systems when the systems cannot be reached directly by broadcast packets due to network configuration. This situation can occur in networks where the management server and managed systems are in separate subnets, and the network between them does not allow broadcast packets to pass from one subnet to the other.

This option generates less network traffic than Unicast discovery and avoids many of the problems associated with filtered broadcasts. In broadcast relay, the management server sends a special discovery request message to a particular managed system, instructing the managed system to perform a discovery on the local subnet using a general broadcast. When managed systems on that subnet receive the discovery request, they reply directly to the management server that made the original request.

You might want to consider this option for discovery if you have multiple physical locations in which managed systems reside, with lower-bandwidth network infrastructure (such as T1 or frame relay) between these physical sites. Because only a single discovery request is sent to each remote network, less traffic fills the WAN connection. Discovery actually takes place locally at full network bandwidth. Only the replies from each discovered system traverse the WAN.
5.3 IBM Director groups

Various types of groups can be created, including dynamic groups, static groups, and task-based groups. You also can create group categories (collections of groups) that are used to organize your groups. Group categories can be especially useful in a large managed environment.

We leave the discussion of creating and editing groups and group categories to the product publication *IBM Director Systems Management Guide*. In this section we focus on providing interesting and potentially useful group and category definitions. We show exactly how we created these groups and categories and discuss how they might be used to save you time and effort.

We need to define a couple of terms before we begin. The term *query* is used for inventory queries built into the Inventory Query Browser, as well as for criteria established to build a dynamic group in the Dynamic Group Editor. These are both, in fact, queries against the IBM Director inventory database. The term *available criteria* comes from the left pane of the Dynamic Group Editor.
5.3.1 Group example: operating system service pack level

It is often useful to determine the exact release of the operating system installed on your managed systems. This information is retrieved easily from the IBM Director inventory database. When this information is gathered from multiple systems, it looks as shown in Figure 5-11.

![Inventory Query Browser: Level 2: IBM Director Agents](image)

<table>
<thead>
<tr>
<th>Available Queries:</th>
<th>All</th>
<th>Query Results: Main OS Details(13)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Name (Syst.)</td>
</tr>
<tr>
<td>Custom</td>
<td></td>
<td>Director 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Watts 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Watts 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FS2-ID510</td>
</tr>
<tr>
<td></td>
<td></td>
<td>pSeries 630</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Snichonish</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Denai</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Columbia</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vesuvius</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Baker</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rundle 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Molinoh 2</td>
</tr>
</tbody>
</table>

Figure 5-11 Inventory query of operating system release level

However, sometimes it is useful to group managed systems based on the precise release or build of the operating system installed. For instance, you might need to install a security patch or device driver on only those managed systems that are running a specific release of an operating system. If you can group these systems using appropriate criteria, it might be possible to apply the update to the entire group at one time, directly from the IBM Director Console.

The following examples explain how this can work in both Windows service pack level and Linux kernel release.
To build a group of managed systems running a particular Windows service pack release, specify query criteria that yield the proper results. For this example, we create a query that returns all managed systems running Windows Server 2003 Service Pack 1 or later (notice the operator $\geq$ in the second criterion).

All true for the same operating system.
- Operating System / Name = Windows Server 2003
- Operating System / Revision (Build Level, Service Pack) $\geq$ Service Pack 1

This query is shown as dynamic group criteria in the Dynamic Group Editor displayed in Figure 5-12.

Figure 5-12 Selecting all Windows Server 2003 systems with SP1 or later
With the new IBM Director Console, it is easy to configure information columns to display any information you want to see about all your managed systems. Figure 5-13 shows a dynamic group called All Windows Systems, sorted by operating system, and the Service pack level installed on each. This is an easy and convenient way to see important information at a glance.

![IBM Director Console showing a dynamic group called All Windows Systems](image)

The service pack level is a fairly high-level indication of the currency of a Windows operating system. It is likely that you would need to have more detailed information available in order to determine if upgrades are necessary. This can be achieved very quickly using the same process as described above, but at a more detailed level.

### 5.3.2 Group example: Windows security patch level

One activity that can take up a significant amount of IT staff resource is that of tracking Windows security patch levels and ensuring that all systems have the
appropriate patches installed. It is fairly straightforward to get information about a particular patch through the Windows Update or Microsoft Update sites. An example of the details regarding a Microsoft security update is shown in Figure 5-14.

![Microsoft security update details](http://update.microsoft.com - Security Update for Win...)

**Security Update for Windows Server 2003 (KB908519)**

Date last published: 1/10/2006

Typical download size: 474 KB

A security issue has been identified that could allow an attacker to compromise your Microsoft Windows-based system and gain control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

**System Requirements**

Recommended CPU: Not specified.

Recommended memory: Not specified.

Recommended hard disk space: Not specified.

**How to Uninstall**

This software update can be removed via Add or Remove Programs in Control Panel.

**Get help and support**

http://support.microsoft.com

**More information**

- [http://go.microsoft.com/fwlink/?LinkId=55919](http://go.microsoft.com/fwlink/?LinkId=55919)

---

*Figure 5-14  Microsoft security update details*
IBM Director can help keep systems current by bringing attention to those systems that are missing critical updates. When you know which systems are missing important Microsoft security patches, you can take appropriate action such as pushing a patch out to managed systems using Software Distribution Premium Edition. Figure 5-15 shows a dynamic group configured in IBM Director that shows all systems that are missing Microsoft Security Update KB908519.

![IBM Director Console](image)

**Figure 5-15** Dynamic group showing all systems missing an important Microsoft security patch

Such a group is not limited to those systems that are missing an important update. This group can also be used as a target for a Software Distribution task that installs the security patch on those systems that do not already have it.

The key to configuring such a group easily is to use the *Installed Patches* software query of the inventory browser. This query displays all software installed and shown in the Add/Remove Programs Control Panel under Windows.

Notice in Figure 5-16 on page 249 that the package ID is a more reliable criterion for consideration than the Name field. In this example, three different package
names (all highlighted in the graphic) are used to describe the same package ID. Therefore, it is much more useful to key on package ID than name when attempting to create a dynamic group for this particular piece of software.

```
<table>
<thead>
<tr>
<th>Name (System)</th>
<th>Package ID (Installed Packages)</th>
<th>Name (Installed Packages)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H520-EBC04</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>TC-860-EBC02</td>
<td>KB908519</td>
<td>Security Update for Windows XP (KB908519)</td>
</tr>
<tr>
<td>HS40-EBC00</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>x366-EBC01</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>CMTOW-EBC</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>x306-EBC01</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>H520-EBC08</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>MSVS01</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>x346-EBC01</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>MSVS-Blade14</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>MSVS01</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>H520-EBC01</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>x336-EBC01</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>x720-EBC02</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>x350-EBC02</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>TC-860-EBC01</td>
<td>KB908519</td>
<td>Security Update for Windows XP (KB908519)</td>
</tr>
<tr>
<td>IntelliStation Z-Pro</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>DC1</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>MSVS-Blade13</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>ThinkPad-T23</td>
<td>KB908519</td>
<td>Windows 2000 Hotfix - KB908519</td>
</tr>
<tr>
<td>x460-EBC01</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>DC2</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>Director 5</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
<tr>
<td>x360-EBC01</td>
<td>KB908519</td>
<td>Security Update for Windows Server 2003 (KB908519)</td>
</tr>
</tbody>
</table>
```

*Figure 5-16  Inventory Query Browser showing systems with Windows security patch installed*
Keeping all of these points in mind, we created the group shown in Figure 5-15 on page 248 using the dynamic group query seen in Figure 5-17. Note that we used a second criterion to eliminate those systems that are not running Windows operating systems in our environment. We used the Operating System / Type = WINDOWS NT query, which is effective in finding all systems running Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003.

![Dynamic Group Editor](image)

*Figure 5-17 Dynamic Group Editor configured to find systems missing a security patch*

### 5.4 SNMP configuration

If you use SNMP to monitor systems or devices on your network, there are a few SNMP configuration tasks to consider as you implement an IBM Director management solution. The first has to do with automatically discovering SNMP devices that send traps to the management server. The next involves compiling MIB files and loading these compiled MIBs into management server memory. The final configuration task deals with native raw SNMP trap forwarding. We address each of these tasks here.

For more information about the SNMP Browser and compiling MIB files in IBM Director see 6.3.18, “SNMP Browser” on page 346.
5.4.1 Automated SNMP device discovery

IBM Director Server can be configured to automatically perform the discovery process on any device from which it receives an SNMP trap. The discovery process adds the device to the management server database, adds a managed object for the device to the management console, and performs an SNMP inventory collection on the device.

To enable automatic discovery of SNMP devices, follow these steps:

1. From the management console main menu, select **Options → Discovery Preferences**.

2. In the Discovery Preferences window, click to enable the **Auto-add unknown agents which contact server** check box, as shown in Figure 5-18.

3. Click **OK** to close the Discovery Preferences window.

Once configured, any SNMP device that sends a trap to IBM Director Server will be discovered and added to the management console so that the
Inventory, SNMP Browser, and other tasks can be used to manage the device.

5.4.2 Auto recompile and load of MIB data

Two processes are required to provide human-readable output in the SNMP Browser task of IBM Director. First, Management Information Base (MIB) files must be compiled by IBM Director Server. Then the compiled MIB data (stored as .mibdata files) must be loaded into memory on the management server.

Recompiling MIB files

IBM Director Server can be configured to recompile MIB files when it starts. In previous versions of the product, this was the default behavior. However, in IBM Director 5.10 the behavior is controlled by the SNMPServer.properties file. By default, MIB files are not recompiled automatically on restart of the management server.

To change this default behavior and configure IBM Director Server to recompile MIB files automatically on restart, perform the following steps:

1. Ensure that all management consoles (local and remote) are logged off.
2. Stop the IBM Director Support Program. At a command prompt enter `net stop twgipc` (Windows) or `twgstop` (Linux default path /opt/ibm/director/bin).
3. Open the SNMPServer.properties file with a text editor.
   This file is located in `C:\Program Files\IBM\Director\data\snmp` (Windows) or `/opt/ibm/director/data/snmp` (Linux).

   **Tip:** It is always a good practice to make a copy of any file you intend to modify before you make changes, to assist in recovering from unexpected results.

4. To begin automatic recompile of MIB files at server restart, change `false` to `true` in the following line:
   ```
   snmp.recompileOnStartup=false
   ```

5. You can also specify that loaded MIB imports should be recompiled on restart. This is generally not necessary, but can be useful in the case of a complicated MIB file that has multiple dependencies. To begin automatic recompile of loaded MIB file imports at server restart, change `false` to `true` in the following line:
   ```
   snmp.recompileImports=false
   ```
Loading MIB data into memory

The second process required to provide human-readable output in the SNMP Browser task is that compiled MIB data must be loaded into memory on the management server. This is achieved manually by using the Manage MIBs subtask under SNMP Browser in the management console.

Manually compiling a MIB file using the Manage MIBs subtask also loads the resulting .mibdata file into management server memory. You can also load and unload MIBs manually by using the Manage MIBs subtask. Any changes made using this technique are written to a binary file (loadedmibs.dat) and stored as persistent data on the management server. Each time the management server is restarted, it reloads into memory all MIB data files that are specified by this file.

5.4.3 SNMP trap forwarding

You can forward SNMP traps in one of two ways:

- Through the Event Action Plan Builder
- By configuring the SNMPServer.properties file

If you use the Event Action Plan Builder to forward SNMP traps, the traps are converted to IBM Director traps. However, there are times when you might prefer to have the unmodified raw SNMP trap forwarded to another host.

Complete the following steps to forward SNMP traps without modification:

1. Ensure that all management consoles (local and remote) are logged off.
2. Stop the IBM Director Support Program. At a command prompt enter `net stop twgipc` (Windows) or `twgstop` (Linux default path `/opt/ibm/director/bin`).
3. Open the SNMPServer.properties file with a text editor.
   This file is located in `C:\Program Files\IBM\Director\data\snmp` (Windows) or `/opt/ibm/director/data/snmp` (Linux).

   **Tip:** It is always a good practice to make a copy of any file you intend to modify before you make changes to assist in recovering from unexpected results.

4. To forward SNMPv1 traps:
   a. Remove the pound character (#) at the beginning of this line:
      
      ```
      #snmp.trap.v1.forward.address.1=
      ```
   b. Type the IP address of the SNMPv1 trap destination at the end of the line.
c. Remove the pound character (#) at the beginning of this line:
    #snmp.trap.v1.forward.port.1=

d. Type the port number of the SNMPv1 trap destination at the end of the line.

5. To forward SNMPv2 traps:
   a. Remove the pound character (#) at the beginning of this line:
      #snmp.trap.v2.forward.address.1=
   b. Type the IP address of the SNMPv2 trap destination at the end of the line.
   c. Remove the pound character (#) at the beginning of this line:
      #snmp.trap.v2.forward.port.1=
   d. Type the port number of the SNMPv2 trap destination at the end of the line.

6. Optional: To set a second or a third destination, edit the applicable lines in the
    SNMPServer.properties file.

7. Save the file, ensuring that you do not change the file name or save it as a .txt file.

8. Restart the IBM Director Server service using `net start twgipc` (Windows)
    or `twgstart` (Linux).

**Important:** Be careful not to configure a trap destination that sends traps to
the management server itself, because you might create a loop.

### 5.5 Using cimsubscribe to process local events

The cimsubscribe utility is used to configure the processing of CIM-based
hardware events (called *CIM indications*) locally on the managed system.

This utility allows you to control what events are sent. For example, if you do not
want to get normal events using SNMP, you could use cimsubscribe to turn off all
the subscriptions to normal event filters and SNMP. You might also want to turn
on local pop-ups for specific events.

In previous versions of IBM Director Agent, you could use the Web-based
Access utility to configure local events. However, this was only for
Windows-based managed systems. The use of cimsubscribe can be on all IBM
Director Agent systems and can be scripted for mass configuration.
The utility is installed as part of IBM Director Agent (both Level-1 and Level-2) in the Director\CIMOM\BIN directory (for Windows installs, for example, this is c:\Program Files\IBM\Director\CIMOM\BIN).

In some respects CIM events are similar in structure to event action plans (EAPs) in IBM Director. Whereas EAPs have event filters, event actions, and event action plans, CIM events have filters, handlers, and subscriptions.

### 5.5.1 Filter

*Filters* can be thought of as thresholds, or items being monitored. You can think of a filter as a simple filter in the Event Action Plan Builder. An example of a filter is *Service Processor Generic Fan Criticals*.

Filters are automatically created during the installation of IBM Director, based on the detected hardware capabilities. Therefore, we do not recommend deleting the predefined filters, even though it is possible to do that. You can also create your own filters.

There are approximately 90 filters predefined, as listed in Table B-2 on page 931.

When specifying a filter name on the cimsubscribe command line, if it has spaces in the name, enclose the name with double quotation marks, such as "Service Processor Generic Fan Criticals".

**Note:** The names of filters are case-sensitive.

After a managed system is discovered by IBM Director Server, a new filter is automatically created. The name of the filter is the unique ID (UID) of the particular management server. See 5.5.5, “Subscriptions to IBM Director Server” on page 264, for details.

### 5.5.2 Handler

A *handler* is a way of processing an event. You can think of a handler as an action in the Event Action Plan Builder. An example of a handler is *pop-up*. Handlers for processing the hardware events, including displaying a pop-up message, logging in the local operating system event log, and converting to SNMP Traps are automatically created during the installation of IBM Director.

As with the standard filters, we do not recommend deleting the predefined handlers, even though it is possible to do that.
The standard handlers are:

- **SNMP**
  This handler sends an SNMP alert to the systems defined by the local operating system.
  For Linux, this is the NetSNMP Agent.
  For Windows, you might first have to install SNMP on the managed system, as follows:
  a. From the Control Panel, start **Add/Remove Programs**.
  b. Click **Add/Remove Windows Components**.
  c. Highlight **Management and Monitoring Tools** and click **Details**.
  d. Select **Simple Network Management Protocol** and click **OK**.
  e. Click **Next** to install SNMP.
  f. During the installation, you might be prompted to supply operating system installation CD-ROMs.

  After SNMP is installed, open Services (run services.msc), scroll down to SNMP Service, right-click it, and click **Properties**. In the Traps tab, enter a community name and trap destinations where you want the alerts to be sent.

- **SMS**
  This handler sends events to Microsoft Systems Management Server (SMS).
  To use this handler, you must have the SMS agent installed locally. This handler is not configurable.

- **PopUp**
  Display a pop-up on the local system. See Example 5-19 on page 262 for an example.

- **Health**
  The Health handler sends events to the IBMPSPG_ComponentHealth Class.
  This is a CIM Class used to store a snapshot of the system’s hardware and its status. A variety of applications including IBM Director uses this information to display status information about the managed system.

- **TEC**
  This handler sends alerts to Tivoli Enterprise™ Console (TEC) and requires that the TEC agent be installed locally.

  There is some configuration that can be done for TEC by editing the file cimom/data/cimclient/TivoliConsumer.cfg. Parameters in this file are:
  - **tecEventCommand**: Specify the Tivoli command to be used to send events to TEC. Choices are TME®, which uses wpostemsg (secure, uses
Tivoli Endpoint Services) or nonTME, which uses postemsg (non secure, no Tivoli endpoint required). TME is the default.

- tecConfigFile: Specify whether the cimom/data/cimclient/tecad_eif.conf file is used to configure the Tivoli adapter. The default is false (no). Consult the Tivoli documentation on how to configure this file. Here the user can configure destination and a wide variety of other settings.

By default, wpostemsg is used with no config file. In this case, the Tivoli End Consumer uses the wpostemsg command and Tivoli Endpoint Services. It sends events to any TEC Server that has discovered this agent.

- Log writes the event to the Windows Event Log or syslog on Linux.

**Note:** The names of handlers are case-sensitive.

After a managed system is discovered by IBM Director Server, a new handler is automatically created. The name of the handler is the unique ID (UID) of the particular management server. See 5.5.5, “Subscriptions to IBM Director Server” on page 264, for details.

### 5.5.3 Subscription

A *subscription* is the assignment of a filter to a handler so the event can be processed. You can think of a subscription as an event action plan.

Subscriptions are automatically created during the installation of IBM Director for most, but not all, handlers. Subscriptions can be created and deleted as needed to modify the processing of the hardware events.

Every predefined filter is by default bound to handlers SNMP, SMS, TEC, and Log and many of the predefined filters are also defined to handler Health. No subscriptions use handler PopUp by default.

A full list of subscriptions showing the filter and handler combinations is shown in Table B-3 on page 936.

After a managed system is discovered by IBM Director Server, a new subscription is automatically created, which enables the sending of events from IBM Director Agent to IBM Director Server. See 5.5.5, “Subscriptions to IBM Director Server” on page 264, for details.
5.5.4 Using cimsubscribe

There are a number of ways to use cimsubscribe:

- As a command line, where all parameters are passed on the command line
- Interactively using the -i parameter
- In batch, using the -b filename parameter where all commands are in the supplied file

In addition, you can issue commands against the local IBM Director Agent installation, or you can specify that the commands update a remote system by using the -l location parameter. The remote system must also have Director Agent (Level-1 or Level-2) installed.

A complete list of the parameters that cimsubscribe accepts can be found in the IBM Director Systems Management Guide or by issuing the following command:

cimsubscribe -h

cimsubscribe -h > cimsubscribe.txt

We recommend that you use the second command listed above to pipe the output of the help parameter to a text file for later review. For convenience, the output of the help command is listed in Example 5-1.

Example 5-1  Output from the cimsubscribe -h command

cimsubscribe
  Create and Delete CIM Indication subscriptions

Create a new Filter:
cimsubscribe -cf -fn <filterName> -q <query>

Create a new Handler:
cimsubscribe -ch -hn <handlerName> -d <destination>

Create a new Subscription:
cimsubscribe -cs -fn <filterName> -hn <handlerName>

Delete an existing Filter:
cimsubscribe -df -fn <filterName>

Delete an existing Handler:
cimsubscribe -dh -hn <handlerName>

Delete an existing Subscription:
cimsubscribe -ds -fn <filterName> -hn <handlerName>

Parameters:
------------------------
-lf -listfilters     List the current set of CIM_IndicationFilter
-1h -listhandlers   List the current set of CIM_IndicationHandlerCIMXML
-1s -listsubscriptions List the current set of CIM_IndicationSubscription
-cf -createfilter   Create a new CIM_IndicationFilter
                     Requires the -fn -q option
-ch -createhandler  Create a new CIM_IndicationHandlerCIMXML
                     Requires the -hn -d option
-cs -createsubscription Create a new CIM_IndicationSubscription
                     Requires the -fn and -hn option
                     Will do a check to ensure the specified
                     handler and filter exist.
-df -deletefilter    Deletes the specified CIM_IndicationFilter
                     Will do a check to ensure the specified
                     filter exists. Also checks to see if an existing
                     CIM_IndicationSubscription is using this filter.
                     Returns error if the filter is in use or does not exist
                     Requires the -fn option or the -a option for ALL
-dh -deletehandler   Deletes the specified CIM_IndicationHandlerCIMXML
                     Will do a check to ensure the specified
                     handler exists. Also checks to see if an existing
                     CIM_IndicationSubscription is using this handler.
                     Returns error if the handler is in use or does not exist
                     Requires the -hn option or the -a option for ALL
-ds -deletesubscription Deletes the specified CIM_IndicationSubscription
                     First checks to ensure that the specified
                     subscription exists.
                     Requires the -fn and -hn option or the -a option for ALL
-q -query           A WQL query used to filter CIM_Indication instances.
                     eg:
                     "SELECT * FROM IBM_AlertIndication where Severity = 2"
-d -destination A URL used to identify an End Consumer location. eg: "http://localhost:6988/CIMListener/syslog"

-fn -filtername Used to identify a specific CIM_IndicationFilter instance

-hn -handlername Used to identify a specific CIM_IndicationHandlerCIMXML instance

-a Used to specify ALL in a deletion operation

Optional parameters:
------------------------

-n -namespace Namespace. The default is "root/ibmsd"

-l -location The hostname and port of the system on which to modify subscriptions. Requires a username and password for non-localhost destinations. Requires a fully qualified hostname when creating a remote filter, handler, or subscription, eg:

remotehost.raleigh.ibm.com:5988
default is:
localhost:5988

-u -username User. Allows input of a username for authentication

-p -password Password. Allows input of a password for server authentication of the command.

-s -secure <yes | no>
Use this flag to specify communication with the HTTP or HTTPS protocol
yes - will connect securely to port 5989 (by default)
no  - will connect to port 5988 (by default)
If this flag is not specified, HTTP will be used.

-k -key <client private key file>
Full system path to the client private key file. Only valid if using HTTPS port
For example, 'c:\test\client.key'

-c -certificate <client certificate file>
Full system path to the client x509 certificate. Only valid if using HTTPS port
For example, 'c:\test\client.cert'

-i Interactive mode
Prompts user for information to assist in Filter/Handler/Subscription creation.

-b Batch mode
Specify a file to read in large batches of subscriptions. Each line of the file is read and processed like a standard cimsubscribe command.

-h or -? Displays this message.

To see what subscriptions, filters, and handlers are already defined, use the matching list command:

```
cimsubscribe -ls  To list all subscriptions
```
```
cimsubscribe -lf  To list all filters
```
```
cimsubscribe -lh  To list all handlers
```

Once again, we recommend that you pipe the output to a text file.

**Tip:** The output of these commands is very long, but we have tabulated the default subscriptions, filters, and handlers in Appendix B, “CIM subscriptions” on page 929.

A review of Table B-3 on page 936 shows that no predefined subscriptions use the Popup handler to display a pop-up on the managed system. This default is different from the one with IBM Director 4.x.

To create a new subscription, use the following command syntax:

```
cimsubscribe -cs -fn filter -hn handler [options]
```

As an example, to create a subscription that associates the pop-up action with filters Storage Criticals and Storage Warnings, issue the following commands:

```
cimsubscribe -cs -fn "Storage Criticals" -hn PopUp
```
```
cimsubscribe -cs -fn "Storage Warnings" -hn PopUp
```
If the command is successful, you are simply be returned to the command prompt, as shown in Example 5-2.

**Note:** The *IBM Director Systems Management Guide* incorrectly lists the syntax of deleting a subscription as `-ds -sn subscription_name`. The correct syntax is `-ds -fn filter -hn handler`.

**Example 5-2  Creating new CIM subscriptions**

C:\Program Files\IBM\Director\cimom\bin>cimsubscribe -cs -fn "Storage Criticals" -hn PopUp
Connecting to localhost:5988...
C:\Program Files\IBM\Director\cimom\bin>cimsubscribe -cs -fn "Storage Warnings" -hn PopUp
Connecting to localhost:5988...

C:\Program Files\IBM\Director\cimom\bin>

**Tip:** There is little error checking with the *cimsubscribe* command. Errors such as leaving off the quotation marks or specifying *popup* instead of *PopUp* will not return an error message. The only way to confirm the update is to issue a *cimsubscribe -ls* command and review the output.

Now when you run low on disk storage on the managed system, you can see the window shown in Example 5-19 on that system.

![Figure 5-19  Error message as a result of the CIM subscription](image)

If you later want to delete these new pop-up subscriptions, use the following commands:

```
cimsubscribe -ds -fn "Storage Criticals" -hn PopUp
cimsubscribe -ds -fn "Storage Warnings" -hn PopUp
```
As we said earlier, you can also use `cimsubscribe` interactively. Example 5-3 shows the output when creating these subscriptions.

Remember the following points when using `cimsubscribe`:

- The default namespace is `root/ibmsd`. However, you must still enter it when prompted.
- If you say Yes to wanting a secure connection, then you must specify the location of a client x509 certificate.
- Case is significant. For example, `popup` and `PopUp` are different handlers.

**Example 5-3 Output from an interactive session**

```
C:\Program Files\IBM\Director\cimom\bin>cimsubscribe -i
What system would you like to connect to?
1. localhost
2. remote host
1
What port would you like to connect to?
1. 5988 (HTTP)
2. 5989 (HTTPS)
3. Another port
1
Enter the namespace.
root/ibmsd
Do you want a secure connection?
1. Yes
2. No
2
Connecting to localhost:5988...
Interactive mode

What would you like to do?
1. Create a filter
2. Create a handler
3. Create a subscription (bind an existing filter and handler)
4. Delete an existing filter
5. Delete an existing handler
6. Delete an existing subscription
7. Exit
3
```

To create a subscription you must provide a Filter->Handler pair.
What is the name of the Filter you would like to use?
Storage Criticals

What is the name of the Handler you would like to bind it to?
PopUp

What would you like to do?
1. Create a filter
2. Create a handler
3. Create a subscription (bind an existing filter and handler)
4. Delete an existing filter
5. Delete an existing handler
6. Delete an existing subscription
7. Exit
7

C:\Program Files\IBM\Director\cimom\bin>

5.5.5 Subscriptions to IBM Director Server

Whenever a management server establishes contact (either through discovery or manually adding the agent to the console), a new filter, handler, and subscription are automatically created. It is this subscription that enables the sending of events from IBM Director Agent to IBM Director Server. This applies to both Level-1 and Level-2 managed systems.

The name of the filter and handler is the unique ID (UID) of the IBM Director Server. The filter receives all events from CIM_AlertIndication, which effectively means all events. The handler sends the event to the IBM Director server with its IP address.

For example, if the IBM Director Server UID is 2f7c756f26b00121, then the filter is defined as:

Name 2f7c756f26b00121
Query SELECT * from CIM_AlertIndication

The handler is defined in one of two ways, depending on whether the managed system has Level-1 or Level-2 agent installed:

- Level-1 (IBM Director Core Services):

  Name 2f7c756f26b00121
  Destination http://192.168.128.51:6988/CIMListener/
  DirectorConsumer/192.168.128.51
Level-2 (IBM Director Agent):

<table>
<thead>
<tr>
<th>Name</th>
<th>2f7c756f26b00121</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td><a href="http://localhost:6988/CIMListener/DirectorConsumer/192.168.128.51">http://localhost:6988/CIMListener/DirectorConsumer/192.168.128.51</a></td>
</tr>
</tbody>
</table>

The handlers for the two agent types are different because a Level-1 agent does not support IBM Director interprocess communications (IPC), while Level-2 IBM Director Agent does. The Level-1 agent uses the DirectorConsumer handler on the management server (the http://192.168.128.51 in the destination), while the Level-2 agent uses the DirectorConsumer handler locally (http://localhost), which, in turn, sends the event using IPC to IBM Director Server.

The subscription that gets automatically created binds the filter and the handler together, so that all CIM indications are forwarded to IBM Director Server for further processing with IBM Director event action plans.

**Note:** Because the handler uses the IP address and UID of the management server, it is essential that these not change. This is why a static IP address is required for the management server.

If the IP address of your management server changes, you must perform the following steps on each agent (assuming the management server UID is as just stated):

1. Delete the subscription with the name of the management server UID. You can get the UID by double-clicking the management server in IBM Director Console to display system attributes:
   ```
cimsubscribe -ds -fn 2f7c756f26b00121 -hn 2f7c756f26b00121
   ```
2. Delete the filter with the name of the management server UID:
   ```
cimsubscribe -df -fn 2f7c756f26b00121
   ```
3. Delete the handler with the name of the management server UID:
   ```
cimsubscribe -dh -hn 2f7c756f26b00121
   ```
4. Delete the managed system from IBM Director Console.
5. Re-discover the managed system.

### 5.6 Management server backup and restore

Configuring IBM Director Server, including the creation of dynamic groups, custom inventory queries, event action plans, resource and process monitors, and so on, can be a time-consuming process that takes weeks or months to
implement fully for your environment. Therefore, we strongly recommend that you plan a backup strategy for IBM Director Server.

There are three main backup mechanisms that should be considered for the management server. You can export many of the most important settings from the management console. You can use special command-line commands at the management server to effect complete backup and restore. You can use a typical system backup approach to back up the management server like any other mission-critical system. These mechanisms do not exclude each other, so it is possible to use a combination of all three of them.

5.6.1 Exporting IBM Director Server settings

The export function is available in a number of places within IBM Director. Probably the two most effective exports in terms of management server backup are in the areas of group management and event action plans. If you regularly export groups and EAPs, you will have captured many of the most crucial settings. No matter which of the other backup mechanisms are used, we strongly recommend periodic export of management server settings in these two areas.

As always with any backup strategy, make sure to store all exports in a safe location on a different system so that you can retrieve them in the event of a disaster.

**Exporting groups**

To export group information from IBM Director Server, follow these steps:

1. In the management console, select **Console → Export Groups** to open the Group Export window.
2. In the Group Export window, select the groups that you want to export using Shift+click or Ctrl+click, as shown in Figure 5-20.

![Group Export window showing multiple groups selected for export](image)

Figure 5-20  Group Export window showing multiple groups selected for export

Not all groups are exportable. Static groups in particular cannot be exported. Many of the default standard groups, such as All Managed Objects, Level-2: IBM Director Agents, Physical Platforms, and others, are not exportable. Most of these groups cannot be deleted and, therefore, exist on any IBM Director Server.
3. Enter the full path and file name for the group export, then click Export to initiate the export.

Any directories in the path must already exist or the export fails. In the example presented in Figure 5-20 on page 267, if the Director Exports directory does not exist, then the export fails with the message shown in Figure 5-21.

![Figure 5-21 Group export failure due to missing directory](image)

When a group export is successful, the export file can be imported into any IBM Director Server. To import groups into a management server, follow these steps:

1. In the management console, select **Console → Import Groups** to open the Group Import window.

2. In the Group Import window, select the source (server or local), then navigate to the group export file you want to import, as shown in Figure 5-22.

![Figure 5-22 Group Import window showing group export file to import from the local system](image)
3. Click **OK** to begin the import process and open a second Group Import window.

4. There are several options for importing groups. In this example, we import groups into a backup management server, so we want to import only the non-duplicate groups. To achieve this, select **Function → Non-duplicates → Add All**, as shown in Figure 5-23.

![Figure 5-23](image.png)  
*Figure 5-23  Group Import window, choosing to add all non-duplicate groups*
5. Continuing our example, we must now select the groups to import. A quick way to select all non-duplicate groups is available in the menu. To do this, choose **Select → Select All Non-duplicates**, as shown in Figure 5-24.

![Group Import window selecting all non-duplicate groups for import](image)

*Figure 5-24  Group Import window selecting all non-duplicate groups for import*
6. With the non-duplicate groups selected in Figure 5-24 on page 270, select **Import → Import Selected Groups** to import the selected groups into the management server.

The final Group Import window shows a summary of the import function, including a Function Result column, which displays Added for each group you selected to import, as illustrated in Figure 5-25.

7. Close the Group Import window. When you return to the management console, all imported groups are now displayed and populated as appropriate.

**Exporting event action plans**

EAPs can be exported in multiple formats. The *archive* format is the one you should choose if you want to import the file into another management server. Just as with group exports, EAP archive exports can be imported into any IBM Director Server at a later time, including a redundant management server or a restored primary management server.

To export one or more EAPs in archive format, follow these steps:

1. Open the EAP Builder and select all EAPs that you want to export using Shift+click or Ctrl+click.
2. Select **File → Export → Archive** to bring up the Select Archive File For Export window, as shown in Figure 5-26.

![Select Archive File For Export window with export file parameters specified](image)

**Figure 5-26 Select Archive File For Export window with export file parameters specified**

3. Choose a location and file name for the export and click **OK** to export. It is not necessary to provide an extension for the file name.

After a set of EAPs has been exported to an archive file, this archive can be imported into any IBM Director Server. To import an EAP archive file, follow these steps:

1. Open the EAP Builder on the management server into which you want to import the EAP archive.

2. Select **File → Import → Archive**.
3. In the Select Archive File For Import window, select the source (server or local), then navigate to the EAP archive export file you want to import, as shown in Figure 5-27.

![Select Archive File For Import window with archive selected](image)

*Figure 5-27  Select Archive File For Import window with archive selected*
4. When you have navigated to the proper file, click **OK** to begin the import process and open the Import Event Action Plan window, as shown in Figure 5-28.

![Import Event Action Plan](image)

Figure 5-28 Import Event Action Plan window showing EAPs about to be imported

5. If the EAP was previously assigned to managed objects or groups, you can preserve those assignments during the import process by clicking the **Preserve Associations** check box.

6. Click **Import** to complete the process and implement the archived EAPs on the current management server.

   Importing an EAP archive reestablishes all EAPs contained in the archive, all Event Filters and Actions contained in those EAPs, and, if selected, all associations with managed systems and groups.
In addition to the archive export, consider the HTML format export for EAPs. This option is very useful for documenting EAPs in human-readable format. You can open the exported HTML document in any Web browser. As you can see in Figure 5-29 on page 276, it is easy to understand the EAP hierarchy from this representation. You can see not only the EAP details, but also specific customizations of event filters and actions.

To export one or more EAPs in HTML format, follow these steps:

1. Open the EAP Builder and select all of the EAPs that you want to export using Shift+click or Ctrl+click.
3. Choose a location and file name and click **OK** to export. The resulting HTML file (Figure 5-29) can be opened with any Web browser or Microsoft Word.

![Event Action Plan](image)

**Event Action Plan**

*Wednesday, November 16, 2005 3:02:08 PM*

**Event Action Plan**: Solitaire Killer
- **Event Filter**: Solitaire Started
  - **Filter Type**: Simple Event Filter
  - **Event Type**: Director, Director Agent, Process Monitors, Process Alert, Process Started, SOL.EXE

**Extended Attributes**
- **Action Name**: Net Send to &System
  - Program Specification: net send &System Stop screwing around and get back to work!
  - Working Directory: null
  - Language: English (United States)
  - Time Zone: America/New_York

- **Action Name**: Solitaire Ticker
  - Message: Solitaire started on &System &Date
  - User(s): *
  - Language: English (United States)
  - Time Zone: America/New_York

- **Action Name**: Kill Solitaire
  - Program specification: C:\Program Files\IBM\Director\support\dakill sol.exe
  - Working Directory: null
  - Language: English (United States)
  - Time Zone: America/New_York

*Figure 5-29 Event action plan exported as an HTML document*
5.6.2 Special command-line tools

There are a few important command-line tools that are very useful in backing up and restoring the state of IBM Director Server. We discuss the `twgsave`, `twgrestore`, and `twgreset` commands here. To use these commands, simply open a command prompt window on the management server.

**twgsave**

The `twgsave` command saves a complete set of management server configuration data to a directory named `director.save.#`, where `#` is the sequential number of the backup on a given management server (for example, the third backup will be saved to a directory named `director.save.3`). The backup directories are saved in `C:\Program Files\IBM` under Windows and `/opt/ibm` under Linux.

The syntax of the `twgsave` command is:

```
twgsave [-s]
```

The optional parameter `-s` means *do not save software distribution packages*. This helps reduce the size of the backup files.

These files should be stored in a separate, safe location. The advantage of this tool is that it saves the complete configuration of your IBM Director Server, which you will be able to restore to a backup management server in the event of a disaster.

**Tip:** An easily implemented process is to schedule a batch file that stops IBM Director Server, performs the `twgsave` command, and then restarts IBM Director Server. In this way you can ensure multiple restore points. You can go back in time if you need to restore the configuration.

**Note:** The `twgsave` command does not save any database information. This data must be saved separately, using the normal database backup procedure.

**twgrestore**

The `twgrestore` command restores saved data to IBM Director Server. This command can also be used to restore configuration data from one management server to another in order to replicate a management server. Be sure that you select the switch to *not* restore the server ID, because having duplicate server IDs causes problems.
The syntax of the `twgrestore` command is:

```
twgrestore [-t] directory
```

The optional parameter `-t` means *restore data but do not restore the server ID and system name*. Use this option when restoring management server configuration data to a different system that takes on the role of management server. This might be a redundant management server or an additional management server to handle a large and complicated network infrastructure. The directory parameter specifies the location of a previously saved set of configuration files created using the `twgsave` command.

**twgreset**

A third command, `twgreset`, returns IBM Director Server to its original installation defaults. It also clears all tables in the database. Optionally, you can specify that you want to erase the system ID files.

The syntax of the `twgreset` command is:

```
twgreset [-i]
```

The optional parameter `-i` means *erase the system’s unique identification files*. You might want to specify this option after using both the `twgrestore` and `twgreset` commands on the same management server in order to ensure that only data from the restored data set is available to the new management server.

**Tip:** If you encounter problems and must consider reinstalling IBM Director Server, try the `twgreset` command first. It can save you time.

You can save and restore management server data using the above commands only when the IBM Director Support Program is stopped. To stop IBM Director Server, open a command prompt and enter `net stop twgipc` (Windows) or `twgstop` (Linux default path `/opt/ibm/director/bin`). To restart IBM Director Server, enter `net start twgipc` or `twgstart`, respectively.

### 5.6.3 Normal system backup

IBM Director Server can and should be backed up on a regular basis using your normal backup software (for example, Tivoli Storage Manager). The advantage of this solution is that backups will be performed automatically with your backup software storing the data in a safe location. To implement this method, simply include the management server with other mission-critical systems that are backed up on a regular basis.
To ensure a more complete backup, we recommend that you stop the IBM Director Support Program on the management server prior to backup. You can do this from the command line as discussed in the previous section.

Any or all of the these three mechanisms can be used to back up IBM Director Server. The first two, exporting management server settings and using the *twgxxxx* commands, can be very effective in bringing up additional IBM Director Servers as well. You might consider adding another management server to your environment for a number of reasons, including a large and complex network infrastructure, or simply to implement redundant IBM Director Servers.
IBM Director tasks

IBM Director provides a robust suite of systems management functionality in its base configuration. Many of these key functions are delivered as tasks in the right-most pane (when visible) of IBM Director Console. In addition, IBM Director's framework allows for optional extensions to be added after initial installation, which enable additional tasks and functionality.

This chapter covers the required agent levels and an overview of base tasks, as well as the tasks that are added by IBM Director extensions that were available at the time of this writing. We have also provided examples of use and configuration for some of the more sophisticated tasks IBM Director provides:

- 6.1, “Tasks by agent level” on page 282
- 6.2, “Tasks by operating system” on page 286
- 6.3, “Base tasks” on page 288
- 6.4, “Mass Configuration” on page 366
- 6.5, “Install-time extension tasks” on page 376
- 6.6, “Free extension tasks” on page 384
- 6.7, “Fee-based extension tasks” on page 398
6.1 Tasks by agent level

It is important to understand the concept of a tiered management agent, because the level of agent you install will be based on the functionality you require in your environment.

To provide functionality, tasks rely on specific code, both on the management server and on the managed object. As described in Chapter 1 of the product publication *IBM Director Planning, Installation, and Configuration Guide*, there are three agent levels supported by the product, Level-0, Level-1, and Level-2.

6.1.1 IBM Director base tasks

Some functionality is available without an agent (Level-0 systems), working only with the underlying operating system. Systems with IBM Director Core Services installed (Level-1 systems) provide a basic set of tasks. Systems with the full IBM Director Agent installed (Level-2 systems) provide the full suite of tasks included with the base IBM Director offering. See Table 6-1 for a summary of base IBM Director tasks and the agent level required for each.

Task functionality is dependant on the level of agent that the managed object is recognized as by IBM Director. Table 6-1 provides an overview of what agent level is required by each task.

*Table 6-1  Tasks available by IBM Director Agent level*

<table>
<thead>
<tr>
<th>IBM Director base tasks</th>
<th>Page</th>
<th>Level-0</th>
<th>Level-1</th>
<th>Level-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset ID</td>
<td>289</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>CIM Browser</td>
<td>290</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Configure SNMP Agent</td>
<td>291</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Event Action Plans</td>
<td>291</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Event log</td>
<td>292</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>External application launcha</td>
<td>292</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>File transfer</td>
<td>307</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Hardware status</td>
<td>308</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Inventoryb</td>
<td>310</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Cluster Browser</td>
<td>314</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Network configuration</td>
<td>314</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Power management support

Managed systems must meet certain criteria for the power management task to work. The power management task is provided using the right-click feature on managed objects in IBM Director Console. Power management support is provided through one or more of the hardware or software:

- A service processor configured for out-of-band communication
- Wake on LAN network interface card (NIC)
- Operating system

Support for system shutdown and restart in the power management task can be provided by the operating system running on Level-0, Level-1, and Level-2 managed systems.

### 6.1.2 IBM Director extensions

In addition to the three agent levels described above, there are extensions (also called subagents or plug-ins) that are available from IBM and third parties that further extend the capabilities of IBM Director. Some of these extensions are provided on the base IBM Director installation CD and are simply selected during installation.

<table>
<thead>
<tr>
<th>IBM Director base tasks</th>
<th>Page</th>
<th>Level-0</th>
<th>Level-1</th>
<th>Level-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Management</td>
<td>283</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Process Management</td>
<td>315</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Control</td>
<td>317</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Session</td>
<td>318</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Resource Monitors</td>
<td>318</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Scheduler</td>
<td>328</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server Configuration Manager</td>
<td>335</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP Browser</td>
<td>346</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Software Distribution</td>
<td>352</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>System Accounts</td>
<td>365</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Update Manager</td>
<td>411</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- a. Varies with application.
- b. Varies with operating system.
- c. See “Power management support”.
- d. Supported on System x servers.
- e. SNMP service/daemon must be installed and running on managed system.
installation. Others are available for download at no charge from the IBM Web site. Others are fee-based products that require a license.

The number of IBM Director extensions is likely to grow, but we present here those that were available at the time of this writing. See 1.5.2, “IBM Director Extensions” on page 14, for more detailed information about each of these extensions.

**Install-time extensions**
The following extensions are options during the installation:

- **BladeCenter Management**
  Provides tasks specific to managing IBM BladeCenter systems such as configuration profiles and management launch pads

- **Rack Manager**
  Enables IBM Director to display the managed environment in a graphic representation, including status and contextual menus for launching other tasks

**Free extensions**
There are a number of IBM Director extensions that can be downloaded from the Web at no additional cost. You can download the following free extensions from:


- **Hardware Management Console (HMC)**
  Provides an interface to the HMC for iSeries™ and pSeries® servers.

- **PowerExecutive**
  Enables monitoring and trending of actual power consumption by supported System x and BladeCenter servers. We describe this extension in detail in Chapter 9, “IBM PowerExecutive” on page 485.

- **ServeRAID Manager**
  Enables the remote management of IBM ServeRAID controllers as a task in the IBM Director environment.

- **System Availability**
  Provides a mechanism for tracking and charting system uptime and downtime, including planned and unplanned outages.

- **Virtualization Manager**
  Enables the monitoring and management of virtual machines running under various hypervisors from a single point of control. We describe this extension in detail in Chapter 10, “IBM Virtualization Manager” on page 513.
Fee-based extensions
The following extensions are fee-based. See 1.6, “IBM Director licensing” on page 20, or contact your IBM sales representative for additional information.

- Capacity Manager
  Provides proactive performance monitoring and bottleneck identification and resolution.

- Remote Deployment Manager
  Enables automated, remote system configuration and bare-metal OS deployments.

- Software Distribution Premium Edition
  Enhances the base Software Distribution task by enabling customer-created distribution packages.

- z/VM Center
  Specific for the virtual Linux server mainframe environment, provides a standardized way to deploy new z/VM virtual Linux systems using the IBM Director Console interface. We describe this extension in detail in Chapter 11, “IBM z/VM Center” on page 569.

Support for agent extensions by agent level
Table 6-2 lists the IBM Director Extensions that include an agent component and which agent levels support them.

<table>
<thead>
<tr>
<th>IBM Director Extension task</th>
<th>Level-0</th>
<th>Level-1</th>
<th>Level-2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacity Manager</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Hardware Management Console(^a)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Rack Manager</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>ServeRAID Manager</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>System Availability</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Virtualization Manager</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>z/VM Center</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

\(^a\) For use with iSeries and pSeries systems only
6.2 Tasks by operating system

Not all tasks are supported on all IBM Director Agents. Table 6-3 lists the tasks that require an agent (Level-0, Level-1, or Level-2), and the operating systems that are supported for each.

<table>
<thead>
<tr>
<th>Function</th>
<th>Windows</th>
<th>Linux</th>
<th>ESX Server</th>
<th>NetWare</th>
<th>AIX</th>
<th>i5/OS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base tasks</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset ID</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CIM Browser</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configure SNMP Agent</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Event Action Plans</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Event Log</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>File Transfer</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Hardware Status</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes^a</td>
</tr>
<tr>
<td>Inventory</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes^b</td>
<td>Yes^c</td>
<td>Yes^b</td>
</tr>
<tr>
<td>Microsoft Cluster Browser</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Process Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Control</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Remote Session</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Resource Monitors</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP Browser</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Software Distribution</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>System Accounts</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Update Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>IBM Director Extension tasks</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capacity Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Hardware Management Console</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Several tasks do not require an agent present on the managed system, since they communicate directly with the hardware (through a service processor) or simply do not need a mechanism to access an agent. This section describes these tasks and the requirements for each.

### BladeCenter Management support

The BladeCenter Management task talks to the service processor (BMC or RSA family adapter) at the physical platform level, so it does not matter which operating system is installed (or even if an operating system is installed).

### Electronic Service Agent support

The Electronic Service Agent extension is designed only for the management server and management consoles. There is no Electronic Service Agent component for the managed systems, since it receives all event data from Level-1 and Level-2 agents. Therefore, it is supported anywhere IBM Director Core Services or IBM Director Agent are installed.

### External Application Launch support

The External Application Launch task is supported by IBM Director Server when installed on x86-based management servers running Windows or Linux. Using External Application Launch, you can configure applications to start on any type of managed object that has been discovered by your installation of IBM Director Server. Before you use External Application Launch to configure an application...
to start on a managed object, you must make sure that the application runs on the selected managed object.

**PowerExecutive support**

PowerExecutive works with the Physical Platform Object (PPO). Therefore, it is not applicable to discuss agent level or operating system support for this task. PowerExecutive will work against any supported System x and BladeCenter server, regardless of operating system and agent level installed.

**Remote Deployment Manager support**

Remote Deployment Manager works with the PPO. Therefore, it is not applicable to discuss agent level or operating system support for this task. RDM can be used to deploy Windows, Linux, and VMware ESX Server operating systems. It does not support deployment of NetWare, AIX, or i5/OS.

**Server Configuration Manager support**

The Server Configuration Manager task talks to the service processor (BMC or RSA family adapter) at the physical platform level, so it does not matter which operating system is installed (or even if an operating system is installed).

### 6.3 Base tasks

Base tasks are the ones in the Tasks pane of the IBM Director Console after installing just the base IBM Director Console product. They are:

- Asset ID
- CIM Browser
- Configure SNMP Agent
- Event action plans
- Event Log
- External Application Launch
- File Transfer
- Hardware Status
- Inventory
- Microsoft Cluster Browser
- Network Configuration
- Process Management
- Remote Control
- Remote Session
- Resource Monitors
- Scheduler
- Server Configuration Manager
6.3.1 Asset ID

One of the most useful aspects of Asset ID is its ability to store important asset tracking information that cannot be found anywhere else in the system software. Examples include lease termination date, company asset number, department to which the system belongs, warranty expiration date, and various costs of supporting the system. This information includes:

- Serialization - serial numbering for system and associated components
- System - basic system information (name, OS, MAC address, and so on)
- User information - name, phone, location, department, position
- Lease - start, end, term (duration), amount, lessor
- Asset - purchase date, inventory date (physical), asset number
- Personalization - free form fields for data specific to customer environment
- Warranty - duration, cost, end date
To use this information, it first must be entered (Figure 6-1). The easiest solution to this challenge is to begin using Asset ID on all new systems that enter the environment. Over time, all systems will provide these important asset tracking data items. For existing systems, Asset ID supports mass configuration, so you can apply Asset ID values *en masse* to groups of systems. Mass Configuration is detailed further in 6.4, “Mass Configuration” on page 366.

![Figure 6-1 Asset ID](image)

**Note:** You cannot use any Asset ID data as event substitution variables for IBM Director events.

### 6.3.2 CIM Browser

The Common Information Model (CIM) Browser allows you to find in-depth information for problem determination. CIM is particularly useful on systems that do not have a management processor. For additional information about CIM visit:  

[http://www.dmtf.org/standards/cim](http://www.dmtf.org/standards/cim)
6.3.3 Configure SNMP Agent

Easily configure SNMP parameters such as community names and management IP addresses. See Figure 6-2. This task also supports mass configuration, further explained in 6.4, “Mass Configuration” on page 366.

![SNMP Configuration window](image)

**Figure 6-2**  SNMP Configuration window

6.3.4 Event action plans

The Event Action Plans task is not a task, rather it is a listing of existing event action plans (EAPs) that you can apply to managed objects, so the desired action occurs when a monitored event occurs on the managed object. EAPs can be applied to either individual objects or to entire groups with a single drag-and-drop action.

For information about creating event action plans see Chapter 12, “Event management” on page 675.

**Tip:** To see what EAPs have been applied, make sure that the Event Action Plans association is checked. In the main menu select **Associations** → **Event Action Plans**.
EAPs that have been applied to group objects do not appear when viewing the associations of individual objects. In Figure 6-3, note that group All Managed Objects has an EAP of Log All Events, while system Skagit only shows the Hardware Alert EAP, even though it is a member of the All Managed Objects group.

![Figure 6-3  EAP associations by group and individual objects](image)

6.3.5 Event Log

The Event Log task provides a collection of filters that you can apply against a managed object or groups. Using the Event Log enables you to display the filtered event log, displaying only the events that meet the filter criteria. For example, if you want to only view critical events on the Level-2 agents, drag and drop the Critical Events filter to the Level-2: IBM Director Agents group. This displays all critical events for that group.

**Note:** Only filters under Simple Event Filter in the Event Action Plan Builder are available options.

6.3.6 External Application Launch

The External Application Launch task provides a means for integrating third-party applications, scripts, and command-line commands into the IBM Director Console user interface. You can integrate external applications manually using a text editor or using the External Application Launch Wizard, if the wizard is installed on the management server.

**Important:** You must install IBM Director Server in the default location to use External Application Launch or the External Application Launch Wizard.

**Using the External Application Launch Wizard**

Installing the External Application Launch Wizard is a simple matter of running the installer on the management server. There are no questions to answer and no options to configure. In fact, the only choice to make is to accept the license agreement. Note that IBM Director Server services must be restarted after installation.
Once the wizard is installed on the management server, use the following procedure to create or modify an External Application Launch subtask using the wizard:

1. Open a command window on the management server.
2. At the command prompt, type the following command and press Enter:
   ```
ealwizard
   ```
   The External Application Launch Wizard opens.
3. In the Name panel, select an existing CMDTask file to modify, or create a new CMDTask file by selecting New and typing a file name, as illustrated in Figure 6-4. Click Next.

![Image of the Name panel of the External Application Launch wizard]

*Figure 6-4  Name panel of the External Application Launch wizard*
4. In the Icons panel, specify GIF files for the task icons to be displayed in IBM Director Console, as shown in Figure 6-5. You can specify a number of different icons, but only the Small Icon (16 pixels) and Large Icon (32 pixels) are being used with Version 5.20. The large icon is displayed in the Tasks pane only when the view is set to Large Icons or when the accessibility preferences are set to use extra large fonts. If no GIF files are specified, default icons are used. Click Next.

Note: The two Selected Icon choices, the Toolbar Icon, and the Rollover Icon choices, as shown in Figure 6-5, are not currently used.
5. In the Title panel, select a default or custom title that will be displayed in IBM Director Console from the Title Options menu.

Choosing the **Use Default Title** option uses the file name entered in the Name panel as the title displayed in the management console. No other information is needed in the Title panel if this option is selected, as shown in Figure 6-6.

Choosing the **Use Custom Title** option requires entry of title text strings for each of the eight languages supported by IBM Director.

**Note:** Only English is required. You will get a warning if you leave one or more blank, but you can still proceed to the next panel.
Choosing the **Provide Java Resource Bundle** option requires entry of the class name and title key of a Java resource bundle that defines national-language titles. For more information about the requirements of this option, see the IBM Director Information Center at:

http://publib.boulder.ibm.com/infocenter/eserver/v1r2/index.jsp?topic=/diricinfo_5.20/fqm0_main.html

Once you have made your selection and required entries, click **Next**.

6. In the Task panel, configure the characteristics of the subtask you are creating. First, select a task type from the Task Type menu. Options are Interactive console task, Noninteractive server task, or Both Interactive console and Noninteractive server tasks. Since we are interested in opening a Telnet session against a target managed system, we have chosen **Interactive console task**, as shown in Figure 6-7.

![Figure 6-7 Task panel of the External Application Launch wizard](image-url)
Next, use the arrow buttons to select the amount of time that IBM Director waits for the external application to successfully launch.

- Select the **Display a launch timeout warning** check box if you want IBM Director to return a warning when the External Application Launch subtask fails to launch within the time specified by the Launch Timeout field.

- Select the **File must exist to use this task** check box if you want to set a dependency on a specific file existing on the management console. If you select this check box, you must also identify the files that must exist in the File Dependency Settings fields.

Once you have made your selection and required entries, click **Next**.

7. In the Parent Task panel, select a parent task under which the external application task will appear in IBM Director Console, as shown in Figure 6-8. The External Application Launch Wizard supports one level of child tasks. Click **Next**.

![Figure 6-8 Parent Task panel of the External Application Launch wizard](image-url)
8. In the Targets panel, select how this External Application subtask will be launched. If the task can be targeted, select one or more appropriate managed-object types, clicking **Add** for each one to move them to the right side of this panel, as shown in Figure 6-9. Only managed-object types that can be legal targets for the external application should be selected. Click **Next**.

*Figure 6-9  Targets panel of the External Application Launch wizard*
9. In the Command panel, select the **Use a shell to run these commands** check box if the application requires an interactive dialog or advanced command-line syntax, such as wildcard expansion or special characters. Otherwise, leave this check box unselected. Our configuration is shown in Figure 6-10.

*Figure 6-10 Command panel of the External Application Launch wizard*

In the Command Configuration section, double-click the appropriate objects to enter commands and working directories.

When you specify a command, the System Attributes tab becomes available. From this tab, you can select system attributes for a command and provide additional system attributes. Click **Add** or **Remove** to change the Selected System Attributes list.

Once you are satisfied with the contents of this pane, click **Next**.
10. In the Summary panel, verify that all of the External Application Launch subtask criteria are correct, as shown in Figure 6-11. Click **Finish** to close the wizard and save the changes.

![Figure 6-11   Summary panel of the External Application Launch wizard](image)
11. In the message box that comes up (Figure 6-12), select **Yes** to restart the wizard to configure another External Application Launch subtask, or **No** if you are finished.

![External Application Launch Wizard Message](image)

*Figure 6-12  External Application Launch Wizard Message dialog box*

12. In the local management console, select **Tasks → External Application Launch → Refresh**. This step is required to update IBM Director Console to use the new or modified External Application Launch subtask. You should see the newly configured External Application Launch subtask in the management console, as shown in Figure 6-13.

![IBM Director Console](image)

*Figure 6-13  Newly created External Application Launch subtask in Tasks pane of management console*
13. Test the new subtask by dragging it onto a managed system (if it is targeted). The external application (in our case, Telnet) should launch, targeting the managed system, as shown in Figure 6-14.

![Telnet 192.168.0.11](image)

Figure 6-14  Telnet session launched against a managed system using External Application Launch

Although the External Application Launch Wizard is run on the management server and defines External Application Launch subtask resources on the management server, these subtasks are run on the management console from which the subtask is started. To start external applications from remote management consoles, you must perform additional configuration of the remote console system, as described in “Remote management console” on page 304.

**Manual subtask creation**

To manually create an External Application Launch subtask, you must create a CMDTask (command task) file in the Director\classes\extenstions directory. The defaults for these are:

- Linux: /opt/ibm/director/classes/extensions
- Windows: C:\Program Files\IBM\Director\classes\extensions

CMDTask files must have the extension .CMDExt (not case-sensitive), although the name of the file is not important. The tasks you create can either be run independently, or targeted against a specific system or group, depending upon the task.

There have been a number of enhancements to External Application Launch that can be accessed via manual subtask creation, including:

- Nested tasks and subtasks
- Additional task types
Chapter 6. IBM Director tasks

- Targeting multiple managed objects
- Additional system attributes
- Additional command-task parameters

External Application Launch is fully discussed in the “Managing External Applications” section of Chapter 4 in the *IBM Director Systems Management Guide*, which should be consulted before any attempt is made at creating a subtask manually.

We present here a very simple External Application Launch subtask that opens a Telnet session against a targeted managed system. Our CMDTask file is shown in Example 6-1.

**Example 6-1  Telnet.CMDExt file used by IBM Director to launch targeted Telnet session**

```plaintext
# Telnet.CMDExt
# Sat Dec 16 2006 @ 12:21:51 EST
#
# Properties file for command task to launch targeted telnet session
#---------------------------------------------------------------
# Small (16 point GIF) icon for console
#
Icon.Small=/CmdTask/Telnet/Images/telnet16.GIF
#
#---------------------------------------------------------------
# Command Launch Timeout - the number of seconds required for
# the specified command to launch.
Timeout=10
#
#---------------------------------------------------------------
# Should timeout warning be displayed if command launch fails?
#
TimeoutWarning=true
#
#---------------------------------------------------------------
# Is persistent shell required for interactive console task?
#
ShellRequired=true
#
#---------------------------------------------------------------
# CONSOLE COMMAND
#
# CommandString contains command that runs on any OS
# CommandString.[OS] contains command that targets specific OS
#
```

Chapter 6. IBM Director tasks  303
For the above External Application Launch subtask to work, the Telnet service (or daemon) must be running on the system targeted by the subtask. Also, you must place an icon file in the directory specified. If this is not done, the default External Application Launch icon is used instead.

**Remote management console**

External Application Launch subtasks are initially created only on the management server. Additional preparation is required to start External Application Launch subtasks using remote instances of IBM Director Console.

To configure a remote instance of IBM Director Console to start an External Application Launch subtask, do the following:

1. Copy the task icon files from the management server to the remote management console system. For the External Application Launch subtask icons to be displayed on the remote instance of IBM Director Console, the GIF files used to define the icons must be present on the management console system with the same path and file names as are used on the management server.

2. Ensure that the application to be started by the External Application Launch subtask, as well as any resources required by the application, is present on the target system. If necessary, install the application on the remote console system. The path and file name for the application that is installed on the management console system must be the same as the path and file name on the management server, as specified in the CMDExt file associated with the External Application Launch subtask.
Helpful tricks

In working with the new capabilities of External Application Launch and the EAL Wizard, we came across a couple of tricks we think might be useful to anyone who intends to create External Application Launch subtasks. Figure 6-15 shows our final External Application Launch hierarchy.

![Figure 6-15](image)

Notice that we chose to place two subtasks under a Communication Tasks item to help organize our new subtasks. Also, since we launched the EAL Wizard many times to create the items documented here, it eventually occurred to us that we could create an External Application Launch subtask that launches the EAL Wizard itself.

In this section we describe how to create a parent task and how to create an External Application Launch subtask that launches the EAL Wizard.
**External Application Launch hierarchy**

Creating a parent task to contain related subtasks is easy using the EAL Wizard. Simply step through each pane in the wizard, specifying options as normal. However, for the following panes, specify the options shown:

- Task pane: Select **Interactive console task**. Leave all other options at default.
- Targets pane: Select **Untargeted**.
- Command pane: Do not specify any commands. Just click **Next** to continue.

Review the summary information and click **Finish** to save the new parent task. The summary pane includes information that indicates that the new task is a parent task and will not actually perform any other function, as shown in Figure 6-16.

![Figure 6-16  EAL Wizard summary showing that the new task is a parent task](image)

**EAL Wizard task**

If you intend to use the EAL Wizard on a regular basis, you might consider creating an External Application Launch subtask to launch the wizard quickly on the management server. This is easily accomplished by stepping through the EAL Wizard, specifying options as normal. However, for the following panes, specify the options shown:

- Task pane: Select **Interactive console task**. Leave all other options at default.
- Targets pane: Select **Untargeted**.
- Command pane: Specify **ealwizard** as the command for either Windows or Linux, depending on the operating system of your management server.

Review the summary information and click **Finish** to save the new parent task. Note that this task will only work properly from a local management console (that is, from a console running on the server), since the EAL Wizard runs only on IBM Director Server.
**DIRCLI command**

A new IBM Director command-line command has been added to update External Application Launch tasks. When you right-click the External Application Launch task in the management console and select Refresh, this new command is run. You can also run the command as any DIRCLI command from the command line on the management server, as follows:

```shell
dircli refreshcmdexts
```

This command can be useful if creating CMDExt files manually. Once your CMDExt file has been saved, issue the `refreshcmdexts` command to update External Application Launch tasks displayed in the management console.

### 6.3.7 File Transfer

File Transfer provides a simple method for point-to-point file transfers, including file transfers between platforms. The following transfers are possible:

- Console to managed system
- Server to managed system
- Console to server

**Tip:** Software Distribution Premium Edition can be used to distribute files in addition to applications. The File Transfer task is limited to a point-to-point transfer, but Software Distribution PE can be used to distribute files to groups.
6.3.8 Hardware Status

The Hardware Status task can be applied to individual objects or to groups to view the status. Systems can have multiple errors of differing severities. However, the Hardware Status only categorizes them according to the most severe error, but displays errors of all severities. Figure 6-17 shows the Hardware Status task applied against all Level-2 systems. Notice that KIDD-VM is categorized as critical, but has both a warning and a critical error.

![Figure 6-17  Hardware Status of all Level-2 Agent systems](image)

For details on event severity associations, consult the *IBM Director Events Reference* publication.
You can also specify IBM Director to ignore certain hardware events. An example of this is where a system has multiple NICs, but they are not all in use. Using the example in Figure 6-17, the second NIC is not required. We have two choices. We can ignore this alert by right-clicking the Network Interface Card, then clicking **Ignore Events**. This greys out the bang icon, indicating that the event is being ignored. Future events will be logged and ignored. Figure 6-18 shows the Hardware Status with the NIC offline error ignored.

Selecting **Clear Events** clears the event and removes the alert completely from that group.

![Hardware Status](image)

*Figure 6-18  Hardware Status with error ignored*

The Hardware Status can also be launched from the Hardware Status dashboard in the lower right corner of IBM Director Console. There must be at least one system with either an informational, warning, or critical error for the dashboard to be present. Clicking any of the active alert icons launches the Hardware Status task against all Level-2 agents. Figure 6-19 shows the dashboard with active alerts, and an ignored alert.

![Hardware Status dashboard](image)

*Figure 6-19  Hardware Status dashboard showing active alerts, before and after ignoring the warning alert*
IBM Director 5.10 introduces additional subtasks under the inventory task. In previous versions, the Inventory task simply launched the inventory browser against the object or group. Expanding the Inventory task in IBM Director 5.10 shows three new tasks:

- **Collect Inventory** performs a collection on an object or group. Inventory data collected with this task is specified in the Inventory Collection tab of the server preferences.

- **Custom Collections** allows you to specify a subset of inventory items for which to collect data. This enables you to run collections that take much less time and have a much lower impact to the network.

For example, if your default collection is hardware only, but you wanted to gather installed software information, you could create a task that will only collect software information about the system or group on which it has been applied.
Figure 6-21 shows a custom collection task that will only collect software data. With the Post Collection Actions, you are able to generate an event on success or failure, which can be added to an EAP to notify you of the status.

![Image of a custom collection task window]

Figure 6-21   Inventory Custom Collection task for software only

- **Inventory Monitors** allows you to monitor for a change in inventory data, both hardware and software, and generate an event when a change is noted. For example, you can monitor the installed memory, and have an event generated when it changes.

The first step is to create the monitor:

a. Right-click **Inventory Monitor** and click **Create**.

b. Give the monitor a name. For our example, we used *Memory change*.
c. Expand **Available Queries** and select the items that you want to monitor. Use the Ctrl key to select multiple items, and click **Add**. For our example we selected **Hardware → Memory → Installed Memory → Changed**, as seen in Figure 6-22.

d. Click **OK** to save the monitor under the Inventory Monitors task.

![Figure 6-22 Inventory monitor for a change in installed memory](image)

The next step is to apply the monitor to systems or groups:

a. Drag and drop the new Inventory Monitor task to the applicable systems/groups.
b. A window similar to Figure 6-23 appears showing the association that will be applied.

c. Click **OK** to save the monitor association. You can verify that it is successful by right-clicking **Inventory Monitors** and clicking **View Applied Inventory Monitors**.

![Applied Inventory Monitors](image)

*Figure 6-23   Applied Inventory monitors*

**Note:** Even though the monitor is applied, a change will not be noted until the next inventory collection takes place. For example, if Inventory Collection runs on Saturdays and a change occurred on Monday, an event would not be generated until the next Saturday. To address this, we recommend that you schedule custom inventory collection tasks to run more frequently on monitored items.
Finally, you must apply an event action plan if you want to be alerted to the change. Without an EAP, the event will be generated, but nothing else will occur. For our example, we configured a console pop-up window to alert that a change in installed memory has occurred, as shown in Figure 6-24.

![Console pop-up alerting to memory change](image)

**Figure 6-24** Console pop-up alerting to memory change

### 6.3.10 Microsoft Cluster Browser

The Microsoft Cluster Browser enables you to browse the resource/node association within a Microsoft Cluster Server (MSCS) cluster. Because this is a browser, you cannot configure or change any settings.

### 6.3.11 Network Configuration

The Network Configuration task allows you to view and edit the following Ethernet network settings for:

- IP addresses
- DNS settings
- WINS settings
- Windows workgroup/domain settings
- Modem, if installed

This task also supports mass configuration, further explained in 6.4, “Mass Configuration” on page 366.
6.3.12 Process Management

Another powerful feature of IBM Director is its ability to manage and monitor system processes. In addition to viewing what processes are currently running on the system, you can start and stop processes, as well as monitor for state change (start, stop, fail).

When a state change on a monitored process occurs, this can generate an event, which in turn can activate an event action plan such as send an e-mail, a page, or even restart the process.

To view the currently running processes, drag and drop the Process Management task onto the managed object.

From the Process Management window (Figure 6-25) you can:

- View and stop current running processes.
- Add a process to Process Monitors.
- View and change the state (start, stop, restart, pause, continue) of services (Windows only).
- View and change the state (start, stop) of device services (Windows only).
- Add a Service Monitor Threshold to generate an event should a service change to specified state.

![Process Management: Rainier](image)

Figure 6-25 Process Management
Process Monitors

Even though you can establish a process monitor from the process management window, it does not provide an option of what particular state (start, stop, fail) for which you want to monitor. To specify what state you want events generated on, you need to specify this in the Process Monitor window.

There are two methods to open the Process Monitors window:

- Click Monitors in the Process Management window.
- Apply the Process Monitors task to the managed Level-2 system.

In the Process Monitors window, check which state you want to monitor for, and the appropriate time out if monitoring for failures. Figure 6-26 shows two process monitors: one for winlogon to stop or fail, and one for Solitaire to start. If any of these occur, an event will be generated, so alerting can occur.

![Process Monitors](image)

*Figure 6-26  Process Monitors*

After process monitors have been configured, they can be used to create a Process Monitor child task. To do this, click **File → Create Task**. Provide an appropriate name and click **OK**. You now have a task under Process Monitors that you use to configure the same process monitors on additional systems.

**Tip:** The Process Monitor subtask can only be applied to individual systems, but a child subtasks can be applied to groups.

Process Tasks

Process Tasks are commands that can be executed against managed systems. These tasks can either be applied manually by drag and drop, or can be incorporated to an event action plan. To create a Process Task, right-click **Process Tasks** and click **Create**. Enter the task, along with a login if it needs to run under the specified account.
Figure 6-27 shows a task to start the print spooler on a Windows machine.

![Process Task to start Windows print spooler](image)

### 6.3.13 Remote Control

Remote Control is a feature in IBM Director that enables a software-based remote console on the managed system. This task is quite beneficial in help desk environments to aid in problem determination and end-user assistance, without the need for in-person support.

It is not intended as a replacement for products such as terminal services/remote desktop, because it does not provide the same level of performance and security. For situations requiring a robust remote working environment, the use of alternate products is recommended.

There are three modes for Remote Control:

- **Active**: You have control of the system.
- **Monitor**: User has control of the system, but you can see the console activity.
- **Suspend**: The remote control session is still active, but no control is active, and the window does not refresh.

Remote control sessions can also be recorded and replayed to assist with training on specific tasks. To record a remote control session:

1. Drag and drop Remote Control on a system, and either click the red dot icon or select **File → Start Session Logging**. You are prompted for a unique name for the recorded file.
2. When you are finished recording, click the blue square icon or select **File → Stop Session Logging**.

3. To view the recording, expand the Remote Control task, and look for an entry with the name you gave you recording.

4. To replay the recorded session, either right-click the recording and select **Open**, or double-click it. When the window opens, click **Actions → Play**.

**Tip:** If you use Remote Control to a Windows system and you only see a black window, it is possible that you have previously used Windows Terminal Services or Remote Desktop Connection to connect to the system, and the Session 0 is still running. Reset the session and try Remote Control again. See the following for details about resetting terminal sessions:

http://www.microsoft.com/technet/prodtechnol/windowsserver2003/library/ServerHelp/fe39192e-0cb5-47da-9e00-26d864e51b0d.mspx

### 6.3.14 Remote Session

The Remote Session task provides a command-line interface to the managed system.

- On Windows system it is a command-prompt.
- On UNIX and Linux systems SSH is the default, but Telnet will be used if SSH is unavailable.

### 6.3.15 Resource Monitors

Monitoring resource utilization is a critical function in today's IT environment where the business pressures to provide higher levels of service with fewer resources is the reality.

To address this, IBM Director provides a vast array of resource monitors, which include a variety monitors on all major subsystems (CPU, memory, storage, and network), processes (differs from Process Management Process Monitors subtask), and even file systems.

On Windows systems there are additional monitors for registry, performance, device, and service monitors.

Resource monitors and thresholds are configured into the agent. The server does not continuously poll the system for this information. When a threshold is passed, the agent generates an event to the IBM Director server for alerting actions. This eliminates unnecessary traffic in the network, but provides comprehensive monitoring.
As with many IBM Director tasks, Resource Monitors can be applied to single systems or entire groups, easing the effort to administer larger environments.

**Note:** When the threshold is passed, an event is sent to IBM Director Server. You must create and apply an event action plan, as described in Chapter 12, “Event management” on page 675, in order to process the event.

**Examples**
For the purpose of this book we provide a few common examples of how resource monitors can be used to assist in providing higher levels of performance and reliability.

**CPU Monitoring**
Recent trends in consolidation have significantly increased the average utilization of Intel systems, and this trend is expected to continue. In the past, you could increase the workload on a system without significant impact to performance, because the system was only running an average of 10% CPU utilization. Today, with systems averaging over 40 or 50%, increasing workloads can easily drive utilization to the point of negative impact on performance.

By monitoring and alerting on CPU utilization, you can assure that acceptable performance levels are maintained.

Before creating any resource monitor, some planning significantly eases the process. For CPUs, there are two things that should be considered:

- **Typical utilization**
  
  What is the typical utilization you see on this system? Chances are that a database server works the CPU a lot harder that a file/print server. What is considered normal? What would you like to be warned about and what do you consider critical?

- **Peak duration**
  
  CPU utilization often spikes, but how long is high utilization considered normal? Consider a mail server utilization on Monday morning, as compared to Wednesday afternoon. Chances are that a spike will last longer on Monday morning.

To create a CPU utilization monitor, follow these steps:

1. Drag and drop the **Resource Monitors** task on the system or group you want to monitor.
2. Expand the managed system in the Available Resources pane.
3. Expand the CPU Monitors item.
4. Drag and drop **CPU Utilization** to the Selected Resources pane. IBM Director issues a query to the agent for the current CPU utilization, as seen in Figure 6-28.

![Figure 6-28 CPU Resource Monitor](image)

This only provides us with current utilization, so the next step is to set the monitor thresholds.

5. Right-click the cell with the utilization, and select **Individual Threshold**, opening the System Threshold window.

6. Provide a name and description (optional).

7. Ensure that “Enabled to generate events” is checked (default), but that “Generate events on value change” is not. In the case of a CPU monitor, this would generate many useless events.

   *Maximum queued events* is the number of events that will be held if the management server is offline. These events will be forwarded when the server can be contacted again.

8. Next, set the minimum duration of the threshold breach. You can choose a timing of seconds, minutes, hours, or days. The default of 5 minutes is probably too short because CPU usage fluctuates. For this example, we use 3 hours.

9. The **Resend Delay** is the period of time that must pass before a subsequent event is generated. The default of 0 disables this. In the case of our CPU monitor, if it exceeded 50% for 3 hours and 1 minute, an event would be
generated, but if it remained above 50% for the next 3 hours, no additional event would be generated.

If at 3 hours and 2 minutes it dropped to 35% utilization, the threshold breach is cleared, and the minimum duration clock would be reset. If at 3 hours and 3 minutes usage jumped back above 50%, it would take another 3 hours before an alert would be generated.

10. Now set the actual threshold settings that determine when an event will be generated. IBM Director provides you with the ability to have high and low thresholds with both warning and critical levels. For our CPU example, we use the high thresholds with 50% a warning and 75% a critical event.
Our completed system threshold is shown in Figure 6-29.

![CPU Monitor Threshold Settings](image)

**Figure 6-29** CPU monitor threshold settings

### Storage Monitoring

What happens when the mail server runs out of disk space? The best case scenario is that some mail might be lost. The worst case scenario might require significant effort to re-establish the service.

Simply creating a monitor on the disk utilization and alerting when the thresholds are reached can save an IT administrator time and help ensure service levels.
Again, some aspects need to be considered prior to configuring the monitor, such as what will you monitor? Percentage used? Percentage available? MB available? It is also important to know the typical consumption rate. If we consume 1 GB per day, our space goes from warning to critical much faster, and quite possibly does not permit enough time to respond to the warning.

To establish a storage monitor, the process is the same as what we did for the CPU monitor.

Disk utilization monitors have items in addition to percentage used—there is also workload (bytes/second), space remaining, and space used (both in MB). As an example of the low thresholds, we use the Space Remaining monitor.

Knowing that our disk is 6 GB in size, we can determine where we want a warning event and a critical event to be generated. For this example, we use 25% (1.5 GB free) as the warning level, and 10% (600 MB) as critical.

Following the same process as the CPU above, expand the Disk Monitors in the Resource Monitor window, then add the Space Remaining monitor to the Selected Resources window.

Right-click the cell with the utilization and select Individual Threshold, opening the System Threshold window.
Complete the fields with the appropriate information. Note in this example that we are using the low thresholds. Because disk space is not likely to fluctuate as much as a CPU utilization, the duration can be considerably shorter. Depending on the criticality of the system, you might want to have frequent resends of the event. Figure 6-30 shows our completed threshold settings.

![System Threshold: Kananskis](image)

**Figure 6-30  Disk monitor for space remaining in MB**

### File Monitoring

Do you have critical files that must exist for an application to run properly? Do you need to monitor directories for modifications such as new files being written to them?

IBM Director can provide an easy method to monitor these items and alert you to changes.
The following attributes can be monitored for both directories and files:

- Existence
- Last modification date

Files have the following additional attributes:

- Checksum
- File size (bytes)

1. To establish file monitors, launch the Resource Monitors task and expand the File Monitors item.

2. Expand the tree until you find the directory or files that you want to monitor.

3. As with the previous examples, drag the required monitors to the Selected Resources pane, and the server will query the agent for the current information.
4. To set the thresholds, right-click the monitor, and the System Threshold windows opens. Depending upon what monitor you selected, it might be slightly different from the other monitors. For example, we have selected to monitor important File.txt for existence. This is simply true or false, as indicated in Figure 6-32.

5. We provide a name and description, change the minimum duration from 5 minutes to 1 second, and change the False string to an Error from normal. This generates a critical event when the file is deleted or renamed.

**Process Monitors**

The final example we provide is for process monitoring. This is different from simply monitoring a process for state change, as with Process Management.
When a process monitor has been set up and applied to a system through the Process Management task (Figure 6-33), you are able to monitor it using Resource Monitors as well. Instead of state, you can monitor for the following information:

- Current active processes
- Maximum running at once
- Maximum running yesterday
- New executions counted
- Times failed to start
- Times started
- Times stopped
- Total execution time
- Yesterday's execution time
- Yesterday's new executions

Because these monitors are numerics, the thresholds are the same as what is available for CPU and disk with high errors and warnings, and low errors and warnings.

In this example we establish a monitor on the total execution time for solitaire. As with previous examples, right-click in the resource cell and select Individual Thresholds to open the System Thresholds window.
Figure 6-34 shows our completed thresholds for this monitor. The agent will generate a warning event when the execution time reaches 60 minutes, and a critical event at 75 minutes. Because we are already measuring a period of time, the duration has been set to seconds to speed up the event generation.

![Figure 6-34 Thresholdds on Solitaire's total execution time](image)

6.3.16 Scheduler

The scheduler enables you to execute noninteractive tasks at a future date and time using a calendar-based scheduler. Tasks can be set up as run-once or repeating jobs.
For example, the IBM Director performs an inventory collection upon discovery of the system, but by default it does not collect software inventory. If you enable the software collection in the server preferences, IBM Director performs a software collection on all systems.

There might be only a few systems for which you want to have software inventory information. This can be accomplished by creating a Custom Collection task in the Inventory task to only collect software information, then schedule this to take place during off hours.

To schedule a task, click in the main Console window, or right-click the Scheduler task and click Open. In the Scheduler window (Figure 6-35) you can view by month, week, day, or job. For this example we use week, because our job will run on a weekly basis.

![Scheduler - weekly view](image)

*Figure 6-35  Scheduler - weekly view*
Create a new task by using the following steps:

1. Right-click the day you want the job to run, and click **New Job**. Because we already selected the day, we need to adjust the time. For this example, we use 3:00AM. See Figure 6-36.

![New Scheduled Job](image)

**Figure 6-36  Date and time of scheduled task**

2. We want this task to repeat, so click the **Repeat** button. Repeating jobs have many options. The Repeat frequency choices are:
   - **Once**, not really a repeat.
   - **Hourly** can be every hour, every second hour, every third hour, up to every 24th hour.
   - **Daily** can be every day, every second day, every third day, up to every 31st day.
   - **Weekly** can be every week, every second week, every third week, up to every 8th week.
   - **Monthly** (days and dates) can be every month, second month, third month, up to 12th month. Additionally, you can also specify days like the 1st Monday, or the last Friday, or specific dates like the 15th.
   - **Yearly** can be every year, every second year, every third year, up to every 10th year.
– *Custom* allows you to set random dates for the job to run.

3. Set the duration a scheduled job will be in effect. Simply specify a date and time for it to end, the length of time the schedule remains active (in hours, days, months, or years), or even to have it effective forever.

For the purpose of our example, we selected for the job to run weekly, every week, on Friday, forever, and clicked **OK**.

4. Click the **Task** tab, and select the tasks that you want to run (Figure 6-37).

![New Scheduled Job](image)

*Figure 6-37*  Tasks that comprise the scheduled job
5. Click the **Targets** tab, and add which systems or groups this job will run against. See Figure 6-38.

![New Scheduled Job](image)

**Figure 6-38** Systems the job is scheduled to run against

6. The Options tab allows you to specify additional options for the job. These include:
   - **Special Execution Options**
     - Delay execution on unavailable systems: If the systems are offline when the job runs, it executes on systems when they become available.
     - Execute on systems that are added to the target group: The job will be executed on new systems when they are added to the group.
     - Execute in the client time zone: The job will run based on the agent time zone, not the server’s time zone.
– Execution History

The scheduled tasks execution history is logged in the Scheduler. This section allows you to configure the parameters of how many entries, and how long they are maintained.

– Events

Scheduled jobs can generate events when certain criteria are met. These events can then be utilized to generate actions such as e-mail notifications. Events can be generated when:

• Job successfully completes.
• Job completes with errors.
• Job successfully completes on target system (will generate multiple events if job is applied to a group or multiple systems.)
• Job completes with errors on target system (will generate multiple events if job is applied to a group or multiple systems.)
Figure 6-39 has events generated if the job has errors on target systems.

Figure 6-39 Additional options for scheduled jobs
When all of the details have been completed, click **File → Save As** and provide the job with a unique, descriptive name. When the job is saved, we can confirm it by viewing the Scheduler calendar. We see the job scheduled every Friday at 3:00 a.m. (Figure 6-40).

![Scheduler Calendar](image)

**Figure 6-40  Software inventory job scheduled every Friday at 3:00 a.m.**

### 6.3.17 Server Configuration Manager

The Server Configuration Manager task is used to create and edit profiles that configure service processors in IBM System x servers. You can create profiles that configure the following parameters with this tool:

- Enable DHCP or static IP addressing.
- Specify a single IP address or a range of IP addresses.
- User account login credentials.
Implementing IBM Director 5.20, server configuration profiles can be created by reading an existing service processor configuration. Figure 6-41 shows the Quick Start window displaying this new option. To see this window, perform a targeted launch of Server Configuration Manager against the service processor (that is, a physical platform object) whose configuration you want to read. If you perform an untargeted launch of Server Configuration Manager, you will not see the option to read current hardware configuration.

![Figure 6-41  Server Configuration Manager Quick Start window](image)

Whether profiles are created manually or by reading the current configuration of a service processor, they can be edited, saved, and applied to a system or a group of systems.
Profiles are made up of components. Server Configuration Manager currently supports four components, which are seen in Figure 6-42. They are:

- IP Address Pool
- Service Processor Alerts Configuration
- Service Processor Login Profile
- Service Processor Network Configuration

![Figure 6-42  Server Configuration Manager Select components window](image)

To create a profile to configure one or more of these components, simply select the components to be configured and click **OK**. Each of the Server Configuration Manager components are detailed here. A profile can contain any or all of these components. After you create a profile, you can apply it to one or more service processors by a simple drag-and-drop action.
IP Address Pool

The *IP Address Pool* component allows configuration of TCP/IP settings, including gateway, subnet mask, and IP address pool. You can add single IP addresses to the pool or establish a range of addresses from which service processors will draw. This component is highlighted in Figure 6-43.

![Figure 6-43  IP Address Pool component of Server Configuration Manager](image)
Service Processor Alerts Configuration

The Service Processor Alerts Configuration component allows configuration of alerting from the service processor. The Alert Recipients tab is used to create a new alert recipient, as well as modify existing recipient profiles. This component is highlighted in Figure 6-44.

Figure 6-44  Service Processor Alerts component, Alert Recipients tab of Server Configuration Manager
When a profile containing this component is applied to a service processor, remote alert recipients are configured immediately. Figure 6-45 shows a browser view of an RSA II service processor after the profile from Figure 6-44 on page 339 is applied. Notice that both remote alert recipients were added to the proper positions (6 and 8), as specified in the profile.

![Browser view of RSA II adapter with Server Configuration Manager profile applied](image-url)
The Alert Configuration tab of the Service Processor Alerts Configuration component allows configuration of service processor alert generation. You can enable or disable alert forwarding, manage global remote alert settings, and specify which types of alerts are forwarded to remote alert recipients. This component is highlighted in Figure 6-46.

![Service Processor Alerts Configuration](image)

**Figure 6-46  Service Processor Alerts component, Alert Configuration tab of Server Configuration Manager**
Service Processor Login Profile

The Service Processor Login Profile component allows configuration of user profiles for the service processor's embedded account list. You can create new accounts, modify existing credentials and access rights, and delete existing accounts. This component is highlighted in Figure 6-47.

The RSA II supports up to 12 user accounts, while the BMC only supports three (four if you count the null user ID, which you cannot change). You are not allowed to add more than 12 user accounts using this component. If you apply a profile containing more than three user accounts to a BMC, only the first three will be applied, but only if there are three empty slots available on the BMC. You cannot overwrite slots that are already occupied on the BMC using Server Configuration Manager.
When a Server Configuration Manager profile containing this component is applied to a service processor, login profiles stored on the service processor are configured and saved immediately. Figure 6-48 shows a browser view of an RSA II service processor after the profile from Figure 6-47 on page 342 is applied. Notice that the three new login accounts are added at the end of the list, beginning at position 12.

Figure 6-48  Browser view of RSA II adapter with Server Configuration Manager login profile applied
Service Processor Network Configuration

The Service Processor Network Configuration component allows configuration of the network interface on the service processor. You can set IP addressing to DHCP or static, as well as configure SNMP properties. This component is highlighted in Figure 6-49.

![Service Processor Network Configuration component of Server Configuration Manager](image)

*Indicates Required Fields.*

Figure 6-49  Service Processor Network Configuration component of Server Configuration Manager
Applying a profile

You apply a Server Configuration Manager profile to a service processor just as any Scheduler job. This means that you can check details of the job status during execution, as well as verify successful completion of the job. Figure 6-50 shows the execution history window for the profile we applied to an RSA II service processor for the previous examples.

Figure 6-50  Execution history of a profile applied to an RSA II service processor
Assigning a profile automatically

Server Configuration Manager also allows you to select a profile that will be automatically applied to any service processor that is discovered or added to IBM Director Console. This feature is called Detect & Deploy.

To select a profile to be used automatically for any new service processors, follow these steps:

1. Open the profile that you want to use by right-clicking it in the Tasks pane of IBM Director Console, and click Edit.
2. Click Server from the navigation tree to select the entire profile.
3. Select Actions → Detect & Deploy from the menu bar. This adds a check mark next to the menu item.
4. Click File → Save Profile to save the change.

The results of any Detect & Deploy actions are recorded in the event log of the service processor, accessible using the Event Log task against that object.

Important: Even though you can configure multiple profiles to have Detect & Deploy set, the Configuration Manager only supports one Detect & Deploy profile for service processors (via the Server Configuration Manager) and one Detect & Deploy profile for BladeCenter chassis (via the BladeCenter Configuration Manager). If you define more than one Detect & Deploy profile, the last profile you configured is the one that will be executed. All others will be ignored. Also, if you do have multiple Detect & Deploy profiles, there is no way to tell after the fact which one will be used.

6.3.18 SNMP Browser

Some consider SNMP and its dotted decimal presentation of object identifiers (OIDs) and traps to be the enigma of systems management because of the
configuration difficulties they present. This section is not an SNMP tutorial, but we do make a few suggestions to help you get the most out of what is likely the most widely used industry standard in systems management. The IBM Director interface into SNMP is the SNMP Browser.

The SNMP Browser is used to browse and configure the attributes of SNMP devices, for example, hubs, routers, or other SNMP-compliant management devices. You can use the SNMP Browser for SNMP-based management, troubleshooting, or monitoring the performance of SNMP devices.

If you have ever opened the SNMP Browser against a managed system running the SNMP service, you probably saw something similar to Figure 6-52. When you have clicked to expand the browser tree often enough to finally reach the end of the line, the information presented hardly seems worth the effort.

![SNMP Browser: Chicago-RSA](image)

**Figure 6-52  SNMP browser showing dotted decimal representation of management data**

It is easy to determine that *something* is at 86% of maximum, but unless you happen to know what 1.3.6.1.4.1.2.3.51.1.2.3.4 means, you cannot be sure whether you need to archive files to free up space on a hard drive or consider purchasing an additional processor for this system.
Now look at Figure 6-53. This is exactly the same view of the SNMP browser targeting the same managed system (actually, a Remote Supervisor Adapter) as in Figure 6-52 on page 347. This time, we see very specific information about the managed device. The selected item is `fan4speed`, which is much more understandable than 1.3.6.1.4.1.2.3.51.1.2.3.4.

In fact, the entire SNMP tree is much more understandable. We quickly and easily recognize specific parameters that are of interest, and the Details pane provides additional information about the parameter selected.

All we have to do to make the SNMP browser more useful is to integrate the appropriate Management Information Base (MIB) file into IBM Director and load it into memory. In IBM Director 5.10, this requires two steps for the SNMP dotted
decimal notation to be translated into the more readable format seen in Figure 6-53 on page 348:

1. Compile the MIB.
2. Load the MIB into memory on the management server.

The MIB file is used to translate the raw SNMP dotted decimal notation into readable text. This is especially useful for SNMP devices that do not have IBM Director Agent installed, such as network hubs, routers, switches, printers, and UPSes.

In addition, SNMP can be an excellent way to manage systems, especially non-IBM systems, onto which you would rather not install IBM Director Agent. An example might be an HP server that already has the HP Systems Insight Manager agents installed. You might want to manage this system through SNMP, rather than buying a license to install IBM Director Agent on such a system. There is no license fee associated with managing devices with SNMP.

**Managing MIBs**

IBM Director Server installs with several MIB files located in the Director\proddata\snmp directory.

The SNMPServer.properties file located in the Director\data\snmp directory can be set to automatically recompile any MIBs placed in the Director\proddata\snmp directory each time IBM Director Server service is restarted. To enable this function, open SNMPServer.properties and change the following line to true:

```plaintext
snmp.recompileOnStartup=true
```

In previous versions of IBM Director, the order of MIB compilation was often critical for a given set of MIBs. However, the current release seeks out MIB dependencies, then compiles and loads them in the proper order. Of course, if a prerequisite MIB is missing (not in the Director\proddata\snmp directory), then compilation of the dependent MIB fails.

For a MIB to do its job and be useful in the SNMP and Event Log tasks, it must be compiled and loaded into management server memory. In previous versions of IBM Director, all compiled MIBs were loaded into memory automatically. This included all MIB files in the Director\proddata\snmp directory, if the auto-recompile function was enabled.

However, having many MIBs loaded uses up management server resources. In order to reduce the impact of this situation, IBM Director 5.10 separates the compile process from the memory load process. As before, when you compile a MIB file in IBM Director, its mibdata file is loaded into memory automatically. However, you can now choose to unload compiled mibdata files from memory.
The loadedmibs.dat file located in the Director\data\snmp\ directory contains the list of mibdata files most recently requested to be loaded. This is persistent data. The most recent list of loaded mibdata files is stored with each change and reloaded when the management server is restarted. If a mibdata file that has been compiled elsewhere (for example, on another IBM Director Server) is copied into the Director\data\snmp directory, it will not be loaded into memory, nor will it be added to the loadmibs.dat file.

The bottom line is that you can have as many compiled MIBs stored on your management server as you want without impacting performance. It is now possible to load any set of mibdata files into memory when you need them, then unload them when you are finished with them.

Compiling MIBs

Compiling a MIB file creates a binary data file named <MIB definition name>.mibdata in the Director\data\snmp directory. The process of manually compiling a MIB file for IBM Director is as follows:

1. In the IBM Director Console window, click Tasks → SNMP Browser → Manage MIBs.
2. In the MIB Management window, click File → Select MIB to Compile.
3. In the Select MIB to Compile window (Figure 6-54), specify the directory and file name of the MIB file that you want to compile, then click OK.

![Select MIB to Compile window with VMware Root MIB selected](image-url)
4. You are returned to the MIB Management window, as shown in Figure 6-55. This window provides status information while the MIB compiles and lists any errors encountered in compiling the MIB file.

![MIB Management window](image)

*Figure 6-55  MIB Management window shows status of MIB compilation and any errors if they occur*

5. After the MIB compilation completes, close the window and return to the SNMP Browser to see more human-readable information for the device you have compiled.

**Loading MIBs into memory**

As discussed in the previous section, it is now possible to reduce memory utilization on the management server by loading only required mibdata files into memory, while unloading all others. To load or unload mibdata files into management server memory manually, follow these steps:

**Tip:** When you compile a MIB, it is automatically loaded into memory, so you do not have to load it manually using these instructions.

1. On the IBM Director Console window, click **Tasks → SNMP Browser → Manage MIBs.**

2. In the MIB Management window, click **File → Select MIB to Load.**
3. In the Load MIBs window (Figure 6-56), select the MIBs you want to load from the Available MIBs column. Move them to the Loaded MIBs column by double-clicking individual items or by using Shift+click or Ctrl+click to select multiple items, then clicking **Add**.

4. When you are finished adding MIBs to load, click **OK**.

![Figure 6-56   Selecting which MIBs to load into management server memory](image)

Any changes made in the Load MIBs window are written to a binary file loadedmibs.dat and stored as persistent data on the management server. Each time the management server is subsequently restarted, it reloads into memory all MIB data files that were most recently specified.

### 6.3.19 Software Distribution (base)

Beginning with IBM Director 5.20, the Update Manager task provides significant functionality that works in conjunction with software distribution to provide a robust system update toolset for IBM System x and BladeCenter products. See for Chapter 7, “Update Manager” on page 411, more information.
The Software Distribution task that is included with the base installation of IBM Director is limited to distribution of IBM supplied packages. These packages can be found on:

- UpdateXpress CD
- IBM Director installation CD
- Web downloads of IBM system BIOS, firmware, and drivers

For Web downloads, look for the presence of an XML file.

The Software Distribution task has changed with the introduction of Update Manager. Here are the changes that we noticed in our lab compared to the task in Version 5.10:

- Software distribution can now deploy IBM system BIOS, firmware, and drivers to all levels of managed systems, including Level-0 systems. This is in addition to its original ability to push IBM Director Agent (or Core Services) to Level-0 systems.

- Software distribution no longer streams packages to multiple Level-0 or Level-1 systems concurrently. Packages can be pushed in parallel only to multiple Level-2 systems. If IBM Director Agent is not installed on the target systems, packages are pushed to one system at a time. Once the entire set of packages destined for a target is delivered, distribution continues with the next system in line. Note that if distribution fails on a system for any reason, it will effectively stop the entire software distribution job. It is therefore a good idea to install IBM Director Agent wherever possible.

- The Software Health Check feature of software distribution can still be used to identify which systems require updates to BIOS, firmware, and drivers. However, Update Manager provides a more automated method of achieving this goal. It also adds the ability to search for updates available from IBM and stores downloaded updates on the management server in a local IBM Director updates library.

You can still generate a current health check from software distribution by right-clicking a package or category and selecting **Perform Health Check**. However, this action no longer creates a dynamic system group in conjunction with the software health check. To create a group, use the File → Create → **Static systems group** option from the software health report report. Note that the groups created are now static rather than dynamic.
At the time of this writing, there is a bug in the software distribution code that applies an internal package ID number to the static group created, rather than the package or category name. This issue is seen in the highlighted area of Figure 6-57. This can make it virtually impossible to determine which package or category should be applied to the group later on.

For this reason, we recommend deleting the static groups created using this mechanism as soon as you are finished with the current software distribution operation. If needed again, they are quick and easy to recreate.

Figure 6-57  Software distribution bug - displays internal ID rather than package name
If you have previously performed a software health check, you can view the latest report by right-clicking a package or category and selecting **View Health Check Report**.

At the time of this writing, there is a bug in the software distribution code that acts as follows: If you attempt to View Health Check Report before one has been performed, a Software Health Check Log window opens that states **Please wait while running compliance check**, but the compliance check never completes, as shown in Figure 6-58. This is not a serious issue, since you can simply close this window and select **Perform Health Check**. Once the initial check is performed, View Health Check Report works as expected.

![Software Health Check Log](image)

*Figure 6-58  Software distribution bug - Software Health Check never completes*

The two right-click items for software distribution categories and packages, Perform Health Check and View Health Check Report, now perform exactly the same function. The Perform Health Check option no longer creates a dynamic system group in conjunction with the software health check. To create a group, use the **File → Create → Static systems group** option from the software health report. Note that the groups created are now static rather than dynamic.

**IBM Update Assistant**

IBM Update Assistant is a wizard that imports software distributed by IBM into the management server and creates a software package for distribution. IBM Update Assistant can import these types of software packages:

- Packages in the **Solution Install** format, an architecture that provides a universal way to package and distribute software
- Packages in the **UpdateXpress for System x** format
Solution Install packages enable software distribution to Level-0, Level-1, and Level-2 managed systems. Solution Install packages contain the following elements:

- Installable unit (IU) of software that is self-extracting, self-installing, and runs in silent, unattended mode
- Installable unit deployment descriptor (IUDD) XML file, the PackagedIU.xml file that describes the dependencies of the package
- Artifact XML file that describes the installation instructions for the IU
- An XML file in System x format that enables Software Health Check for the package

A Solution Install package can be in the form of a JAR file, a Zip file, or a Solution Install formatted directory structure that can be accessed through the ComponentNamePackagedIU.xml file (the ComponentName prefix is optional).

UpdateXpress packages can be distributed only to Level-2 managed systems. UpdateXpress packages contain the following elements:

- The software-update file that is self-extracting, self-installing, and runs in silent, unattended mode.
- An XML file in System x format that describes the software-update file and how to install it. This file must also contain Software Health Check information in order for this function to work.

**IBM Director installation packages**

The IBM Director CD includes several Install Solution packages that can be imported into the Software Distribution task. Table 6-4 shows a list of the IBM Director installation packages that are included on the IBM Director CD and their locations on the CD.

<table>
<thead>
<tr>
<th>Installation package</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Director Agent for Windows</td>
<td>director\agent\windows\i386\META-INF</td>
</tr>
<tr>
<td>IBM Director Agent for Linux</td>
<td>director\agent\linux\i386\META-INF</td>
</tr>
<tr>
<td>IBM Director Core Services for Windows</td>
<td>coresvc\agent\windows\i386\META-INF</td>
</tr>
<tr>
<td>IBM Director Core Services for Linux</td>
<td>coresvc\agent\linux\i386\META-INF</td>
</tr>
<tr>
<td>Open SSH for Windows</td>
<td>coresvc\openssh\windows\i386\META-INF</td>
</tr>
</tbody>
</table>
For more information about using the Software Distribution task to push IBM Director Agent or Core Services, see 13.2, “Automated IBM Director Agent promotion” on page 776.

IBM Director installation packages that can be imported into the Software Distribution task are also available for download from the IBM Web site, including the ServeRAID Manager subagent and System Availability subagent. These can be downloaded for no additional charge from:


**UpdateXpress packages**

*UpdateXpress* is a set of self-contained CDs whose task it is to update system and subsystem BIOS, firmware, and device drivers on all System x and BladeCenter servers. At the time of this writing, there are three CDs in the UpdateXpress set, as follows:

- CD 1 updates System x servers running Windows operating systems.
- CD 2 updates System x servers running Linux operating systems.
- CD 3 updates BladeCenter servers, regardless of operating system.

All three CDs contain an operating-system-independent boot sequence for BIOS and firmware updates on their respective systems.

UpdateXpress is available as a regular CD subscription service. You can also download UpdateXpress CD images in ISO image file format from:


Once imported by IBM Update Assistant, any UpdateXpress packages can be distributed to managed systems by the Software Distribution task.

To import UpdateXpress packages, do the following:

1. Double-click the **Software Distribution** task in IBM Director Console.
2. Double-click **IBM Update Assistant**.
3. Select whether the files are local or on the IBM Director Server system, and click **Browse**. This opens a window (Figure 6-59) from which you can browse to the update files source.

*Figure 6-59  IBM Update Assistant: specify the XML file*
4. Select the desired XML package descriptor file and click **OK**. For UpdateXpress, choose the **index.xml** file at the root of the CD or server share (Figure 6-60). For Web downloads, choose the XML file that was downloaded from the package download page.

**Tip:** Checking **Mark Categories Private** makes them visible to only the IBM Director account that created them.

*Figure 6-60  The index.xml file on an UpdateXpress server share*
5. Click **Next** to see a list of all of the packages available (Figure 6-61). If you are using the UpdateXpress CD, there is an extensive list of systems on the left, and package details on the right. If you are using an XML file from a downloaded package, you can see only a single package on the right, and the details on the left.

![IBM Update Assistant package selection](image)

*Figure 6-61  IBM Update Assistant package selection*

The UpdateXpress CD contains updates for multiple systems. The updates are categorized by System x server model and type number to make it easy to decide which updates to apply to which managed systems later. Selecting any particular update provides a complete description of that update in the right pane of this window.
Tip: To select an entire category of updates, right-click the desired model-type and click Select All Items, as shown in Figure 6-62. You also can choose just to select all critical updates for a particular system.

![Figure 6-62 Selecting all updates for a specific system](image)

6. When you have selected all desired updates for import, click Finish to begin the import. Depending on the number of packages selected, the import process can take several minutes. The package currently being imported is documented in the status line at the bottom of the window.
After the packages have been imported, the IBM Director Console window displays them as subtasks under the Software Distribution task, as shown in Figure 6-63.

Figure 6-63  IBM Director Console showing imported UpdateXpress packages ready for distribution
7. If you right-click a software distribution package category (for example, the xSeries 440 entry highlighted in Figure 6-63 on page 362) and click **Open**, the Edit Package Category window opens, displaying details for the package category. Figure 6-64 shows an example of this detail.

![Edit IBM eServer xSeries 440-8667 -- Linux - UpdateXpress Server -- 1.0](image)

The **Available Packages** pane on the left side of this window lists all packages that are available in all categories. Greyed-out entries are already in the current category and shown in the **Selected Packages** pane on the right. Green entries are other packages that are not in the current category but can be added by double-clicking each. You can remove packages from the category by selecting the package name in the **Selected Packages** pane and clicking **Remove** (or by double-clicking them).

Each package in the current category can specify that a reboot be performed after its installation, and some packages have this checked by default. You can change this for some packages by clicking the check box. If the Reboot check box will not allow you to deselect it, this is an indication that the package has a reboot command hardcoded. You can also specify whether a reboot of the target system is to be performed after all packages in the category are distributed.
Implementing IBM Director 5.20

The order displayed in the Selected Packages pane is the order in which packages are installed if the entire category is installed. You can change this order by selecting the package to be moved and clicking the up or down arrow buttons (↑ and ↓) next to the list of packages, or by right-clicking the package name and selecting Move Package Up or Move Package Down, as seen in Figure 6-65.

![Selected Packages](image)

Figure 6-65  Modifying package installation order

8. To install packages or complete categories of packages to a system or a group of systems, simply drag and drop the appropriate entry in the Tasks pane onto a system or a group. You are then prompted whether you want the task to execute now or be scheduled to run later.

There are some additional tasks you can perform on packages including:

- View Package Summary provides an overview of the package specifics such as supported platforms, install path, and reboot required.
- Create Package for Delayed Distribution installs the package to a distribution server without requiring it to be pushed to any agents.
- View Distribution History shows the systems to which the package has been applied, grouped by status (success and fail).
- Secure Package locks the package so that an ID and password must be supplied to modify the package.

**Software Health Check**

The Software Health Check subtask of Software Distribution allows you to determine which systems are candidates for distribution packages. For example, one of the first packages you will probably create is the IBM Director Agent.

**Important:** If the Reboot at end of Category Distribution check box is selected, target systems in the distribution will be rebooted even if no updates are performed.
installation package. For more about using the Software Distribution task to push IBM Director Agent or Core Services, see 13.2, “Automated IBM Director Agent promotion” on page 776.

Following the steps in the previous section, we create a package for IBM Director Agent installation. The required XML package descriptor can be found on the IBM Director CD in the director\agent\os\i386\META-INF directory, where os is either Windows or Linux.

After the package has been imported into software distribution, simply right-click it and select **Perform Health Check**.

Software Health Check performs a scan of all managed systems, and provides a list of systems that have IBM Director Agent software installed, as shown in Figure 6-66. Any systems running the same version (or later) of IBM Director Agent are listed in one section of the report, while systems running earlier versions are listed in another section. Note that only systems that have IBM Director Agent already installed are included in the list. Level-0 and Level-1 managed systems are not included.

![Software Health Check Log](image)

**Figure 6-66** Software Health Check for IBM Director agent 5.10 showing two candidates

### 6.3.20 System Accounts

The System Accounts task allows you to administer local system accounts remotely on managed systems.
To use it, simply drag and drop the task on the system you wish to manage (Figure 6-67).

![System Accounts Window](image)

**Figure 6-67 The System Accounts window**

### 6.3.21 Update Manager

The new Update Manager task provides integrated management of updates for managed systems, including new tasks for creating profiles, downloading updates, comparing updates defined in profiles against systems, and generating reports.

Since Update Manager enables a significant new set of functionality in IBM Director related to keeping your system firmware and drivers up to date, we have dedicated an entire chapter to covering this topic. See Chapter 7, “Update Manager” on page 411, for more information.

### 6.4 Mass Configuration

Mass Configuration is not actually a task in IBM Director. Rather, using the Profile Builder subtask, you can create and edit Mass Configuration profiles that can be executed against managed systems and groups in IBM Director Console.
These profiles store configuration information for one of four base IBM Director tasks:

- Asset ID
- Configure Alert Standard Format
- Configure SNMP Agent
- Network Configuration

After a Mass Configuration profile has been created, it is used to automatically configure a managed system or group of systems to the parameters stored in the profile. This can save significant time and effort, as well as reduce the potential for errors associated with editing these parameters manually.

Rather than examine each of the supported tasks in detail, we take a brief look at how you might use Mass Configuration with two of the supported IBM Director tasks to save time and effort. You can apply the principles presented here to create Mass Configuration profiles for any of the supported IBM Director tasks.

### 6.4.1 Asset ID Profile Builder

To create an Asset ID Mass Configuration profile, right-click the Asset ID task in IBM Director Console and select **Profile Builder**.
Figure 6-68 shows the Asset ID Profile Builder, in which you can specify any Asset ID information for later distribution to managed systems. Click **New Profile**, enter a profile name, then click **OK**. The new profile opens for editing.

![Asset ID Profile Builder window](image)

*Figure 6-68  Asset ID Profile Builder window*

In our example, we have received a large number of new systems that are being staged for deployment. These are leased systems, so we would like to track the lease start and end dates, as well as the lease cost of these systems. For simplicity, we assume that all systems have the same cost.
From the Lease tab (Figure 6-69) click the check box to the left of each field to enable that field in the profile for editing. Then enter the appropriate information and save the Mass Configuration profile.

If Enable Changes is unchecked, other administrators will be unable to make changes to this Mass Configuration profile. To enable other administrators to update or alter this profile and distribute to systems, click the **Enable Changes** box.

Once saved, the profile shows up under the Asset ID task in the management console. The easiest way to send this Asset ID profile to our new systems is to create a group that will include only these new systems. Refer to the Managing groups section of Chapter 2 in the *IBM Director Systems Management Guide* and 5.3, “IBM Director groups” on page 243, of this book for more information about working with groups in IBM Director.
When the new systems have come online and are available for management, simply drag the appropriate Asset ID profile onto the group created for this purpose. Figure 6-70 shows the Status window, which provides confirmation that the profile was received and processed by each managed system in the group.

![Status window](image1.png)

**Figure 6-70  Asset ID Mass Configuration Profile Status window**

You can recall the list of managed systems to which any Mass Configuration profile has been sent by right-clicking the profile in the management console and clicking **Profile Manager**. The status window shown in Figure 6-71 is displayed, from which you can check the status of each profile against each managed system.

![Profile Manager window](image2.png)

**Figure 6-71  Asset ID Mass Configuration Profile Manager window**

Once a Mass Configuration profile has been sent successfully to a managed system, all data included in the profile replaces that stored in the managed system’s Asset ID file.
6.4.2 Configure SNMP Agent Profile Builder

If you use SNMP in your environment, it is very useful to be able to configure the Traps pane of the SNMP service properties remotely on multiple systems at once. You can use mass configuration to do this.

Figure 6-72 shows an example of how you might change the SNMP Community Name (an important security measure described in Chapter 3, “Security planning and implementation” on page 93) and Trap Destinations for your managed systems.

**Tip:** IBM Director Inventory does not reflect this update until an inventory collection is completed successfully for that managed system.

Note that a Configure SNMP Agent profile will only configure the Traps pane, not the Security pane. Therefore, adding a Community Name in the profile will add
this Community Name only as a trap destination. For IBM Director Server, you must add this same Community Name manually in order for IBM Director to receive traps sent to this community.

To check what IBM Director server is configured for, in the main menu click **Options → Discovery Preferences**. Then click the **SNMP Devices** tab, which displays the SNMP configuration, as seen in Figure 6-73.

![Figure 6-73  SNMP configuration in IBM Director server](image-url)
Also, if you want to be able to perform SNMP sets on managed systems, you must modify the Security pane manually in the SNMP service properties window, adding the proper Community Name as READ WRITE or READ CREATE enabled on each managed system. This configuration is illustrated in Figure 6-74.

![Figure 6-74 Security pane of the SNMP Service Properties window](image)

Also, we strongly advise that you remove the default public community name in the Security pane of the SNMP service properties window. For security reasons discussed in Chapter 3, “Security planning and implementation” on page 93, it is important that you do this manually for any managed system running the SNMP protocol. See 3.4.8, “SNMP access control” on page 145, for details about how to do this.

As in the Asset ID example, you can confirm that the Configure SNMP Agent profile has been successfully delivered to and processed by each managed system to which it is sent.

### 6.4.3 Network configuration

Our final discussion of mass configuration centers on remotely configuring the Network Control Panel settings on managed systems. Most large IT
infrastructures use a combination of DHCP and static IP addressing. It is a
typical practice to use DHCP for IP configuration of client systems and many
servers, while using static IP configuration for key servers, especially the DHCP
server itself, Windows Domain Controllers, DNS servers, and the like.

Mass configuration of network settings is an extremely useful capability. In the
element illustrated in Figure 6-75, we use mass configuration to add the IP
address of a new DNS server into the network configurations of all managed
systems currently using a static IP configuration.

Simply enable the check box to the left of the IP address box, enter the IP
address for the new DNS server in the box at the right, and click the < button to
move the address into the list box. Save the profile and you can make this
change on any managed system in your environment.

Because this particular profile is likely to be applied only to managed systems
using static IP configuration, it is helpful to create a group in advance that
includes only those managed systems using static IP configuration.

In addition to changing static IP configuration, you can use mass configuration to
ensure that managed systems are using DHCP as intended. In some settings,
more technically advanced users attempt to circumvent established IT guidelines
by changing certain system settings. A properly configured network configuration profile, sent to managed systems on a regular basis, can help ensure that DHCP is used where appropriate. This can help keep the IP environment working optimally for all users.

Another useful capability of the network configuration profile is the ability to place a managed system in the proper Windows domain. Figure 6-76 shows how you might configure such a profile if you wanted to ensure that your managed systems were logging in to the Windows Domain called *IBM*.

![Network Configuration Profile Builder - Windows domain](image)

*Figure 6-76 Network Configuration Profile Builder - Windows domain*

You can even have a computer account created in the domain, but to do this you must include the user name and password of a user account that has the right to add workstations to the domain. Any account in the default Domain Admins group has this right in addition to others. Using Windows Domain Security Policy, you can grant only this right to an account for a more secure environment.
6.5 Install-time extension tasks

These extensions are provided on the IBM Director installation CD and can be selected for installation during initial installation of base IBM Director components. They are:

- 6.5.1, “BladeCenter Management” on page 376
- 6.5.2, “Rack Manager” on page 381

6.5.1 BladeCenter Management

BladeCenter Management consists of two tasks that can be used to rapidly deploy IBM BladeCenter chassis. Similar to the Server Configuration Manager, they are profile-based tasks that can be applied to one or more chassis to configure many settings. See 6.3.17, “Server Configuration Manager” on page 335, for details on that task.

BladeCenter Configuration Manager

This subtask is essentially identical to the Server Configuration Manager task, although it allows for the configuration of additional hardware components that can be installed only in a BladeCenter chassis. You can use the BladeCenter Configuration Manager to create a profile that contains BladeCenter configuration information. Once created, the profile can be reused and modified.

A few enhancements have been added to this tool in IBM Director 5.20. You can use the BladeCenter Configuration Manager to generate an XML configuration file that can be used with the IBM Director command-line interface. In addition, you can read the current hardware configuration from a BladeCenter chassis. Finally, you can create a profile that, when applied to a BladeCenter, will configure the boot sequence for all blades in the chassis.

The BladeCenter Configuration Manager enables you to create a profile that includes configuration settings for the components of a BladeCenter chassis, as well as settings for switches and management modules, and configuration parameters for iSCSI communication. Using the BladeCenter Configuration Manager, you can create a profile that will configure the following components:

- IP Address Pool containing IP addresses for the network interfaces of the management and switch modules.
- Ethernet Switch for configuring the Cisco, IBM, and Nortel switch modules for:
  - Module protocols: login accounts, IP address, enable/disable HTTP and Telnet, SNMP communities and hosts, enable/disable external ports.
  - VLAN configuration: names, IDs, egress and individual port configuration.
Fibre Switch for configuring Brocade and IBM Fibre Channel switch module for module protocols: login accounts, IP address, enable/disable HTTP and Telnet, SNMP communities and hosts, enable/disable external ports.

Management Module for configuring the IBM BladeCenter management module for:

- Login accounts: Set login accounts and authority level (administrator/read-only).
- Network interface: DHCP or static, SNMP communities and hosts and SNMPv3 authentication information.

Reading the current BladeCenter configuration

You can use the BladeCenter Configuration Manager to create a profile based on the current hardware configuration of a BladeCenter unit that is managed by IBM Director.

To create a BladeCenter configuration profile by reading the current hardware configuration of a BladeCenter chassis, complete the following steps:

1. Select the BladeCenter chassis with the configuration that you want to read in the Group Contents pane of the management console.

2. Select Tasks → BladeCenter Management → BladeCenter Configuration Manager → BladeCenter Configuration Manager: chassis_name.
   
   Where chassis_name is the name of the chassis of interest.

3. In the Quick Start window, click the Read current hardware configuration icon.

4. The Configuration Manager Editor window displays all components for the BladeCenter chassis. Click a component to read or modify the component information. If you make changes to the profile, make sure to save them.
Creating a BladeCenter profile manually

To create a profile, double-click the **BladeCenter Configuration Manager** task. Click **Create New Profile** in the Quick Start window. Provide a name for the configuration profile. In our example, we use DevTest, and select the applicable items for our DevTest chassis in Figure 6-77.

![Select components](image)

*Figure 6-77  Components selected for profile configuration*
Click **OK**, and the Configuration Manager Editor windows opens. Select one of the components in the left pane and populate the fields in the right pane with the required information. Figure 6-78 shows the IP Address Pool configuration.

![Configuration Manager Editor - BladeCenter DevTest](image)

**Figure 6-78  IP Address Pool configuration editor**

Simply continue working through all of the components on the left side, providing the required information in the right pane.

**Tip:** Scroll through the window to the right to see the Add buttons. They are not visible in Figure 6-78.

After all the components have been configured, click **File → Save Profile**.
The new profile is listed under the BladeCenter Configuration Manager. This profile can now be dropped on the discovered BladeCenter chassis to configure them.

![BladeCenter Management Diagram]

*Figure 6-79  New DevTest configuration task*

**Network Device Manager**

The Network Device Manager task enables you to launch a management interface (Telnet/Web) and specify the default protocols used to communicate with the switch modules.

![Network Device Manager Interface]

*Figure 6-80  BladeCenter Network Device Manager*

To manage a device, simply drag and drop the task onto the device you want to manage. If a default has been set in the interface in Figure 6-80, it automatically
launches the specified session (Telnet or Web). If no default is specified, you have the option of which to use, as seen in figure Figure 6-81.

![Network Device Manager](image)

*Figure 6-81  Network Device Manager application launch interface*

### 6.5.2 Rack Manager

Rack Manager is used to group your equipment in rack suites. Using Rack Manager, you can create *virtual* racks by associating equipment such as managed systems and devices, networking devices, power devices, and monitors with a rack to visually represent an existing rack in your environment. If the inventory collection feature of IBM Director does not recognize a managed system or device in Rack Manager, you can associate it with a predefined component of a similar size.
Figure 6-82 shows a rack configuration in a graphical view. A table view also is available.

*Figure 6-82 Rack Manager graphic view*
You can use Rack Manager to view hardware status alerts that occur on managed systems or devices in a rack. If a rack component has a hardware status alert, the rack component is outlined in red, blue, or yellow, depending on the alert level. An example of a critical hardware status (red outline) indication is provided in Figure 6-83.

**Tip:** When you highlight a system, it is shown with a green box even if the hardware status of the system displays as red.

![Rack Manager showing a system with critical hardware status](image)

**Important:** Certain devices from the Monitors group of Rack Manager Components include a hollow red rectangular box as part of the graphic itself. Do not confuse this with the red system outline indicating critical hardware status.

It is easy to confirm hardware status in Rack Manager by looking for the hardware status icons in the tree view in the left pane of the display. The devices are the T54A Flat Panel Monitor Model AG1, the T540 Flat Panel Monitor Model AG4, and the IBM T55a Flat Panel Monitor Model AG1.
6.6 Free extension tasks

There are a number of IBM Director extensions that can be downloaded from the Web at no additional cost. You can download free IBM-developed extensions from:


In addition, many third parties are working on extensions to IBM Director. These extensions may be free Web downloads or, in some cases, may be fee-based offerings. See the Web site of the appropriate third party for more details.

Refer to the following sections for information about the free extensions to IBM Director that were available at the time of this writing:

- 6.6.1, “APC PowerChute Extensions for IBM Director” on page 384
- 6.6.4, “ServeRAID Manager” on page 391
- 6.6.5, “System Availability” on page 393

In addition to the tasks provided by the extensions listed above, we cover a few free extensions in sufficient detail as to warrant dedicated chapters for each. You will find detailed information about these extensions in the following chapters:

- Chapter 8, “IBM Electronic Service Agent” on page 459
- Chapter 9, “IBM PowerExecutive” on page 485
- Chapter 10, “IBM Virtualization Manager” on page 513

6.6.1 APC PowerChute Extensions for IBM Director

The APC PowerChute Extensions for IBM Director are a pair of extensions, one for IBM Director Server and one for IBM Director Console, that integrate inventory and event data from the APC PowerChute Business Edition (PCBE) Agent or APC Network Management Card into IBM Director.

The PowerChute Extensions work in much the same way IBM Director Upward Integration Modules integrate information from IBM Director Agent into higher level managers. This is a change from previous versions of APC plug-ins for IBM Director because there is no longer an agent extension.

The IBM Director Server extension does all the work of translating APC inventory and events into a format IBM Director can understand. The IBM Director Console extension provides the user interface components for the integration. The data itself comes from the PowerChute Business Edition (PCBE) Agent running on a system with a serial connection to an APC UPS, or directly from a supported APC Network Management Card. In this latter case, no agent of any type is required,
because direct communication is established between the UPS and the IBM
Director Server.

Using the APC PowerChute Extensions, you can manage PowerChute data and
events directly from IBM Director Console. The software can be downloaded from:
http://www.apc.com/tools/download/

Look for PowerChute Extensions for IBM Director under Software Upgrades -
Management Platform Integration.

Installation is simple and straightforward, especially in the case of IBM 3000X
Uninterruptible Power Supplies. These are APC-manufactured UPSes that
include the APC Network Management Card. Therefore, no PCBE agent is
needed to manage these UPSes. The PowerChute Extensions for IBM Director
installer is shown in Figure 6-84.

Figure 6-84   APC PowerChute Extensions for IBM Director installation window

To manage any APC UPS that includes an APC Network Management Card,
simply install both extensions (one for IBM Director Server and one for IBM
Implementing IBM Director 5.20

Director Console (on your management server. Optionally, you can also install the PowerChute Extensions for IBM Director Console on any remote management consoles in your environment.

To manage an APC UPS that does not have an APC Network Management Card installed, you also need to install the PCBE Agent on a system to which the UPS is connected with a serial cable.

When you have installed the APC PowerChute Extensions for IBM Director successfully, you can see a number of changes within the management console, including the addition of the Systems with APC Extensions dynamic group and the APC UPS Browser task in IBM Director Console, as shown in Figure 6-85.

![IBM Director Console with APC PowerChute Extensions installed](image-url)

*Figure 6-85  IBM Director Console with APC PowerChute Extensions installed*
As already mentioned, with the PowerChute Extensions for IBM Director installed, you can track UPS inventory data. Figure 6-86 shows an example of an Inventory query run against a couple of APC UPSes.

Figure 6-86  Inventory query showing details on APC UPSes
In addition, UPS resource monitors are added, which allow you to determine exactly what is going on with your APC UPSes. Items such as input, output, and battery voltage, temperature, humidity, and input line frequency, among others, can be monitored, as seen in Figure 6-87.

![Resource monitors provided by the APC PowerChute Extensions](image)

Figure 6-87  Resource monitors provided by the APC PowerChute Extensions

The APC tasks can show battery level remaining on a monitored UPS. You can also track battery replacement date, utility line voltage, and many other parameters. You can even establish resource monitors or use Capacity Manager to track UPS performance over time.
In addition to monitoring various parameters, event action plans can be configured to alert you in the event of a problem with your AC line power or UPS battery life, as well as other situations. Automated action can also be achieved via a properly configured event action plan. Figure 6-88 shows a number of event filters that are added by the PowerChute Extensions.

Figure 6-88   Event Filters added by APC PowerChute Extensions
Finally, the Shut down or Reboot UPS Event Action is added to the Event Action Plan Builder, as shown in Figure 6-89. This action can be applied automatically by an event action plan when a particular event occurs.

![Event Action Plan Builder showing Shut down or Reboot UPS event action](image)

**6.6.2 Electronic Service Agent**

The Electronic Service Agent (ESA) is a *no-charge* software tool that resides on the customer's system to monitor events and transmit system inventory information to IBM on a periodic, customer definable time table. This monitor tracks and captures system inventory, hardware error logs, and performance.
information, automatically reporting hardware problems to IBM as long as the server is under an IBM Maintenance agreement or within the IBM warranty period. Information collected through ESA is available to IBM service support representatives to assist in diagnosing problems. With the early knowledge of potential problems, provided by ESA, IBM can proactively respond to customers and assist in maintaining higher availability and performance.

For more information see Chapter 8, “IBM Electronic Service Agent” on page 459.

6.6.3 PowerExecutive

The IBM PowerExecutive tool is available for selected IBM BladeCenter and System x servers and allows direct power monitoring through IBM Director. This tool helps customers monitor power consumption to allow better utilization of available power resources.

This application software enables customers to trend actual power consumption and corresponding thermal loading of System x and BladeCenter servers running in their environment with their applications.

For more information see Chapter 9, “IBM PowerExecutive” on page 485.

6.6.4 ServeRAID Manager

The IBM ServeRAID Manager extension enables you to remotely manage IBM ServeRAID controllers in System x servers and IntelliStation workstations.

The ServeRAID Manager extension supports the following controllers:

► ServeRAID family of controllers and adapters
► HostRAID controller

The LSI MegaRAID controller and IBM ATA 133 RAID adapter are not supported.

See Chapter 3 of the ServeRAID Manager Installation and User's Guide available from the following URL for details of the level of support:

http://www.ibm.com/systems/management/director/resources

With the functionality provided, you can:

► View controller status (arrays and LUNs).
► Scan for new or removed drives.
► Manage (create/delete/increase) arrays and LUNs.
► Manage drives - change status (online/offline), assign hot spares.
► View the details and status of the external enclosure (if present).
View the event log.

Views of the IBM ServeRAID Manager are shown in Figure 6-90 and Figure 6-91 on page 393.

![ServerRAID Manager](image)

**Figure 6-90   RAID array with failed drive**
To use the ServeRAID function within IBM Director, you must install the server component on the server, the agent component on the managed system, and the console component on any system running the console.

![Console event log](image)

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Source</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/11/2005</td>
<td>10:44:42 AM</td>
<td>mckunley...</td>
<td>Physical drive removed: controller 3, channel 1, SC51D 3</td>
</tr>
<tr>
<td>09/11/2005</td>
<td>10:43:54 AM</td>
<td>mckunley...</td>
<td>Removed the defunct drive from controller: controller 3.</td>
</tr>
<tr>
<td>09/11/2005</td>
<td>10:44:32 AM</td>
<td>mckunley...</td>
<td>Deleted logical drive: controller 3, logical drive 1</td>
</tr>
<tr>
<td>09/11/2005</td>
<td>10:43:21 AM</td>
<td>mckunley...</td>
<td>Defunct drive: controller 3, channel 1, SC51D 3 (FRU part # 345433)</td>
</tr>
<tr>
<td>09/11/2005</td>
<td>10:43:21 AM</td>
<td>mckunley...</td>
<td>Logical drive is critical: controller 3, logical drive 1</td>
</tr>
<tr>
<td>09/11/2005</td>
<td>10:42:36 AM</td>
<td>mckunley...</td>
<td>ServeRAID Manager started.</td>
</tr>
<tr>
<td>09/11/2005</td>
<td>07:58:58 AM</td>
<td>mckunley...</td>
<td>Periodic scan found one or more critical logical drives: controller 3. Repair as soon...</td>
</tr>
<tr>
<td>09/10/2005</td>
<td>11:58:47 PM</td>
<td>mckunley...</td>
<td>Periodic scan found one or more critical logical drives: controller 3. Repair as soon...</td>
</tr>
<tr>
<td>09/10/2005</td>
<td>03:58:45 PM</td>
<td>mckunley...</td>
<td>Periodic scan found one or more critical logical drives: controller 3. Repair as soon...</td>
</tr>
<tr>
<td>09/10/2005</td>
<td>07:58:40 AM</td>
<td>mckunley...</td>
<td>Periodic scan found one or more critical logical drives: controller 3. Repair as soon...</td>
</tr>
<tr>
<td>09/09/2005</td>
<td>11:58:33 PM</td>
<td>mckunley...</td>
<td>Periodic scan found one or more critical logical drives: controller 3. Repair as soon...</td>
</tr>
<tr>
<td>09/09/2005</td>
<td>04:05:15 PM</td>
<td>mckunley...</td>
<td>Defunct drive: controller 3, channel 1, SC51D 3 (FRU part # 345433)</td>
</tr>
<tr>
<td>09/09/2005</td>
<td>04:08:16 PM</td>
<td>mckunley...</td>
<td>Logical drive is critical: controller 3, logical drive 1</td>
</tr>
<tr>
<td>09/09/2005</td>
<td>04:04:13 PM</td>
<td>mckunley...</td>
<td>ServeRAID Manager started.</td>
</tr>
<tr>
<td>09/09/2005</td>
<td>04:04:47 PM</td>
<td>mckunley...</td>
<td>Defunct drive: controller 3, channel 1, SC51D 3 (FRU part # 345433)</td>
</tr>
<tr>
<td>09/09/2005</td>
<td>04:04:47 PM</td>
<td>mckunley...</td>
<td>Logical drive is critical: controller 3, logical drive 1</td>
</tr>
</tbody>
</table>

**Figure 6-91  ServeRAID manager console log viewer**

### 6.6.5 System Availability

System Availability analyzes the availability of a managed system or group. You can view statistics about managed system uptime and downtime through reports and graphical representations.

The System Availability extension was updated with IBM Director 5.20 to make changes associated with the U.S. energy bill that will lengthen daylight saving time by four weeks starting in 2007.

System Availability can identify problematic managed systems that have had too many unplanned outages over a specified period of time or a managed system that has availability data that is too old or fails to report data to IBM Director Server. When a System Availability report is generated, managed systems that meet the criteria you specify as being problematic are flagged as such.
System Availability can display managed system outage information graphically as a percentage of total downtime (Figure 6-92) by the day of the week (Figure 6-93 on page 395) or by the hour of the day (Figure 6-94 on page 395). These displays can be very helpful in recognizing patterns of system outage that might not otherwise be apparent.

![System Availability showing the distribution of system outages](image)

*Figure 6-92  System Availability showing the distribution of system outages*
Figure 6-93  System Availability showing outages by day of the week

Figure 6-94  System Availability showing outages by hour of the day
In addition, you can *tear off* (separate) any of the graphic displays in order to compare items. Figure 6-95 shows two such graphs for system outages by hour of day.

The top graph is from a group of six servers in our managed environment. By comparing this to the lower graph, which shows one of the subject systems (Shackleton) during the same period, it is easy to see that Shackleton is responsible, to a large degree, for the high number of unplanned outages experienced by this group.

*Figure 6-95   Two torn off graphs from System Availability arranged for comparison*
Finally, System Availability also can display the raw availability data and summary information in a table format, as shown in Figure 6-96. This can be especially useful in determining how the graphs are plotted and in determining percentage uptime for a given managed system or group of systems.

To identify a managed system as problematic, the managed system must have the IBM Director 5.10 System Availability Agent installed.
6.6.6 Virtualization Manager

IBM Virtualization Manager is a follow-on to the Virtual Machine Manager (VMM) extension to IBM Director. It allows you to manage both physical and virtual machines from a single IBM Director Console. You can use Virtualization Manager to provide various views of your environment, and monitor the status and performance of virtual and physical machines.

We cover this extension in detail in Chapter 10, “IBM Virtualization Manager” on page 513.

6.7 Fee-based extension tasks

These extensions require a license, which is purchased prior to installation of the software. These extensions add significant additional functionality to the base IBM Director environment. See 1.6, “IBM Director licensing” on page 20, for more information about IBM Director licensing, including where and how to purchase licenses for these extensions.

Refer to the following sections for more information about the fee-based extensions to IBM Director that were available at the time of this writing:

- 6.7.1, “Capacity Manager” on page 399
- 6.7.2, “Remote Deployment Manager” on page 400
- 6.7.4, “IBM z/VM Center” on page 409

Important: For special considerations when upgrading IBM Director Agent 4.x and Server Plus Pack code on existing managed systems, see 4.3, “Server Plus Pack considerations” on page 177.
6.7.1 Capacity Manager

Capacity Manager is a resource management planning tool that you can use to monitor system performance. It identifies bottlenecks and potential bottlenecks, recommends ways to improve performance through performance analysis reports, and forecasts performance trends. A network utilization forecast is shown in Figure 6-97.

Capacity Manager is a fee-based extension to IBM Director. You must purchase a Capacity Manager license for each managed system on which you want to use its functionality.
**Important:** If you upgrade your IBM Director environment from Version 4.x, uninstall any Server Plus Pack extensions before you install IBM Director Agent 5.x and the Capacity Manager 5.x subagent.

If you fail to uninstall any Server Plus Pack components before installing IBM Director 5.x, then unexpected results could occur. See 4.3, “Server Plus Pack considerations” on page 177, for information about how to clean up the installation.

Similar to the Resource Monitors task, which you can also use to monitor resource utilization, Capacity Manager can be used to capture resource monitor trends and for longer-term resource utilization monitoring. You can use Capacity Manager on any managed system with the Capacity Manager agent installed.

Additional information about how to configure and use these features is provided in the online help provided with the product. For more information about how to use Capacity Manager to help monitor and optimize server performance, see the book *Tuning IBM System x Servers for Performance*, SG24-5287.

### 6.7.2 Remote Deployment Manager

Remote Deployment Manager (RDM) is an IBM Director extension that facilitates the deployment of IBM and non-IBM systems. RDM allows for the remote, unattended installation of new and existing systems. RDM helps automate tasks such as initial OS installation, firmware updates, and even disposal of retired systems.

RDM now includes the ability to clone multiple partitions on a hard drive, as well as a template to clone Linux systems. By including RDM as a task within IBM Director, you are able to provide complete life-cycle management (deploy, manage, retire) of your environment from a single console. RDM provides support for both Windows and Linux operating systems.
RDM task functionality
The subtasks that are children of the Remote Deployment Manager task in IBM Director Console are actually templates. These templates can be used to create tasks that perform various functions on target managed systems. Figure 6-98 shows the templates associated with RDM, each of which is described in detail, as follows:

- The *CMOS Update* template is used to create a CMOS Update task that remotely configures BIOS settings on one or more target systems. The settings that you can update include:
  - Assignments for devices and input/output (I/O) ports
  - Power-on password
  - Start options, including startup (boot) sequences
  - Interrupt request (IRQ) settings
To use this template, you configure a donor system with the desired BIOS settings, then capture the settings using a utility such as srcmos.exe or cmosutils.exe. After the settings have been captured to a file, a task is created to configure other systems with identical settings.

► The *Custom* task template is a general-purpose template that you can use to create additional tasks that are not installed with RDM. You can use the Custom task template to create a task that performs the RDM commands that you define. The RDM *User's Reference* provides additional details.

► The *Donor Image* template provides access to the *Get Donor* and the *Put Donor* tasks. The Get Donor task creates an RDM image that includes the entire contents (all partitions) of the first hard disk drive of the donor system. The drive can contain Windows or Linux partitions. The Put Donor task is used to deploy a donor image. The donor image is the content of the partitions from the donor system.

► The *Linux Clone Install* template is used to create tasks that use a clone image to install Linux on target systems. You select the image from a list of Linux clone images. The same image can be downloaded to multiple systems.

► The *Linux Native Install* template is used to create a task that remotely installs the Linux operating system onto target systems. The Linux Native Install template uses a wizard to gather the configuration information and create tasks.

► The *Power Restore* template performs two related operations—backups and restores of the boot partition and the Master Boot Record. The Power Restore task uses the Power Restore program and the DeployCenter application from Symantec to perform the following functions:

  - The save-to-backup operation, which creates a backup image of the boot partition (usually the C: drive) of the target system and also can create a backup copy of the Master Boot Record
  - The restore operation, which restores the boot partition from the selected image and also can restore the Master Boot Record from its backup copy

► The *RAID Clone Configuration* template is used to create tasks that capture configuration information from RAID controllers and copy these configuration settings to another controller. The following RAID controllers are supported:

  - IBM ServeRAID controllers
  - Integrated SCSI controllers with RAID capabilities (LSI 1020 or LSI 1030)
  - IDEal RAID controllers
  - LSI1064 (LSI Logic Integrated RAID) controllers

► The *RAID Custom Configuration* template is used to create tasks that configure RAID controllers by using a wizard to gather RAID configuration
information and create other tasks. The following RAID controllers are supported:

- IBM ServeRAID controllers
- Integrated SCSI controllers with RAID capabilities (LSI 1020 or LSI 1030)
- IDEal RAID controllers
- LSI1064 (LSI Logic Integrated RAID) controllers

The Remote Storage Configuration template is used to create tasks that allocate and deallocate a logical unit number (LUN) on a remote storage network. Working with network storage devices requires the following tasks:

- Add the network storage devices. Use the Network Storage tool to add information about your network storage devices.
- Configure the remote storage. Use the Remote Storage Configuration task to configure your network storage devices.

FASTT Storage Manager 8.42 or later must be installed on the RDM server to use this template.

The Scan template is used to create tasks that query the hardware of target systems and add that inventory information to the IBM Director database. Since RDM tasks cannot run until a system has been scanned, the Scan task is the first RDM task that you run against each target system. The Scan task accomplishes the following:

- Adds the target system to IBM Director Console, if the system was not already displayed
- Obtains hardware information about the system
- Optionally, obtains user-defined information that is entered at the target system
- Optionally, renames a BladeCenter blade.
The **Script** template is used to create a task that runs a sequence of other RDM tasks against a target system. You can choose existing tasks as subtasks of a Script task. The subtasks are run against the target system in the order you specify. For example, a Script task could consist of all the steps required to roll out a system:

- Flashing the system firmware
- Updating CMOS
- Configuring RAID
- Installing an operating system and applications

The **Secure Data Disposal** template is used to create tasks designed to remove (scrub) data from the drives on target systems. All drives and partitions that are accessible by the BIOS on the target system can be scrubbed. Four subtasks are already available to perform the following:

- **Level-1: Limited Partition Removal** overwrites the master boot record, the first 100 sectors of each partition, and the last two sectors of all of the drives and partitions that are accessible to the system BIOS.
- **Level-2: 1-Overwrite Security** overwrites every sector on all of the drives and partitions that are accessible to the system BIOS.
– **Level-3: 4-Overwrite DOD Security** overwrites every sector on all of the drives and partitions that are accessible to the system BIOS on the target system. A secure disposal overwrites every sector on the applicable drives that are installed on the system four times. This disposal method is intended to make the data inaccessible by any technique and meets the United States Department of Defense standards.

– **Level-4: 7-Overwrite DOD Security** overwrites every sector on all of the drives and partitions that are accessible to the system BIOS on the target system. A secure disposal overwrites every sector on the applicable drives that are installed on the system seven times. This disposal method is intended to make the data inaccessible by any technique and meets the United States Department of Defense standards.

The *System Firmware Flash* template is used to create a System Firmware Flash task to update the firmware on target systems that support RDM. This task can be used to deploy firmware only to IBM systems. To deploy firmware to non-IBM systems, you must create a Custom task.

The *VMware Native Install* template is used to create a task that remotely installs VMware ESX Server on a target system. The VMware Native Install template uses a wizard to gather installation information and create a task.

The *Windows Clone Install* template is used to create tasks that use a clone image to install a Windows operating system and application set on target systems. You select the image from a list of Windows clone images that have already been created using the Get Donor task. The same image can be downloaded to multiple systems.

The *Windows Native Install* template is used to create tasks that install Windows and applications on target systems. The Windows Native Install template uses a wizard to gather the configuration information and create tasks.

### 6.7.3 Software Distribution Premium Edition

The Premium Edition of Software Distribution extends the base task functionality by enabling you to create your own distribution packages.

It provides wizards to build distribution packages based on:

- UpdateXpress or Install Solution packages
- AIX InstallP packages
- Windows MSI
- Windows InstallShield
- Linux RPM
- i5/OS Restore Packages
Additionally, there is a Custom Package Editor that allows you to create your own installation package.

The list of available package types is shown in Figure 6-100.
As an example, we create an Adobe® Reader distribution package:

1. Double-click the type of package you will be using. In this example we use Microsoft Windows Installer Package.

![MSI Package wizard](image)

Figure 6-101  MSI Package wizard
2. Provide a unique name for the package (Figure 6-101 on page 407) and browse for the install package. In our example, it looks for an MSI package to use (Figure 6-102).

![Completed package selection](image)

*Figure 6-102  Completed package selection*

3. Click **Finish** to complete the configuration and start the package build process.

4. Depending upon the type of package you are building, there might be additional options available if you click **Next** (if available). For example, an MSI package has options for a transform file location and additional Windows installer parameters.
After the package builder is finished, a new software distribution package is available. Figure 6-103 shows the addition of the Adobe MSI and RPM package.

![Software Distribution]

Figure 6-103   Newly created Adobe Reader® install packages

**Tip:** Software Distribution Premium Edition can be used to distribute files in addition to applications. While the File Transfer task is limited to a point-to-point transfer, you can use Software Distribution PE to distribute to groups.

### 6.7.4 IBM z/VM Center

The z/VM Center extension to IBM Director is specific for the virtual Linux server mainframe environment. z/VM Center provides a standardized way to deploy new z/VM virtual Linux systems through the easy-to-use IBM Director interface that does not require specific z/VM knowledge to operate.

It leverages the management access point (MAP) interface to z/VM that offers a CIM-based interface for z/VM system management functions. Its concept of virtual server templates and operating system templates allows you to repeat the creation of z/VM virtual guests and the deployment of Linux into these guests easily in a customized way.

See Chapter 11, “IBM z/VM Center” on page 569, for more information.
Update Manager

This chapter covers the new Update Manager task in detail, paying particular attention to creating and using profiles to manage firmware, BIOS, and driver updates for System x and BladeCenter hardware. We also spend considerable space discussing issues and pitfalls to avoid when using this new tool, as well as a few miscellaneous details that are not covered in the product publications.

- 7.1, “Update Manager overview” on page 412
- 7.2, “Updating IBM systems using Update Manager” on page 414
- 7.3, “Updating the management server” on page 433
- 7.4, “Update Manager and software distribution” on page 439
- 7.5, “Important considerations” on page 442
- 7.6, “Adding undiscovered machine types” on page 445
- 7.7, “Update Manager events” on page 448
- 7.8, “DIRCLI commands for Update Manager” on page 450

The IBM Director Planning, Installation, and Configuration Guide and the IBM Director Systems Management Guide are good sources of information related to working with the Update Manager user interface.

**Important**: We would like to call special attention to 7.5, “Important considerations” on page 442, where we establish basic expectations for this tool and point out a few design issues that can lead to serious situations if Update Manager is used without careful consideration and observation.
7.1 Update Manager overview

The new Update Manager task provides integrated management of updates for managed systems, including new tasks for creating profiles, downloading updates, comparing updates defined in profiles against systems, and generating reports. Update Manager augments the capabilities provided by previous versions of IBM Director, such as software distribution and IBM Update Assistant.

Update Manager uses profiles to provide the following core capabilities for managing System x and IBM BladeCenter firmware and driver updates:

- Acquiring updates automatically at scheduled intervals
- Checking the health of system software and reporting system status
- Creating software-distribution packages containing updates
- Deploying updates to remote System x and BladeCenter servers

The basic process used by Update Manager to keep systems up to date is shown in Figure 7-1. This diagram shows three basic steps, but there is significantly more to the process, and many points to keep in mind while building an update strategy.

Figure 7-1  The basic steps used by Update Manager to keep systems up to date
Some BladeCenter updates can be distributed over an out-of-band path through the chassis management module without requiring that the blade is even powered on. This distribution method has no requirements on the operating system or installed applications on the BladeCenter component.

In addition to the automated system updating capabilities introduced by Update Manager itself, other tasks and functions of IBM Director can be employed to configure a robust system update management mechanism. For example, the Scheduler can be used to kick off Update Manager downloads of new system updates from IBM on a regular basis, and an event action plan can be configured to alert you that new updates are available and have been downloaded. All you need to do is determine which updates to deploy and when to deploy them.

Update Manager works closely with software distribution, managing update profiles, which are used to download updates from IBM. Software distribution packages and categories can be created directly from an Update Manager profile. Performing a Software Health Check can also be accomplished directly from a profile.

IBM Update Assistant can still be used to push software distribution packages out to managed systems. Update Manager provides the additional ability to manage updates using profiles. This can be a convenient and useful way to organize updates for managed systems.

### 7.1.1 Update Manager profiles

Update Manager uses *profiles* to manage system updates. Profiles can be created for individual updates, or for update bundles. You use profiles to specify criteria that determine which updates are downloaded to your updates library. Using profiles, you can also determine which systems in your IBM Director environment are out-of-date and require updated system software.

Criteria for both types of update profiles include machine type and operating system combination. Individual update profile criteria can be further narrowed by selecting severity levels or update categories (for example, BIOS firmware updates) to include. If you want to receive individual updates, you can select multiple machine type and operating system combinations in one profile, or use a unique profile for each combination. Profiles for update bundles will search for UpdateXpress System Packs that match a single machine type and operating system pair. Only one update bundle can be included in an update bundle profile.

### 7.1.2 UpdateXpress System Packs

An UpdateXpress System Pack is an integration-tested bundle of online firmware and driver updates for IBM System x and IBM BladeCenter servers.
UpdateXpress System Packs simplify the downloading and installation of all online driver and firmware updates for a given system, ensuring that you are always working with a complete, current set of updates that have been tested together and bundled by IBM. A single click downloads the entire update bundle, along with a readme file and a complete change history, if available.

UpdateXpress System Packs are created for a machine type and operating system combination. Separate UpdateXpress System Packs are provided for Windows and each of the Linux distributions. Therefore, there could be several UpdateXpress System Packs for one particular machine type.

You can use Update Manager to automatically download UpdateXpress System Packs for a particular machine type and operating system combination.

### 7.2 Updating IBM systems using Update Manager

Update Manager makes updating IBM System x and BladeCenter servers easy. You can use Update Manager to create profiles, which are essentially groups of updates. One logical way to assign profiles is by system type. In our example, we create an Update Manager profile for an IBM System x3650 server running Windows Server 2003.

**Tip:** We recommend that you create an Update Manager profile for each IBM machine type being managed. This will make it easier to ensure that the most recent updates are deployed. We will discuss reasons for this as we proceed through our example.
Here we step you through a simple system update scenario for a single machine type. To create an Update Manager profile, do the following:

1. **Double-click the **Update Manager** task in IBM Director Console (or right-click and select **Create New Profile** to open the Create New Profile wizard, as seen in Figure 7-2).**

![Create New Profile wizard](image)

*Figure 7-2  Update Manager Create New Profile wizard - name the profile*

2. Type a name for the profile. Make this as descriptive, yet as concise, as possible. One way to do this is to make it obvious which system model is managed by this profile.
3. Click **Next** to move to the next step in the process, as seen in Figure 7-3.

![Image of Update Manager Create New Profile wizard]

**Figure 7-3** Update Manager Create New Profile wizard - select bundles or individual updates

4. Select whether you want to search the update repository for **Update bundles** or **Individual updates**. An update bundle is actually an UpdateXpress System Pack, which is an integration-tested bundle of online firmware and driver updates for IBM System x and IBM BladeCenter servers, as described above. If you select **Individual updates**, you must also select which types of updates are of interest. The default is to search for all individual updates.
5. Once your selection is made, click **Next** to proceed to the system selection window shown in Figure 7-4.

![Figure 7-4](image)

**Figure 7-4**  **Update Manager Create New Profile wizard - specify systems to include**

6. Select the system/OS pairs that will be managed by this profile from the list of systems discovered by the management server. These can be Level-0, Level-1, or Level-2 systems. You can verify that appropriate machine type inventory information is available by checking the **Inventory task** under **Hardware → SMBIOS → Component ID**. Note that if you manage a machine type that runs multiple operating systems (that is, Windows and Linux), that machine type will be listed for each OS running on that system type.

**Important:** This step determines which updates are downloaded from IBM. All updates for machine types selected in this window are downloaded from IBM, regardless of which updates are selected for inclusion in the profile.
7. Click **Next** to display a window that shows all of the updates currently in the updates library on the management server for the machine types and operating systems selected.

If this is the first time you are creating a profile, or if there are no updates in the local repository for the machine type and operating system combinations you selected, you are presented with the window shown in Figure 7-5. Proceed to step 9 on page 420.

**Tip:** You can manually add machine types to this window that have not been discovered by editing the updatePlatforms.txt file found in the Director\data directory. See 7.6, “Adding undiscovered machine types” on page 445, for details on how to do this.

![Create New Profile](image)

*Figure 7-5  Update Manager Create New Profile wizard - no updates in local update library*

If the update library on the management server contains updates for the items selected, you see a window showing all of the updates available in the local
update library that match the machine type and operating system combinations selected, as shown in Figure 7-6.

All of the updates in this list have already been downloaded from IBM and are stored in the local Update Manager library, which can be found on the management server in the Director\data\UpdateLib directory (assuming a default installation of IBM Director Server on a Windows system).

![Update Manager Create New Profile wizard - select updates to manage in profile](image)

**Figure 7-6**  Update Manager Create New Profile wizard - select updates to manage in profile

**Important:** When updates are downloaded from IBM, Update Manager retrieves all updates available for the selected machine type and operating system combinations and not just the individual updates selected from the list shown in Figure 7-6.
8. From the list of updates shown, select those you want to manage in the profile you are creating and click **Next** to move to the next window, which is shown in Figure 7-7. If you leave a check box unchecked, it is not included in the profile. If a check box is disabled, the update is provided by a third-party provider and is not available via download from IBM.

![Update Manager Create New Profile wizard - download the updates](image)

9. Select the check box on this window to download updates once profile creation is complete.

You do not need to download updates now. You might choose not to download updates now if you have configured a scheduled job to download updates regularly and automatically.

**Note:** To download updates from IBM later, after the profile has been created, right-click the profile name in IBM Director Console and select **Download Updates from IBM.**
Once your check box selection is made, click **Next** to move to the profile summary window shown in Figure 7-8.

![Create New Profile](image)

**Figure 7-8  Update Manager Create New Profile wizard - summary window**

10. This window summarizes the profile you are about to create, including profile name, which update categories will be included, and the machine type/operating system combinations that will be managed. Any specific updates selected are also listed. Once you are satisfied with the information displayed here, click **Finish** to complete the wizard. The new profile is
displayed under Update Manager in the Tasks pane of the IBM Director Console next to the individual update icon ( ).

If you selected the “Yes, download updates when I finish creating this profile” check box in the previous window, you are presented with the standard Scheduler job option dialog to determine when the updates should be downloaded, as shown in Figure 7-9.

![Download Updates from IBM...](image)

**Figure 7-9**  Update Manager - download updates now or schedule for later
11. Click **Execute Now** to begin a job that downloads the selected updates from IBM immediately. The standard Execution History window opens (see Figure 7-10) to show the status of the job.

**Important:** All updates for the machine type and operating system combinations selected in step 6 on page 417 are downloaded, regardless of the specific updates selected in step 8 on page 420. This latter step selects the updates that will be managed by the Update Manager profile being created and has nothing to do with the updates that are downloaded from IBM to the local update library on the management server.

The only useful part of this window is the **Status** line near the top. Do not be concerned about the list of Not Applicable items that fill the rest of this window. This is an artifact of using the standard Execution History window to display the results of an untargeted job. Since there are no specific targets (that is, managed systems) for this job, each of the individual status lines displays Not Applicable. In addition, no systems will appear in the lower portion of the window, again because no systems have been targeted for this particular job.
Only the overall Status item at the top of the window is meaningful. This item will change to \textit{Complete} when all selected updates have been downloaded, as seen in Figure 7-11.

\begin{figure}
\centering
\includegraphics[width=0.5\textwidth]{figure711.png}
\caption{Update Manager update package download status - complete}
\end{figure}
If you are interested in the details of the download process, select **File → View Log** from the Execution History window. This opens a window that shows details of the current job. As usual, you will need to select **View → Detail → High** and **View → Dynamic Update** to make this window useful. An example of a download log window is shown in Figure 7-12. Once the task has completed successfully, close any status windows that remain open and continue to the next step.

![Download Log Window](image)

**Figure 7-12** Update Manager update package download status - details in log

12. Now that the updates have been downloaded, it is time to determine whether any managed systems require any of the updates. Running a software health check compares the versions of system software updates in a profile with the versions of the system software currently installed on target systems.

Since it is important to have accurate inventory data, it is a good idea to run an inventory collection immediately before each software health check. Once you are sure that IBM Director inventory data is current, drag and drop an Update Manager profile onto a target system or group of systems to perform...
Implementing IBM Director 5.20

the software health check on those systems and open the Software Health Check window, as seen in Figure 7-13 through Figure 7-16 on page 428.

The Profile Compliance Report has three sections:
  - A section ordered by update that lists target systems that are out-of-date for each update (Figure 7-13)
  - A section ordered by target system that lists updates that are out-of-date for each target (Figure 7-14 on page 427)
– A section ordered by update that lists updates that IBM Director could not check and the reasons why each update could not be checked (Figure 7-15 on page 428)

– A section ordered by target system that lists IBM Director Server systems and multi-node systems (Figure 7-16 on page 428), which are excluded from any static group created from this profile compliance report

Figure 7-14   Software Health Check window - ordered by target system

When a profile compliance report is generated, only the individual updates selected in step 8 on page 420 are considered for the report. All unselected updates are ignored.
If certain updates cannot be checked for compliance, these will be listed in a separate section, with the reason for the missing compliance check listed, as seen in Figure 7-15.

![Software Health Check window - updates that could not be checked for compliance](image1)

**Figure 7-15  Software Health Check window - updates that could not be checked for compliance**

If you target one or more IBM Director Servers or multi-node systems for the software health check, you will see a section at the end of the profile compliance report similar to the one shown in Figure 7-16.

![Software Health Check window - management servers are not included in static groups](image2)

**Figure 7-16  Software Health Check window - management servers are not included in static groups**
This section contains confusing text with regard to IBM Director Servers. You will see the introductory statement Systems requiring Director Server updates. It is meant to say Systems running Director Server that require updates. If any IBM Director Servers or multi-node systems are targeted by the software health check, these systems will not be included in a static group created from the profile compliance report.

IBM Director Servers are excluded from automatically created static groups in order to avoid unintentional updating of the management server itself, which could result in a reboot of the management server while it is deploying updates to other managed systems. Updates to IBM Director Servers should always be handled individually. For our recommendation on how to do this, see 7.3, “Updating the management server” on page 433.

Multi-node systems are excluded from automatically created static groups in order to avoid incomplete or inconsistent updating of individual nodes. IBM Director Server is only able to update the primary node, since this is the only managed object it sees.

**Duplicate systems:** For managed Windows systems, depending on the Network Driver Configuration settings for IBM Director Agent (twgipccf.exe), it is possible to have multiple native managed objects (NMOs) appear in the management console for a single managed system. For example, you might see a Level-2 system, as well as a Level-1 or Level-0 system.

If a software health check is run against multiple NMOs representing the same system, then this system will be listed multiple times in the profile compliance report. There is generally no harm in this, although it might seem a bit confusing.

However, if an IBM Director Server and multi-node system are discovered as two separate NMOs, they could be included in the static group created for software distribution. You must check for this and remove any management servers and multi-node systems found in the group.

13. With the profile compliance report complete, you can now create a static group of all systems requiring updates managed by the profile created in step 10 on page 421 above. To do this, select **File → Create → Static systems group** from the Software Health Check window. A static group is automatically created, which contains each system that requires at least one of the updates managed by this Update Manager profile.
The new static group is found in the Groups pane of the Management Console and in the drop-down list of available groups at the top center of the console. The group is named in the following format:

Health-[profile name]-ymmd_hhmmss

Where profile name is the name you assigned to the Update Manager profile, and yymmd_hhmmss is a date and time stamp that indicates exactly when the static group was created.

Note that this naming convention includes the date and time of creation to differentiate it from other groups created from the same profile. Figure 7-17 shows an example of such a group in the management console.

14. Before updates can be deployed to systems, appropriate software distribution packages must be created to push the updates to managed systems. To do this, select File → Create → Software distribution packages from the Software Health Check window.
This opens the Creating Software Distribution Packages and Categories window, which displays progress of this process. Using this method, software distribution packages are created only for those updates needed by one or more systems, as stated in the Profile Compliance Report. To verify completion without errors, scroll to the bottom of this window, as shown in Figure 7-18.

![Creating Software Distribution Packages and Categories](image)

*Figure 7-18  Update Manager automatically builds software distribution packages*

15. Once you have verified completion, click **Close** to close the window and return to the management console. Any software distribution packages created in the previous step are now displayed in the Tasks pane, under the Software Distribution task. One or more software distribution categories are automatically created as a containers for the packages, as shown in Figure 7-19 on page 432. The naming convention used for categories is:

\[tttt\] - [profile name]_[os]_ymmd_hhmmss

Where *tttt* is the machine type, *profile name* is the name you assigned to the Update Manager profile, *os* is the operating system running on the target system, and *ymmd_hhmmss* is a date and time stamp that indicates exactly when the static group was created. If the profile contains updates for multiple operating systems, a software distribution category will be created for each operating system in the profile.
At this point, IBM Director is ready to deploy any updates needed. To do this, simply drag and drop the newly created software distribution category onto the static group created in step 13 on page 429. In the dialog box that appears, click **Execute Now** to deploy updates to the target systems immediately or **Schedule** to perform the updates at a later time.

If there are packages for updates that do not apply to target systems, these updates are not performed. For example, if you create a software distribution category that includes both Linux and Windows drivers and drag it onto a group that contains only Windows systems, only the appropriate Windows drivers are installed. The same holds true for firmware packages. If you create a group that
contains multiple machine types, only the appropriate firmware is sent to each target system.

**Important:** If the software distribution category indicates that a reboot will take place after distribution (that is, the “Reboot at end of Category Distribution” check box is selected), then target systems in the distribution will be rebooted even if no updates are performed.

### 7.3 Updating the management server

Since you rely on your management servers to execute your system update mechanism, you should update these systems independently from other managed systems. The safest approach is definitely to update management servers manually.

**Important:** If a management server is discovered as multiple NMOs (one as Level-2 and one as Level-1 or Level-0), it is possible that a static group created from an Update Manager software health check will include the management server. You should always check to make sure that systems running IBM Director Server are not included in static groups used for software distribution. If you find a management server in such a group, right-click it and select **Remove from Group**.

However, we have found that using Update Manager and software distribution to perform these updates can be a viable option if you keep a few things in mind. First, Update Manager will exclude management servers from any static groups it creates. This should not be a problem, since we intend to update management servers one at a time.
Creating an Update Manager profile for a management server is useful, since we can generate a Profile Compliance Report to determine exactly which updates are needed by the management server. For our example, the last section of this report is shown in Figure 7-20. We see that a total of four updates are of interest.

```
<table>
<thead>
<tr>
<th>System</th>
<th>Lithium</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Host</td>
<td>lithium.nucleus.itso.ral.ibm.com</td>
</tr>
<tr>
<td>IP Address</td>
<td>9.42.170.164</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Update Name</th>
<th>Update ID</th>
<th>Update Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM eServer xSeries 236 Flash BIOS Update (Windows)</td>
<td>NRE1</td>
<td>Version 1.06 -[NRE13CA-1.06]-</td>
</tr>
<tr>
<td>IBM Hard Disk Drive Update Program (Windows)</td>
<td>FD_1</td>
<td>Version 1.19 -[FD_119-1.19]-</td>
</tr>
<tr>
<td>IBM xSeries 236 Diagnostics Flash Update (Windows)</td>
<td>NRYT</td>
<td>Version 1.05 -[NRYT14A-1.05]-</td>
</tr>
<tr>
<td>Broadcom NetXtreme Firmware (Windows)</td>
<td>L202</td>
<td>Version 1.20.24 -[L2024-1.20.24]</td>
</tr>
</tbody>
</table>
```

*Figure 7-20  Profile compliance report showing updates needed by the management server*
As for any other managed system, we create software distribution packages and a category for these updates, as shown in Figure 7-21. For any updates that do not reboot the target system, the process works exactly as it would for any managed system. We are now ready to distribute four updates to our management server (named Lithium).

*Figure 7-21  Software distribution ready to send updates to the management server*
As discussed previously, the order in which update packages are listed in the management console view is not necessarily the order in which they will be distributed. The four packages will actually be sent in the order shown in the software distribution category editor, which is shown in Figure 7-22.

![Software distribution category editor shows order of package delivery](image)
When our management server pushes this group of updates to itself, the process works properly until immediately after it processes the first reboot command. As seen in Figure 7-22 on page 436, this will be just after the hard disk drive update is delivered and installed. At this point, the update job fails (since the management server is rebooted) and subsequent updates are not performed. The Jobs tab in the Scheduler window shows the failed job in Figure 7-23.

![Scheduler window showing failed job](image)

Figure 7-23  Distribution of updates to management server fails after first reboot
If we look at the details of this job (shown in Figure 7-24), we see that the first three updates were performed successfully (marked by arrows in the figure) and the job is marked Incomplete at this point. The fourth package was not sent because the management server was being rebooted.

Figure 7-24 Details of a software distribution job run against the management server
Since we know exactly how far the distribution got, we can finish the process in a second pass. The only package left to distribute is the Broadcom firmware update, so we open the software distribution category and drag that single package onto our management server. This update also requires a reboot, so as soon as the package is delivered and installation completes, our management server is rebooted again. Figure 7-25 shows that after the management server comes back online, the Jobs tab of the Scheduler window confirms that this final update was performed successfully.

![Scheduler Window](image)

Figure 7-25   The Broadcom firmware update has completed successfully

To confirm that all updates have been installed successfully, we perform a Profile Compliance Report. In preparation for performing the report, we obtain a fresh inventory collection. Then we drop the Update Manager profile containing the four updates we just deployed onto our management server. The report shows that our management server no longer needs any of the updates.

### 7.4 Update Manager and software distribution

As we have described above, Update Manager works closely with Software Distribution to provide a comprehensive system update mechanism. Concurrent with the addition of Update Manager, Software Distribution has been enhanced
to allow distribution of packages to additional managed object types. Software Distribution can now deploy packages to the following managed object types:

- Level-0 Tier Managed Objects (TMOs): These are discovered systems that do not have IBM Director Agent or IBM Director Core Services installed, and are represented by a TMO icon ( ) in IBM Director Console.

- Level-1 TMOs: These are systems that have IBM Director Core Services installed, and are represented by a TMO icon ( ) in IBM Director Console.

- Level-2 Native Managed Objects (NMOs): These are systems that have IBM Director Agent installed, and are represented by various NMO icons ( and ) in IBM Director Console.

- BladeCenter chassis Physical Platform Managed Objects (PPMOs): These are BladeCenter Management Modules and Advanced Management Modules, and are represented by chassis icons ( ) in IBM Director Console.

- BladeCenter server PPMOs: These are individual blade servers, and are represented by physical platform icons of their BMCs ( ) in IBM Director Console.

- BladeCenter switches: These are managed as SNMP devices, and are represented by special icons that resemble their hardware ( and ) in IBM Director Console.

- BladeCenter pass-through modules are not represented in IBM Director Console. To deploy a Software Distribution package to a pass-through module, drag the package onto the BladeCenter chassis icon.

### 7.4.1 Software health check

We have found that a Software Health Check will produce differing results, depending on whether it is initiated from Update Manager or Software Distribution. The reason for this is that different assumptions are made based on which tool generates the report.

If a software health check is initiated from an Update Manager profile (that is, by dragging an Update Manager profile onto a target system or group of systems in the management console), a Profile Compliance Report is generated. However, if a software health check is initiated from the Software Distribution task (that is, by right-clicking a software distribution package or package category), a Current Health Report is generated. These two reports represent different information.

**Profile Compliance Report**

This report lists each system that is targeted by the drag-and-drop operation and each update that is managed by the Update Manager profile (selected in step 8 on page 420). As described in step 12 on page 425, there are multiple sections
of this report. The key thing to remember is that all targeted systems and all managed updates are listed, whether or not a given system needs any updates or a given update is needed by any system. The top portion of a Profile Compliance Report is shown in Figure 7-26.

![Software Health Check](image1.png)

**Figure 7-26  Top few lines of a Profile Compliance Report**

**Current Health Report**

This report is not targeted against specific systems, so it includes information about the Software Distribution packages selected and whether the firmware or software in them is present on any managed system that has been discovered by the management server. For each package selected, this report will list each system that has the firmware or software installed and whether it is out of date. The top portion of a Current Health Report is shown in Figure 7-27.

![Software Health Check](image2.png)

**Figure 7-27  Top few lines of a Current Health Report**
You can generate a current health check from Software Distribution by right-clicking a package or category and selecting **Perform Health Check**. If you have previously generated a report, you can view the latest report by right-clicking a package or category and selecting **View Health Check Report**.

At the time of this writing, there is a bug in the Software Distribution code that acts as follows: If you attempt to **View Health Check Report** before one has been performed, a Software Health Check Log window opens that states **Please wait while running compliance check**, but the compliance check never completes, as shown in Figure 7-28. This is not a serious issue, since you can simply close this window and perform the health check. Once the initial check is performed, View Health Check Report works as expected.

![Software Health Check Log](image)

*Figure 7-28  Software Distribution bug - Software Health Check never completes*

**Both reports**

Managed objects must have the subject firmware and software installed in order for them to show up in either report. If a managed system does not have the firmware or software contained in the packages or managed by the profile, it is not listed, even if the package could be sent to the system. For example, if a managed system has an RSA II adapter present, but does not have appropriate drivers installed, both reports will exclude this system from consideration.

## 7.5 Important considerations

Now that we have discussed what you can do and how you do it with Update Manager, it is important to establish a few basic expectations for this new tool. We also highlight certain design issues that might not be obvious without careful examination of the tool. Some of these issues can lead to unintended results, even unsupported system configurations, if not considered when using Update Manager.
7.5.1 Update Manager needs supervision

Update Manager should not be relied upon to keep systems up to date without careful regular maintenance. If you create a single profile for all managed systems and simply use the Select All button to add all updates to the profile, you should plan on running into serious problems at some point.

It is important to monitor the list of updates in the IBM Director updates library. As new updates become available you must add them to appropriate profiles and remove old versions of the updates. Update Manager will not do this automatically.

The order in which packages are sent to systems by Software Distribution is the order in which they appear in the Package Category Editor and not necessarily in the order of their display in the management console, which is alphabetic. This is important, since getting packages out of order in a Software Distribution category can result in systems receiving older versions of updates last. The end result of this can be that back-level code is deployed, even though everything looks fine on the surface.

This is one reason why we suggest setting up individual Update Manager profiles for each machine type being managed. It is much easier to verify the installation order and currency of packages in a short list of updates meant for a single machine type than a full list of all updates for all systems being managed.

It is a good idea to ensure that only the latest version of an update is included in any Update Manager profile, unless there is a good reason to include multiple versions of the update. Update Manager will not automatically select the latest update for a given system. In fact, it will not even add the latest update to a profile automatically. You must regularly inspect and edit Update Manager profiles to ensure that the updates that they manage are the ones that you intend. Maintaining your profiles in this manner will also help ensure that you do not push back-level updates to systems.

**ServeRAID and Update Manager**

In addition to the issues of currency and installation order discussed in the previous section, ServeRAID firmware and drivers present further potential for misconfiguration through Update Manager. In order to configure IBM ServeRAID adapters and to receive events and alerts from them, various pieces of firmware and software must be installed:

- ServeRAID adapter firmware
- ServeRAID adapter drivers
- ServeRAID Manager software (stand-alone)
- ServeRAID Manager software (IBM Director extension)
It is critically important that the version of each component listed is compatible with all other components installed on any system. In addition, the stand-alone version of ServeRAID Manager and the IBM Director ServeRAID Manager extension should not be installed on the same system.

Unfortunately, Update Manager does not understand or consider any of this. You must evaluate packages that contain ServeRAID firmware, drivers, applications, and IBM Director extensions to make sure that the versions you deploy to any system are compatible (that is, supported).

7.5.2 It is called Update Manager for a reason

Update Manager is used to update system BIOS, firmware, and drivers, and not for initial installation. If a particular driver is not already installed, an Update Manager Profile Compliance Report will not let you know that the driver is missing. It looks only at software that is already installed and found in the IBM Director inventory database.

If you need to push drivers or other IBM software packages (such as IBM Director Agent) to systems that do not already have a previous version of the software installed, you may be able to use Software Distribution to perform the initial installation. For system updates that are downloaded in the proper format from IBM, as well as IBM Director Agent and IBM Director Core Services software, you can use IBM Update Assistant to import the updates and create Software Distribution packages that can be pushed out to managed systems. For other software, such as third-party applications or Microsoft security updates, you will need to use Software Distribution Premium Edition, which is a fee-based extension to IBM Director (see 6.7.3, “Software Distribution Premium Edition” on page 405, for more about this).

7.5.3 Static groups have a short half-life

The static groups created from Update Manager Profile Compliance Reports and Software Distribution Current Health Reports have limited usefulness, since they are accurate only at the moment in time that they are created. They become inaccurate as soon as updates are deployed to any system in the group.

For this reason, we recommend creating these static groups only if you intend to deploy updates immediately. In addition, we recommend deleting any static groups created for this purpose as soon as one or more updates have been deployed to any members of the group.

For more information about Profile Compliance Reports and Current Health Reports and how they compare to one another, see 7.4, “Update Manager and software distribution” on page 439.
7.5.4 Package categories should be cleaned up

As with static groups, Software Distribution categories created from Update Manager Software Compliance Reports should be deleted as soon as they have been used. The rationale for this is very similar to that described for static groups. These particular Software Distribution categories are themselves a type of static group of update packages, which are based on criteria that were true at a given moment in time.

When you create Software Distribution packages from a Profile Compliance Report, any update noted in the report as being out of date on any system in the report will be exported to a package and placed in a category. Once you apply this type of Software Distribution category to any systems needing an update contained in the category, you effectively change the results that would be contained in the Profile Compliance Report if it were regenerated. This, in turn, would result in a change in the Software Distribution packages and categories that would be created from the new report.

For example, if we perform a Software Compliance Report that tells us two updates are needed on system A, then use the File → Create → Software distribution packages option from the report window. Packages are created only for the two updates needed by system A. If we successfully distribute the Software Distribution category to system A, then run the Software Compliance Report again, we would see that no updates are required for any systems. In this case, we cannot create Software Distribution packages from the report, since no updates are required.

7.5.5 Rules for success with Update Manager

In summary, when working with Update Manager and Software Distribution, we recommend that you follow these basic rules:

- Create an Update Manager profile for each machine type.
- Inspect and edit Update Manager profiles regularly.
- Include only the latest version of a given update in a profile.
- Create static groups only when ready to deploy updates.
- Remove management servers and multi-node systems from static groups.
- Delete static groups as soon as update distribution is complete.
- Update all management servers and multi-node systems independently.

7.6 Adding undiscovered machine types

It is possible to add undiscovered IBM machine types to an Update Manager profile. Information about IBM machine types is found in the following text file on
the management server (assuming IBM Director Server installation using default settings on a Windows system):

c:\Program Files\IBM\Director\data\updatePlatforms.txt

This file is fully documented. Systems are listed as shown in Example 7-1. To add a system type that already exists in this file to an Update Manager profile, delete the #- characters in the first column of the line containing the desired machine type, operating system, and platform type.

**Example 7-1   A portion of the updatePlatforms.txt file**

<table>
<thead>
<tr>
<th>System Type</th>
<th>Machine Type</th>
<th>Operating System</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000</td>
<td>IBM System x3650</td>
<td>Windows 2000</td>
<td>x32</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>IBM System x3650</td>
<td>Windows 2003</td>
<td>x32</td>
</tr>
<tr>
<td>Windows NT</td>
<td>IBM System x3650</td>
<td>Windows NT</td>
<td>x32</td>
</tr>
<tr>
<td>Windows PE</td>
<td>IBM System x3650</td>
<td>Windows PE</td>
<td>x32</td>
</tr>
<tr>
<td>Windows XP</td>
<td>IBM System x3650</td>
<td>Windows XP</td>
<td>x32</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>IBM System x3650</td>
<td>Windows Vista</td>
<td>x32</td>
</tr>
</tbody>
</table>

To add a system type that does not appear in this file, add a new line containing information in the following format:

Description : Machine Type : Operating System : Platform

An edited version of a portion of this file is shown in Example 7-2.

**Example 7-2   An edited version of the same updatePlatforms.txt file**

<table>
<thead>
<tr>
<th>System Type</th>
<th>Machine Type</th>
<th>Operating System</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 2000</td>
<td>IBM System x3650</td>
<td>Windows 2000</td>
<td>x32</td>
</tr>
<tr>
<td>Windows 2003</td>
<td>IBM System x3650</td>
<td>Windows 2003</td>
<td>x32</td>
</tr>
<tr>
<td>Windows NT</td>
<td>IBM System x3650</td>
<td>Windows NT</td>
<td>x32</td>
</tr>
<tr>
<td>Windows PE</td>
<td>IBM System x3650</td>
<td>Windows PE</td>
<td>x32</td>
</tr>
<tr>
<td>Windows XP</td>
<td>IBM System x3650</td>
<td>Windows XP</td>
<td>x32</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>IBM System x3650</td>
<td>Windows Vista</td>
<td>x32</td>
</tr>
<tr>
<td>Undiscovered Type</td>
<td>Nonexistent System</td>
<td>Windows 2003</td>
<td>x64</td>
</tr>
</tbody>
</table>

The exact text in the description area does not matter. However, you must include -[xxxx]- (where xxxx is a four-digit number representing the actual machine type) in the machine type area in order to get the system to show up in the Update Manager profile. Also, you must specify a recognized operating system. If the operating system text is not recognized, the line is ignored and Update Manager will not show the system in its list.

Finally, if the platform text is not “x32,” it will be appended to the operating system by Update Manager in order to differentiate between systems of a single machine type that are running multiple operating systems. For example, you can...
see in the highlighted area of Figure 7-29 that the operating system is listed as Windows 2003 x64.

After editing and saving the updatePlatforms.txt file, Update Manager makes appropriate changes to the list of systems available for a profile, as seen in Figure 7-29. This change is dynamic and does not require a restart of the management server. Note that we added a made-up system to the list for clarity.

If you make a mistake editing the updatePlatforms.txt file and your entry cannot be interpreted by Update Manager, a warning message is added to TWGRas.log each time you launch the Update Manager New Profile wizard.

Use this ability to prepare for systems that are not yet part of the managed environment. This might include systems that have been ordered, but have not yet been deployed, as well as systems in the environment that are not being managed by IBM Director.
You could create an Update Manager profile for these systems and then use this profile to check the IBM Director updates library for updates, download matching updates from IBM, and view update details for these systems. Obviously, you will not be able to perform a software health check, nor will you be able to deploy updates using Software Distribution until IBM Director has discovered and performed an inventory collection on these systems. Alternatively, you could export updates from an Update Manager profile using the `exportprof` command (see 7.8.3, “The exportprof command” on page 457) to perform manual updates on systems not managed by IBM Director.

### 7.7 Update Manager events

It is possible to configure an event action plan to alert you of various Update Manager events by using the new `Director → Update Manager` event filters. Update Manager events occur after any of the following conditions:

- An update is downloaded successfully.
- An update fails to download.
- A profile setting changes.
- A profile is deleted.
If you select the Update Manager check box in the Event Filter Builder tree, as shown in Figure 7-30, the event filter will process all of the event types that are specified in the Update Manager subtree.

![Event Filter Builder showing event types for Update Manager](image)

You can also choose to select specific event types that are displayed under the Update Manager node in the Event Filter Builder tree. The event filter will process only the event types that you select. The event types available for Update Manager are summarized in Table 7-1.

Table 7-1  Update Manager event details

<table>
<thead>
<tr>
<th>Event type</th>
<th>Event text</th>
<th>Severity</th>
<th>Category</th>
<th>Extended attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download failed</td>
<td>Update Manager Download Failed One event is generated after a download has completed with failures</td>
<td>Harmless</td>
<td>Alert</td>
<td><em>Profile name</em> is the name of the profile used to download the updates.</td>
</tr>
</tbody>
</table>
Implementing IBM Director 5.20

For a detailed discussion of using event action plans see Chapter 12, “Event management” on page 675.

7.8 DIRCLI commands for Update Manager

A few new simple commands have been added to the DIRCLI command line arsenal for Update Manager. This section provides details on each of the new commands.

7.8.1 CLEANLIB command

Any Update Manager profile can be removed once it is no longer needed. However, all updates associated with the profile remain in the updates library on the management server. The `cleanlib` command is used to remove updates associated with removed profiles from the updates library.

There are no arguments or switches for this command. Simply enter `cleanlib` at the command prompt on the management server. All updates no longer associated with any Update Manager profiles are deleted from the updates library.

<table>
<thead>
<tr>
<th>Event type</th>
<th>Event text</th>
<th>Severity</th>
<th>Category</th>
<th>Extended attributes</th>
</tr>
</thead>
</table>
| New updates downloaded| Update Manager New Updates Downloaded One event is generated for each profile download, not for each update downloaded | Harmless | Alert    | ✧ *Profile name* is the name of the profile used to download the updates.  
 ✧ *Severity* indicates the severity of the most critical update. |
| Profile modified      | Update Manager Profile Modified   | Harmless | Alert    | *Profile name* is the name of the profile that was modified or deleted. |

For a detailed discussion of using event action plans see Chapter 12, “Event management” on page 675.
You might want to create a scheduled job to run this command on a regular basis. To do this, create a Process Task to run the command (see Figure 7-31) and use Scheduler to configure a repeating job to execute the Process Task. This is documented in the figures that follow.

![Figure 7-31 A simple Process Task used to run the CLEANLIB command](image1)

Test the newly created Process Task by dragging it onto a management server and clicking **Execute Now**. Details of its execution are shown in Figure 7-32.

![Figure 7-32 Job execution details show successful execution of a DIRCLI command](image2)
Once the Process Task has been tested, it can be executed on a regular basis by creating a Scheduler job. Set up the repeating nature of the job as shown in Figure 7-33.

![Figure 7-33 New Scheduled Job set to repeat weekly](image)
Add the Process Task you just created as the only task to perform for this job, as shown in Figure 7-34.

![Figure 7-34](image)

*Figure 7-34 New Scheduled Job runs Process Task automatically*
Select all management servers as targets for this job, as shown in Figure 7-35.

Figure 7-35  New Scheduled Job targets the management server
Select any job options that you prefer before saving the job. It is a good idea to have jobs generate events upon completion, as shown in Figure 7-36. This way, jobs can be added to event action plans and IBM Director Event Logs.

![New Scheduled Job](image)

**Figure 7-36  New Scheduled Job generates event upon completion**
The job is displayed in the Jobs tab of the Scheduler window, with details of its execution presented in the Status pane of the window, as shown in Figure 7-37.

IBM Director Scheduler will now keep the local updates library from filling up with old, unwanted updates. Each week Scheduler will execute the `cleanlib` command on the management server.

### 7.8.2 IMPORTUP command

The `importup` command is used to import individual or UpdateXpress System Pack updates from the file system into the updates library on the management server.

**Importing individual updates**

You might need to use the `importup` command to import individual updates if you receive updates on a CD or download them from a third party.
Importing an individual update involves importing these components of the update:

- The metadata:
  - The XML descriptor file
  - The readme file
  - Any available change history
- The installable unit that contains the code fix

First, copy the proper files (all of the available components from the bulleted list above) into a temporary directory on the management server. Then, on the management server, enter the following command:

```
dircli importup \tmpdir/\update_name.xml
```

Where `\tmpdir` is the path to the temporary directory holding the files, and `\update_name.xml` is the name of the XML descriptor file for the update.

The destination directory for importing the components is fixed and cannot be changed. The updates library on the IBM Director Server is located at:

```
c:\Program Files\IBM\Director\data\UpdateLib
```

**Importing UpdateXpress System Pack updates**

Exactly the same process is used to import an UpdateXpress System Pack update using the `importup` command. The resulting import is treated as an update bundle by Update Manager.

When performing the import, specify the UpdateXpress System Pack XML file only. The `importup` command analyzes the XML to determine that an UpdateXpress System Pack is specified. The `importup` command imports all of the XML files, readme files, change history files, and installable unit (IU) files for all of the updates in the bundle that are described in the XML file. The `importup` command also imports the XML file, the readme file, and the change history file for the UpdateXpress System Pack into the updates library.

When performing an import of this type of update, if one of the components or updates in the UpdateXpress System Pack is missing, the import will fail.

### 7.8.3 The exportprof command

Use the `exportprof` command to export the updates in an update profile to any directory in your network file system. To export updates to a file system, issue the `exportprof` command:

```
dircli exportprof profile_name -d F:\my_updates_directory
```
Where *profile_name* is the name of the profile from which you are exporting updates and F:\*my_updates_directory* is the fully qualified path to your destination directory.

Exporting a profile copies the metadata (the XML file, the readme file, and the change history when available) and the installable unit (IU) for each update in the profile to the directory specified. The update also remains in the updates library.

**Note:** If you are exporting an update bundle profile containing an UpdateXpress System Pack, and intend to use the UpdateXpress System Pack to update systems outside of IBM Director, you must also export the individual update profile containing the installation tool for the UpdateXpress System Pack. We recommend that you export the installation tool to the same directory to which you export the UpdateXpress System Pack.
IBM Electronic Service Agent

Electronic Service Agent (eSA) is a software tool that monitors hardware events and transmits system inventory of IBM systems information to IBM. It is available on IBM Systems platforms as a stand-alone tool, but for System x and BladeCenter platforms eSA is also available as an IBM Director extension for both Windows and Linux.

This chapter covers eSA in detail, paying particular attention to installing, configuring, and enrolling systems for use with eSA:

- 8.1, “Overview” on page 460
- 8.2, “Installation” on page 462
- 8.3, “Configuration” on page 465
- 8.4, “Enroll systems” on page 477
8.1 Overview

Electronic Service Agent (eSA) for System x and IBM BladeCenter is a no-charge software tool that resides on your IBM servers to monitor events and transmit system inventory information to IBM.

eSA is available as a standalone tool or as an extension to IBM Director. In this chapter we focus on the Electronic Service Agent extension for IBM Director.

eSA has two core functions, and with these functions eSA can monitor, track, and capture system hardware errors and inventory:

- **Automatic hardware problem reporting**
  eSA monitors System x and BladeCenter servers for hardware errors. Hardware errors that meet certain criteria for criticality are automatically reported to IBM. Problems typically reported include Predictive Failure Analysis (PFA) based events, power failures, system overheating (as detected by the service processor), and RAID drive failures.

- **Inventory collection**
  eSA also administers hardware and software inventory collections, and reports inventory changes to IBM. All information sent to IBM is stored in a secure IBM database and used for improved problem determination.

8.1.1 How Electronic Service Agent works

It works as follows:

1. An event is generated when a hardware error exceeds a preset threshold.
2. Electronic Service Agent sends a service request to IBM.
3. The service request is forwarded to the call management system for the machine’s country. Details sent with the service request include unique identifiers, system machine type, serial number, machine name (as displayed in IBM Director), company, contact person, location details, and other useful inventory and diagnostic information.
4. IBM responds to the Electronic Service Agent by returning a service request number, branch number, and country code.
5. Electronic Service Agent generates an event using the information from IBM. This event, together with the service request information, is recorded in IBM Director’s Event Log and History tab of the targeted systems configuration notebook.
Transmission of data
Electronic Service Agent sends information from the IBM Director management server when a Service request is generated and when transmitting inventory data to IBM. The process for transmission of data is shown in Figure 8-1.

8.1.2 Implementing Electronic Service Agent

Implementing Electronic Service Agent is divided into three stages.

1. Installing Electronic Service Agent
   This must be installed on all IBM Director management servers and IBM Director consoles.

2. Configuring Electronic Service Agent
   Setting up your company specific information, default users, and locations.

3. Enrolling systems for Electronic Service Agent
   Each supported managed system must be enrolled before any automated service requests and electronic information can be transmitted to IBM.
8.1.3 Obtaining Electronic Service Agent

Electronic Service Agent for System x Version 5.0 is an extension for IBM Director and can be downloaded from:

http://www.ibm.com/support/electronic

To download the code, follow these steps:
1. From the left-hand navigation bar, click **Electronic Service Agent**.
2. Click **Download Service Agent**.
3. Click **System x**.
4. Click **Director Extension - Windows** or **Director Extension - Linux**.
5. You can download additional documentation such as user guides and readme files from the Reference Guides section.

8.2 Installation

Electronic Service Agent is installed on IBM Director management server and IBM Director Console. The IBM Director extension version of eSA is not installed on managed systems, as the Level-1 or Level-2 IBM Director Agent provides the mechanism for capturing hardware alerts and providing inventory information to eSA.

8.2.1 Installing on Windows Systems

To install on Windows:

2. Select the installer language, follow the usual prompts, and accept the license agreement.
3. The Communications Charges window opens. Electronic Service Agent is provided at no charge by IBM for System x and IBM BladeCenter systems. However, customers are responsible for any communication changes associated with Internet or dial-up connection to IBM. Click Yes to accept the license agreement and continue, as shown in Figure 8-2.

![Electronic Service Agent (TM) for xSeries](image)

**Figure 8-2  Electronic Service Agent communication charges agreement**

4. The InstallShield wizard copies associated files and prompts you to view the readme file. Click Yes if you want to view the readme now or click No if you want to view the file later. The readme file is saved in the following location, provided that you installed IBM Director in the default install path:

```
C:\Program Files\IBM\Director\classes\com\ibm\eservice\readme.txt
```

5. The InstallShield wizard completes and you are prompted to restart the system.

**8.2.2 Installing on Linux systems**

These instructions assume that you are using an X11 window manager to perform the actual installation. The setup program is an X application.

To install Electronic Service Agent on your IBM Director Server:

1. Log in as the user root.
Important: Do not use the su command to become the user root, as eSA will not install properly.

2. Download the binary as described in 8.1.3, “Obtaining Electronic Service Agent” on page 462.

3. Change to the directory where you stored the installation program and run the following command, where eSA_install.bin is the binary file that you downloaded.

   ./eSA_install.bin

4. At the Electronic Service Agent Setup panel, click Next to continue with the setup program.

5. If you accept the terms and conditions of the license agreement, click Yes to continue with the setup program.

6. Click Finish to complete the installation.
8.3 Configuration

Once Electronic Service Agent is installed you can access the Electronic Service task icon ( ) from the Tasks section of the IBM Director console, as shown in Figure 8-3.

Figure 8-3  Electronic Service Agent console task

The steps are:

1. Double-click the **Electronic Service** task or right-click the task and click **Open**.

**Note:** If you drag the Electronic Service task to a managed system and have not run the setup wizard, the Electronic Service Agent Setup wizard starts automatically.
2. The Electronic Service Agent Setup Wizard opens, as shown in Figure 8-4. Click **Next** to configure.

*Figure 8-4  Electronic Service Agent setup wizard*
3. The Electronic Service Agent country selection window opens, as shown in Figure 8-5. Select your country or region from the drop-down menu. Click Next.

**Important:** Ensure that your country details are correct, as eSA will use this information when generating services requests and for dialer information if you are using a modem to provide Internet connectivity.

*Figure 8-5  Electronic Service Agent country or region selection*
4. The Electronic Service Agent connection window opens, as shown in Figure 8-6. Select either the **Modem** or **Internet** radio button. Click **Next**.

![Electronic Service Agent Setup Wizard](image)

*Figure 8-6  Electronic Service Agent connection wizard*

If you selected **Modem** in step 4, skip to step 7 on page 471. Otherwise continue with step 5 on page 469.
5. The Proxy configuration wizard starts and you are prompted to enter proxy information if the management server requires a proxy server to access the Internet. If you do not use a proxy server to access the Internet, leave the **Use Proxy** box unchecked. A sample configuration window is shown in Figure 8-7.

![Electronic Service Agent Proxy configuration wizard](image)

*Figure 8-7  Electronic Service Agent Proxy configuration wizard*
6. Click **Test Connection** to verify that the management server can access the Internet and establish a connection to IBM. You should see a window similar to Figure 8-8. Verify that the Internet connection tests successfully. Click **OK** to continue. Skip to step 9 to configure company details.

![Figure 8-8  Electronic Service Agent Internet connection test](image)
7. The Dialup configuration wizard starts and you are prompted to select the modem and dialup information for the management server to access the Internet. Select the appropriate region and city, and insert any dialing prefixes before the number in the Number to Dial section if required to access an external line. A sample configuration window is shown in Figure 8-9.

![Electronic Service Agent dialup configuration wizard](image)

*Figure 8-9  Electronic Service Agent dialup configuration wizard*
8. Click **Test Connection** to verify that the management server can access the Internet through the modem. You should see a window similar to Figure 8-10. Verify that the Internet connection tests successfully. Click **OK** to continue.

![Modem Connection Test](image)

*Figure 8-10  Electronic Service Agent modem connection test*
9. The company details window opens, as shown in Figure 8-11. Configure your company details and ECI ID if appropriate and click **Next** to continue.

**Note:** The Enterprise or ECI ID field is optional. Your company may have an Enterprise number or an ECI ID that is used for customer identification and unique service terms and conditions. Your purchasing team may be able to provide an Enterprise number, and your help desk may be able to provide an ECI ID. ECI ID is also known as ESC+ID, or an ECCO ID.

*Figure 8-11  Electronic Service Agent company details*
10. The default user configuration window is displayed, as shown in Figure 8-12. Configure the default user as the primary contact person within your organization. Click **Next** to continue.

![Electronic Service Agent default contact person](image)

*Figure 8-12  Electronic Service Agent default contact person*
11. The default location configuration window is displayed. Configure the default location as the primary location for the majority of your managed systems. A sample window is shown in Figure 8-13. Click **Next**.

*Figure 8-13  Electronic Service Agent default location*
12. The Electronic Service Agent setup wizard completes, as shown in Figure 8-14. Click **Finish** to save the user setting and exit the wizard.

![Electronic Service Agent Setup Wizard](image)

**Figure 8-14  Electronic Service Agent complete**

The eSA Configuration window opens and you can review and modify your settings. You can also access three new tabs, which were not accessible during the initial configuration:

- **Scheduler**
  Allows you to schedule when inventory information is sent to IBM.

- **Inventory**
  Allows you to specify the type of inventory data sent to IBM.

- **Advanced tab**
  Allows you to specify users who can access data collected by eSA over the Web.
8.4 Enroll systems

Once you have installed and configured Electronic Service Agent, you must enable (enroll) each of your managed systems for Electronic Service before the agent can perform information-gathering operations and send service requests to IBM. The following steps show you how to enroll managed systems for eSA:

1. Drag and drop the Electronic Service task icon ( ) to a managed system or right-click a managed system and select **Electronic Service**.

**Tip:** You can review your settings at any time by double-clicking the Electronic Service task icon ( ) or right-clicking the task and click **Open**. This can be useful if you want to add additional contacts, locations, or change connectivity settings.

**Note:** You can only enroll Level-1, Level-2, or IBM BladeCenter chassis managed systems, and you can only enroll one system at a time. Systems eligible for the Electronic Service Agent are located in the dynamic group *Electronic Eligible systems.*
2. The Electronic Service Agent configuration window opens on the System tab, as shown in Figure 8-15. Enroll the managed system by enabling the **Enable for Electronic** check box.
3. Click the **Services** tab, which will allow you to enable or disable eSA services for the managed system, as shown in Figure 8-16.

![Electronic Service Agent Configuration: Lithium](image)

**Figure 8-16  Electronic Service Agent Services tab**

**Base Services**

- Inventory service reports system hardware and software inventory to IBM periodically.

- Optional Service Request service reports system faults to IBM automatically.

- You may disable or temporarily suspend the service request.

- [ ] Service Requests enabled

- [ ] Diagnostics enabled
4. Click the **Contact/Location** tab, which allows you to select the contact person and location for the managed system, as shown in Figure 8-17. You can also create additional users and locations from this tab.

*Figure 8-17  Electronic Service Agent Contact/Location tab*
5. Skip the PMR and History tabs and select the **Test** tab. Click **Apply**. You should now be able to click **Enroll System**, as shown in Figure 8-18.

**Tip:** To click the Enroll System button, you must **Apply Changes** first. If the changes have not been applied or the system has already been enrolled for eSA the Enroll System button will be disabled. If the Test Service Request button is disabled, then the system is not enrolled for Electronic Service or enrollment is in still in progress.

![Figure 8-18   Electronic Service Agent Test tab](image)

6. Click the **History** tab to verify that the managed system has enrolled successfully. This may take a few minutes depending on the type and speed of your Internet connection.
7. Optionally, click **Test Service Request**, and the Service Request window is displayed, as shown in Figure 8-19.

![Service Request Test](image)

Figure 8-19  **Electronic Service Agent test service request**

8. Optional: Verify the Service request is successful and click **OK** to continue.
9. Optional: Click the **PMR** tab, as shown in Figure 8-20. You can view detailed information of the Problem Management Report (PMR) by clicking an event in the PMR Event log.

*Figure 8-20  Electronic Service Agent PMR tab*
10. Optional: Click the **History** tab, as shown in Figure 8-21. You can view detailed information of the history by clicking an event in the History event log.

![Electronic Service Agent Configuration: Lithium](image)

*Figure 8-21  Electronic Service Agent History tab*

8.4.1 Event filters

Installing the Electronic Service Agent adds a number of event filters for use with Event Actions Plans (EAPs), which can be used to notify you of electronic service requests or issues. These filters can be very useful for managing internal notification of service requests to your help desk or support staff. Refer to 12.4.2, “Event Type tab” on page 696, for more information about Electronic Service events and filters.

For more information refer to the *IBM Electronic Service Agent for xSeries Version 5.0 - Director Extension User’s Guide*, which is included with the installation package.
IBM PowerExecutive

Today’s power and thermal demands of systems are placing strains on customer data centers and IT infrastructure. PowerExecutive is designed to ease this strain by enabling customers to monitor and reallocate power resources as needed.

PowerExecutive uses a combination of software, hardware, and firmware to enable monitoring of power and thermal characteristics of systems with the ability to cap (limit) power on supported platforms.

This chapter covers the PowerExecutive extension for IBM Director, paying particular attention to installing and managing systems to achieve greater thermal efficiencies within the data center.

- 9.1, “Overview” on page 486
- 9.2, “Installation” on page 489
- 9.3, “Using PowerExecutive” on page 491
9.1 Overview

IBM PowerExecutive enables customers to measure, track, and control system power consumption. The console interface can help customers understand how power is used within the data center, and provides the insight required to optimize servers and their workloads for the optimal performance.

IBM PowerExecutive enables customers to monitor actual power usage and thermal loading information of systems. This gives customers the ability to accurately predict and trend power consumption, enabling:

- Reduced infrastructure required for redundancy
- More systems installed with less power requirements
- Lowering overall data center capital and operation costs
9.1.1 PowerExecutive communication

PowerExecutive communicates directly with the Management Module on the IBM BladeCenter chassis or the BMC service processor on IBM System x servers. PowerExecutive also maintains its own Apache Derby database (separate from the IBM Director database) containing power objects and historical data. Refer to Figure 9-1 for a diagram of the PowerExecutive communication process.

![PowerExecutive communication diagram](image)

**System x physical platform objects**

PowerExecutive communicates with the BMC service processor in System x servers. It does not communicate with an RSA II adapter if installed. You must ensure that the BMC IP address is configured correctly for out-of-band communication to PowerExecutive. In-band management of the BMC through the operating system IPMI driver is not supported.

You must launch PowerExecutive tasks against an System x BMC physical platform object (PPO). You cannot drag a PowerExecutive tasks to Level-0, Level-1, or Level-2 managed systems associated with the BMC PPO.
Important: At the time of writing it was not possible to add a BMC PPO to the IBM Director console if an RSA II PPO already exists. As PowerExecutive only communicates with the BMC, you must delete the RSA II PPO and add the BMC PPO if you want to take advantage of PowerExecutive functions.

As RSA II and BMC PPOs cannot coexist on the same management server, you will be unable to manage RSA II adapters through IBM Director if you want to manage your systems with PowerExecutive.

Blade server physical platform objects
PowerExecutive communicates with the IBM BladeCenter Management Module even when managing individual blades. As PowerExecutive only communicates with the IBM BladeCenter Management Module, there is no need to configure the BMC IP address on the blade server.

You can launch PowerExecutive tasks against the IBM BladeCenter Management Module or individual blade PPO. However, you cannot drag PowerExecutive tasks to Level-0, Level-1, or Level-2 managed systems associated with the blade PPO.

Important: It is not possible to configure the BMC IP address on a blade. All BMC information for blades is passed through the IBM BladeCenter MM. Although you can set the IP address of the BMC in the BIOS setup, the settings are not saved and you cannot connect to the IP address.

At the time of writing, installing the IPMI driver and OSA mapping layer software on blades interfered with the BMC PPO in IBM Director. When the BMC is discovered in-band through the IPMI driver, IBM Director will try to communicate directly with the BMC, which is not supported, and the IP address will be inaccessible. After initial discovery, the BMC PPO will go offline, as out-of-band management communication will fail with no response from BMC.

This also causes issues in PowerExecutive, as two entries appear for the Blade PPO—one reported by the MM and the other reported by the BMC through the IPMI driver, which shows up in other systems with a communicate error.

We suggest that you do not install the IPMI driver and OSA mapping layer on blades if you plan on using PowerExecutive.
9.2 Installation

PowerExecutive is installed on IBM Director management servers and consoles. It is not installed on Level-0, Level-1, or Level-2 agent systems. After PowerExecutive is installed, the PowerExecutive icon ( ) appears as a task in the Tasks pane of the IBM Director Console.

Important: PowerExecutive requires the BladeCenter Management extension for IBM Director 5.x even if you do not plan on managing IBM BladeCenter systems.

9.2.1 Obtaining PowerExecutive

PowerExecutive is available as an extension for IBM Director or as a standalone tool. Both versions can be downloaded from:


Note: At the time of writing, PowerExecutive 1.1 was the latest version. However, Version 2.0 is due for release.

9.2.2 Installing on Windows Systems

This section provides instructions for installing PowerExecutive on IBM Director management servers and consoles that are running Windows. PowerExecutive talks directly to the BMC or IBM BladeCenter Management Module, there is no need to install PowerExecutive on managed systems you plan on monitoring.

The steps required to install PowerExecutive are:

1. Run the executable code that you downloaded in the previous section.
2. Follow the usual prompts and accept the license agreement.
3. A Warning window appears indicating that the installation will stop the IBM Director Server service, as shown in Figure 9-2. Click Next.

**Note:** If you are installing PowerExecutive Server and IBM Director Server is running, then this installation stops the IBM Director service before the PowerExecutive installation begins. Ensure that you are not running any critical tasks before installing PowerExecutive. After the PowerExecutive installation is completed, the IBM Director service is restarted.

![PowerExecutive warning window](image)

*Figure 9-2  PowerExecutive warning window*

4. Click **Install** to start the installation process.

5. After copying files and restarting the IBM Director Server service, the installation wizard completes. Click **Finish**.

### 9.2.3 Installing on Linux systems

This section provides instructions for installing PowerExecutive on systems that are running Linux. To install PowerExecutive on a Linux system:

- On systems where you are installing PowerExecutive Server, enter the following command:
  
  ```bash
  rpm -Uv pwrexec_install-server.rpm
  ```

  Where `pwrexec_install-server.rpm` is the binary file you downloaded.
On systems where you are installing PowerExecutive Console, enter the following command:

```
rpm -Uv pwrexec_install-console.rpm
```

Where `pwrexec_install-console.rpm` is the binary file you downloaded.

**Note:** If you are installing PowerExecutive Server and IBM Director Server is running, then this installation stops the IBM Director service before the PowerExecutive installation begins. Ensure that you are not running any critical tasks before installing PowerExecutive. After the PowerExecutive installation is completed, the IBM Director service is restarted.

### 9.3 Using PowerExecutive

Once PowerExecutive is installed, the PowerExecutive Task icon and sub-task icons are added to the IBM Director Console Tasks pane, as shown in Figure 9-3.

![Figure 9-3 PowerExecutive Console task as sub-tasks](image-url)
You can launch the PowerExecutive tasks in a number of ways:

- Double-click the PowerExecutive icon to open the task for all supported systems and power objects.
- Drag and drop the PowerExecutive task icon or sub-task icon to an individual supported system PPO.
- Right-click a supported system PPO and click **PowerExecutive** or a PowerExecutive sub-task.
9.3.1 PowerExecutive Console

The PowerExecutive Console is divided into three panes. These major console areas are shown in Figure 9-4.

The major consoles are:

- Navigation pane
  
  The left side of the PowerExecutive Console contains the navigation pane, which displays power objects currently targeted by PowerExecutive in a tree.
structure. Refer to Table 9-1 on page 494 for information about power object status.

**Table 9-1  Navigation pane icon descriptions**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="monitoring" /></td>
<td>Object is currently being monitored.</td>
</tr>
<tr>
<td><img src="image" alt="monitoring_disabled" /></td>
<td>Object has monitoring disabled or suspended.</td>
</tr>
<tr>
<td><img src="image" alt="not_present" /></td>
<td>Object is not present in the IBM BladeCenter chassis.</td>
</tr>
</tbody>
</table>

**Detail pane (Current Data)**

The upper right side of the window contains the detail pane, which uses a table to display information about the power object that is currently selected in the tree structure (Figure 9-5). If you select an IBM BladeCenter power domain, all power objects in the domain are displayed, as shown in Figure 9-6 on page 495). If Power Managed Systems is selected in the tree structure, information about all power objects is displayed as shown in Figure 9-7 on page 495.

<table>
<thead>
<tr>
<th>Power-Managed Systems ▶ Nitrogen</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Current Data</strong></td>
</tr>
<tr>
<td>Field</td>
</tr>
<tr>
<td>Time</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Power Meter</td>
</tr>
<tr>
<td>Metering Level</td>
</tr>
<tr>
<td>Power Savings Supported by Platform</td>
</tr>
<tr>
<td>Nameplate Watts (ac)</td>
</tr>
<tr>
<td>Average Watts (ac)</td>
</tr>
<tr>
<td>Average Watts (dc)</td>
</tr>
<tr>
<td>Pcap (dc)</td>
</tr>
<tr>
<td>Pmax (dc)</td>
</tr>
<tr>
<td>Pmin (dc)</td>
</tr>
<tr>
<td>°C Ambient</td>
</tr>
<tr>
<td>°C Exhaust</td>
</tr>
<tr>
<td>Effective CPU Speed (%)</td>
</tr>
<tr>
<td>Last Policy</td>
</tr>
</tbody>
</table>

**Figure 9-5  Detail pane (Current Data) for an individual power object**

**Tip:** You can verify whether a power object supports power capping by verifying the Metering Level field. Power objects that do not support capping display a metering level of Monitoring Only if the object supports power monitoring, or None if the object does not support power monitoring.
## Chapter 9. IBM PowerExecutive

### Figure 9-6  Detail pane (Current Data) for an IBM BladeCenter power domain

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Bay</th>
<th>Power Meter</th>
<th>Metering Level</th>
<th>P...</th>
<th>Average Watts (dc)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Module 1</td>
<td>Power Module</td>
<td>1</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>78</td>
</tr>
<tr>
<td>Power Module 2</td>
<td>Power Module</td>
<td>2</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>78</td>
</tr>
<tr>
<td>Hydrogen</td>
<td>Blade Server</td>
<td>1</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>140</td>
</tr>
<tr>
<td>Helium</td>
<td>Blade Server</td>
<td>2</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>140</td>
</tr>
<tr>
<td>Silicon</td>
<td>Blade Server</td>
<td>3</td>
<td>Version 1.0</td>
<td>Monitoring Only</td>
<td>No</td>
<td>190</td>
</tr>
<tr>
<td>Phosphorus</td>
<td>Blade Server</td>
<td>4</td>
<td>Version 1.0</td>
<td>Monitoring Only</td>
<td>No</td>
<td>99</td>
</tr>
<tr>
<td>Sulphur</td>
<td>Blade Server</td>
<td>5</td>
<td>Version 1.0</td>
<td>Monitoring Only</td>
<td>No</td>
<td>85</td>
</tr>
<tr>
<td>Chlorine</td>
<td>Blade Server</td>
<td>6</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>140</td>
</tr>
<tr>
<td>N/A</td>
<td>Blade Server</td>
<td>7</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>I/O Module 1</td>
<td>I/O Module</td>
<td>1</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>45</td>
</tr>
<tr>
<td>I/O Module 2</td>
<td>I/O Module</td>
<td>2</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>45</td>
</tr>
<tr>
<td>Management M...</td>
<td>Management M...</td>
<td>1</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>25</td>
</tr>
<tr>
<td>N/A</td>
<td>Management M...</td>
<td>2</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>I/O Module</td>
<td>3</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>I/O Module</td>
<td>4</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>I/O Module</td>
<td>7</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>I/O Module</td>
<td>8</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>I/O Module</td>
<td>9</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>N/A</td>
<td>I/O Module</td>
<td>10</td>
<td>N/A</td>
<td>N/A</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>Media Tray 1</td>
<td>Media Tray</td>
<td>1</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>10</td>
</tr>
<tr>
<td>Midplane 1</td>
<td>Midplane</td>
<td>1</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>10</td>
</tr>
<tr>
<td>Fan Pack 1</td>
<td>Fan Pack</td>
<td>1</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>30</td>
</tr>
<tr>
<td>Fan Pack 2</td>
<td>Fan Pack</td>
<td>2</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>30</td>
</tr>
<tr>
<td>Fan Pack 3</td>
<td>Fan Pack</td>
<td>3</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>30</td>
</tr>
<tr>
<td>Fan Pack 4</td>
<td>Fan Pack</td>
<td>4</td>
<td>None</td>
<td>N/A</td>
<td>No</td>
<td>30</td>
</tr>
</tbody>
</table>

Summary for Power... 119.56

### Figure 9-7  Detail pane (Current Data) for an individual power object

<table>
<thead>
<tr>
<th>Name</th>
<th>Data Collection</th>
<th>Average Watts (ac)</th>
<th>°C Ambient</th>
<th>°C Exhaust</th>
<th>BTUs/hr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nitrogen</td>
<td>Enabled</td>
<td>257</td>
<td>24.0</td>
<td>36.0</td>
<td>876.9</td>
</tr>
<tr>
<td>Carbon</td>
<td>Enabled</td>
<td>265</td>
<td>25.0</td>
<td>31.0</td>
<td>964.2</td>
</tr>
<tr>
<td>BladeCenter</td>
<td>Enabled</td>
<td>2248</td>
<td>24.0</td>
<td>32.5</td>
<td>7670.2</td>
</tr>
</tbody>
</table>

Summary for... 2770 9451.2
Trend pane (Trend Data)

The lower right side of the window contains the Trend Data pane, which provides a graphical (Figure 9-8) or tabular (Figure 9-10 on page 497) view of power data over time about the power object that is currently selected in the tree structure.

![PowerExecutive Show Trend Data as chart](image)

**Figure 9-8**  PowerExecutive Show Trend Data as chart

![PowerExecutive chart legend](image)

**Figure 9-9**  PowerExecutive chart legend
Figure 9-10   PowerExecutive Show Trend Data as table

For more information about the Trend Data pane refer to 9.3.6, “Show trend data” on page 506

**PowerExecutive toolbar**

The PowerExecutive toolbar contains the functions that are described in Table 9-2.

Table 9-2   PowerExecutive toolbar

<table>
<thead>
<tr>
<th>Toolbar icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Suspend icon" /></td>
<td>Suspend data collection. Suspends data collection on IBM BladeCenter chassis or supported server. Data collection cannot be suspended for individual power objects within a chassis.</td>
</tr>
<tr>
<td><img src="image2" alt="Resume icon" /></td>
<td>Resume data collection. Resumes data collection on an IBM BladeCenter chassis or supported server. The toolbar icon is available only when data collection has been suspended</td>
</tr>
<tr>
<td><img src="image3" alt="Manage Trend icon" /></td>
<td>Manage Trend data. Opens a dialog to control how often and how much historical trend data is written to the database and when trend data is deleted. Refer to 9.3.3, “Manage trend data” on page 499.</td>
</tr>
</tbody>
</table>
9.3.2 PowerExecutive data descriptions

PowerExecutive presents data in a variety of formats. Details of the data types displayed in graphical or tabular format are listed in Table 9-3. For more information about all data descriptors for IBM BladeCenter chassis and System x servers refer to the users guide *IBM Systems IBM PowerExecutive Installation and User's Guide Version 2.0*.

Table 9-3  Trend data descriptions

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time at which the current data was collected.</td>
</tr>
<tr>
<td>Average Watts (AC)</td>
<td>Average Watts (AC).</td>
</tr>
<tr>
<td>Average Watts (DC)</td>
<td>Average Watts (DC).</td>
</tr>
<tr>
<td>Pcap (DC)</td>
<td>Current power cap.</td>
</tr>
<tr>
<td>Upper percentile (DC)</td>
<td>An upper percentile of 90% sets the upper end of the range to the smallest power value such that at least 90% of the hits in the power histogram are below that value. The default value is 100%</td>
</tr>
</tbody>
</table>
9.3.3 Manage trend data

You can manage trend data using the Edit menu of PowerExecutive, or by clicking the Manage Trend Data toolbar icon.

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower percentile (DC)</td>
<td>A lower percentile of 10% sets the lower end of the range to the largest power value such that at least 90% of the hits in the power histogram are above that value. The default value is 0%</td>
</tr>
<tr>
<td>Pmax (DC)</td>
<td>Maximum possible power cap.</td>
</tr>
<tr>
<td>Pmin (DC)</td>
<td>Minimum possible power cap.</td>
</tr>
<tr>
<td>°C ambient</td>
<td>The current ambient (inlet) temperature.</td>
</tr>
<tr>
<td>°C exhaust</td>
<td>The current exhaust (outlet) temperature</td>
</tr>
<tr>
<td>Effective CPU speed</td>
<td>The average CPU speed as a percentage.</td>
</tr>
<tr>
<td>Events</td>
<td>Description of event.</td>
</tr>
</tbody>
</table>
Historical trend data is written to the PowerExecutive database. You can control how often and how much historical trend data is written to the database, and when trend data is deleted, as shown in Figure 9-11. The Manage Trend Data dialog is useful if you want to change the amount of data collected and database size for PowerExecutive.

![Manage Trend Data](image)

**Figure 9-11 PowerExecutive Manage Trend data**

### 9.3.4 Manage power

You can manage power using the Edit menu of PowerExecutive or by clicking the Manage power toolbar icon ( ).

The power cap (Pcap) value, specified in Watts, is the value to which a given blade or server will be capped by IBM BladeCenter MM or System x BMC (when the firmware supports capping). You can apply the power policy immediately by clicking **Apply Now**, or save the power policy as a task for quick access later. The saved power policy is added as a sub-task under Manage Power in the Tasks pane of the IBM Director console. You can also delete previous power policies you have saved by selecting the power policy name from the policy name drop-down box and clicking **Delete**.
Understanding capping

Applying a power policy to a system that supports capping limits the amount of power a system can request. If the system attempts to request more power than the current Pcap, the CPU is throttled. The maximum allowable range for Pcap is defined by Pmin and Pmax, which is dynamically calculated by the BMC or IBM BladeCenter MM. Refer to Figure 9-12.

Tip: PowerExecutive 1.1 saves the power policy name incorrectly as “Enter a new policy or select an existing policy”. If you try to save additional policies, the duplicate policy name error message is displayed. To delete the policy you must select Enter a new policy or select and existing policy name drop-down box and click Delete. This is due to be fixed with PowerExecutive 2.0.

Table 9-4 PowerExecutive chart descriptions

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power (Watts) CPU Utilization</td>
<td>Current power consumption and CPU utilization</td>
</tr>
<tr>
<td>Nameplate power</td>
<td>Measured value at maximum configured system</td>
</tr>
<tr>
<td>Pmax</td>
<td>Maximum capping allowed based on system configuration</td>
</tr>
</tbody>
</table>
PowerExecutive will dynamically change Pmin and Pmax as directed by the BMC or IBM BladeCenter MM based on changes to system configuration. Hardware modifications such as hot-swap PCI adapter insertion or removal raises or lowers Pmin and Pmax, as shown Figure 9-13.

**Figure 9-13** PowerExecutive dynamic cap changed based on hardware changes

**Figure 9-14** PowerExecutive chart legend
Power policies
From the Create or Edit Power Policy window, you can specify the new policy in one of three ways:

► Power limit range

For a single system, or for a group of similar systems for which the same Pcap value is appropriate, you can specify a Pcap value either by adjusting the slider or by entering the desired value directly in the text box, as shown in Figure 9-15.

Figure 9-15  PowerExecutive Set a power cap in Watts
Percentage of power limit range

Specify Pcap as a percentage between Pmin and Pmax rather than a specific Pcap value. This is particularly useful in the case of a group of unlike systems where a specific Pcap value is not appropriate. Refer to Figure 9-16.

Example 9-1  Specifying Pcap as a percentage

System1: Pmin = 400 Watts, Pmax=500 Watts
System2: PMin = 600 Watts, PMax=800 Watts

Specifying a Pcap of 50% will result in:
System1: Pcap = 450 Watts (50% of the difference between Pmin & Pmax)
System2: Pcap = 700 Watts (50% of the difference between Pmin & Pmax)

Figure 9-16  PowerExecutive Set a power cap as a percentage of Pmax
Compute power limit based on historical data

Specify a historical period to examine, using the drop-down list box, and a power-limiting goal, using the slider. A power-limiting goal of 0% corresponds to a Pcap value equal to the maximum observed power over the period of interest. A negative percentage corresponds to a Pcap value lower than the observed maximum, and a positive percentage corresponds to a Pcap value greater than the observed maximum (allowing room for the power consumption to grow without incurring throttling). Refer to Figure 9-17.

![Manage Power Window]

Figure 9-17  PowerExecutive Set a power cap based on trend data

9.3.5 Derate power

The derating factor is the percentage of the static maximum power that is used when estimating the power in use for Blade or System x servers. Derate power is only supported on systems that are not power meter enabled, and for all other power objects such as IBM BladeCenter blowers. The derating factor does not apply to power objects when information about the actual power consumed is available from the IBM BladeCenter MM or System x BMC.
The derate power factor is applied to the label power to estimate the power-in-use (average Watts), and can be useful for derating power objects that may not be consuming nameplate power consumption. Refer to Example 9-2.

**Example 9-2  PowerExecutive Derate power**

8678 HS20 Blade (No power metering enabled)
Nameplate Watts = 140
Derate Power Factor = 100
Average Watts = 140

Changing Derate Power Factor = 50 (%)
Average Watts = 70

You can derate power using the Edit menu of PowerExecutive, or by clicking the Derate power toolbar icon ( ).

You can set the derating power factor for an individual power object. By default, the derating power factor is 100%, which means that the reported power is not derated at all. Refer to Figure 9-18.

![Derate Power](image)

*Figure 9-18  PowerExecutive Derate power*

### 9.3.6 Show trend data

The Trend data pane is always displayed, but you can switch the displayed format between a graphical (chart) or tabular view. Click the Show Trend Data as chart toolbar icon ( ) or click Show Trend Data as table ( ) to view the trend data in the desired format.

**Modifying the time range**

You can modify the time range display for both the chart and table view by selecting predefined or custom time ranges from the time range drop-down box.
The predefined data ranges are:

- Last hour
- Last 12 hours
- Last 24 hours
- Last 48 hours
- Last week
- Last 2 weeks
- Last month
- Last 6 months
- Last year

If you select Add/change custom interval custom range, the Custom Trend Data Interval dialog opens, as shown in Figure 9-19. Select the time range and click **OK**. The custom time interval cannot be selected from the time range drop-down box.

![Custom Trend Data Interval dialog](image-url)
Show Trend Data as chart

The Trend Data chart consists of two sub-charts, as shown in Figure 9-20, which are always displayed. The upper chart displays power data and the lower chart displays temperature and CPU throttling data. The two sub-charts share the same time axis. A legend identifying the various chart elements appears above the upper sub-chart. The check boxes in the legend allow you to control the display of individual chart elements to be enabled or disabled.

![Figure 9-20  PowerExecutive Show Trend Data as chart](image)

The upper chart displays average power (AC and DC) over time, along with the Pcap, Pmax, and Pmin. Upper and lower percentiles for power-in-use can be optionally set, with the range between the upper and lower percentile displayed in light grey.

An upper percentile of 90%, for example, sets the upper end of the range to the smallest power value such that at least 90% of the hits in the power histogram are below that value. A lower percentile of 10% sets the lower end of the range to the largest power value such that at least 90% of the hits in the power histogram are above that value. The default upper percentile is 100%, corresponding to maximum power. The default lower percentile is 0%, corresponding to minimum power. The default power display of power in use, minimum and maximum power in use, and event information.
Show trend data as table

The Trend Data table consists of two sub-tables, as shown in Figure 9-22, which are always displayed. The upper table displays power data and the lower chart displays temperature and CPU throttling data. The two sub-tables share the same time axis.

<table>
<thead>
<tr>
<th>Time</th>
<th>Average Watts (ac)</th>
<th>Average Watts (dc)</th>
<th>Fcap (dc)</th>
<th>Upper Percentile (dc)</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/13/06 9:44:27 AM</td>
<td>206</td>
<td>204</td>
<td>510</td>
<td>207</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:45:27 AM</td>
<td>272</td>
<td>191</td>
<td>510</td>
<td>207</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:46:26 AM</td>
<td>259</td>
<td>178</td>
<td>510</td>
<td>183</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:46:27 AM</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:47:26 AM</td>
<td>308</td>
<td>223</td>
<td>510</td>
<td>255</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:47:27 AM</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:48:26 AM</td>
<td>340</td>
<td>252</td>
<td>510</td>
<td>255</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:48:27 AM</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:49:26 AM</td>
<td>342</td>
<td>253</td>
<td>510</td>
<td>255</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:50:26 AM</td>
<td>342</td>
<td>254</td>
<td>510</td>
<td>255</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:51:26 AM</td>
<td>344</td>
<td>255</td>
<td>510</td>
<td>255</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:51:27 AM</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:52:26 AM</td>
<td>344</td>
<td>265</td>
<td>510</td>
<td>261</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:53:26 AM</td>
<td>344</td>
<td>255</td>
<td>510</td>
<td>261</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:54:25 AM</td>
<td>316</td>
<td>230</td>
<td>510</td>
<td>261</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:54:26 AM</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td></td>
</tr>
<tr>
<td>12/13/06 9:55:25 AM</td>
<td>260</td>
<td>180</td>
<td>510</td>
<td>189</td>
<td></td>
</tr>
</tbody>
</table>

Figure 9-22  PowerExecutive Show Trend Data as table
Customizing displayed trend data

You can modify what trend data information is displayed in the Trend Data pane chart or table view by selecting or de-selecting items, as shown in Figure 9-23.

<table>
<thead>
<tr>
<th>Power (Upper Chart):</th>
<th>Temp/CPU (Lower Chart):</th>
<th>Events (Either Chart):</th>
</tr>
</thead>
<tbody>
<tr>
<td>☑ Average (ac)</td>
<td>☐ Upper Percentile (dp)</td>
<td>☑ Exhaust Temperature</td>
</tr>
<tr>
<td>☑ Average (uc)</td>
<td>☑ Lower Percentile (dp)</td>
<td>☐ Critical</td>
</tr>
<tr>
<td>☑ Pcap (dc)</td>
<td>☐ Pmax/Pmin (dc)</td>
<td>☑ Ambient Temperature</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☑ Warning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☑ Effective CPU Speed (%)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☐ Harmless</td>
</tr>
</tbody>
</table>

Figure 9-23  Customizing trend data

9.3.7 PowerExecutive console tasks

PowerExecutive adds the following tasks and sub-tasks (Figure 9-24) to the IBM Director console, which can be executed against support PPOs:

- Data Collection
  - Disable: disables data collection for the specified power object
  - Enable: enables data collection for the specified power object

Figure 9-24  PowerExecutive console Tasks

- Cap
  - Maximum Performance: sets Pcap to Pmax (maximum capping level) for the specified power object
  - Min Power: sets Pcap to Pmin (minimum capping level) for the specified power object
  - <Saved power policies>: sets Pcap to the value specified in the power policy

- Monitor Only
  Disables power capping support for the specified power object
Note: At the time of writing, the only way to turn on monitoring for a power object that was set to Monitor Only was to execute a Cap task against the object. The Cap task would fail. However, the task would re-enable monitoring for the specified power object.
Chapter 10. IBM Virtualization Manager

IBM Virtualization Manager is a follow-on to the Virtual Machine Manager (VMM) extension for IBM Director. It allows you to manage both physical and virtual machines from a single IBM Director management console. You can use Virtualization Manager to provide various views of your environment and monitor and status and performance of virtual and physical machines.

In this chapter we discuss our experience using IBM Virtualization Manager to integrate with our VMware VirtualCenter environment. We managed physical and virtual machines running Windows Server 2003 and Red Hat Enterprise Linux.

The topics in this chapter are:

- 10.1, “Overview” on page 514
- 10.2, “Components” on page 515
- 10.3, “Installation and configuration” on page 519
- 10.4, “One tool, two interfaces” on page 529
- 10.5, “Event filters” on page 559
- 10.6, “Event actions” on page 559
- 10.7, “DIRCLI commands” on page 565
10.1 Overview

IBM Virtualization Manager is an extension to IBM Director that allows you to discover, visualize, and manage both physical and virtual systems from a single console. Virtualization Manager simplifies management of both VMware and Microsoft Virtual Server environments. A technology preview for Xen management is included, but we did not explore this area. Virtualization Manager also integrates with and complements VMware VirtualCenter, linking together management for physical and virtual resources.

Note: The terminology applied to the resources of different virtualization environments varies by vendor. Virtualization Manager uses the term farm to refer to a container of hosts and their associated virtual servers within which you can perform migrate tasks. This terminology was in sync with the same term used by VMware in VirtualCenter 1.x. However, with the release of VirtualCenter 2.0, VMware no longer uses the term farm. Although it has additional implications beyond the scope of this book, the VMware term cluster now encompasses the Virtualization Manager notion of a farm.

10.1.1 Features

Virtualization Manager has a number of features that are useful in managing any IT environment that includes virtual machines. Using Virtualization Manager, you can visualize and navigate virtual to physical resources and relationships, seeing information in either a tree or a graphical topology view. You can check the status and resource utilization of physical hosts and virtual machines and see events that have occurred on both.

Basic functionality also includes the ability to create, delete, start, shut down, suspend, resume, and restart virtual machines, as well as add or remove physical hosts to/from farms.

You can statically migrate virtual machines on VMware, Microsoft Virtual Server, and Xen from one physical host to another. In this type of operation, the virtual machines are shut down or suspended, then migrated and powered on or resumed. Virtualization Manager can also be used to invoke VMware’s VMotion technology directly from the user interface or through automated event action plans.

If there is something you need to do that requires the vendor’s user interface, you can invoke the VMware or Microsoft Virtual Server interface directly from the management console. Virtualization Manager also includes links into the HMC for System p virtualization management.
10.2 Components

Virtualization Manager includes software components that are extensions to the corresponding IBM Director components. The Virtualization Manager extension for IBM Director includes the following software components:

- **Virtualization Manager Server**
  
  Virtualization Manager Server maintains the Virtualization Manager environment and manages all Virtualization Manager operations. Virtualization Manager Server communicates with each Virtualization Manager Agent and Virtualization Manager Console to display status and perform operations for Virtualization Manager objects. Virtualization Manager Server communicates with IBM Director Server to provide event filtering and event actions that support IBM Director event action plans that involve Virtualization Manager objects.

  Virtualization Manager Server must be installed on the management server. When you install Virtualization Manager Server, the Virtualization Manager Console extension, along with the Web interface, is installed automatically on the same system, so it can be used as a management console as well.

- **Virtualization Manager Console**
  
  Virtualization Manager Console provides the user interface extension to IBM Director Console. Virtualization Manager Console must be installed on all management consoles from which a system administrator will remotely access the management server and perform Virtualization Manager tasks using IBM Director Console.

  Virtualization Manager also includes a Web-based user interface that does not require you to have the Virtualization Manager Console installed on the Web browser system. You can access the Web-based interface that is installed on the management server, from a Web browser on any management console.

- **Virtualization Manager Agent**
  
  Virtualization Manager provides a different version of Virtualization Manager Agent for each virtualization environment that it supports. The installation program for Virtualization Manager automatically detects which virtualization application is installed, and displays the correct installation choice for the applicable version of Virtualization Manager Agent. Only one Virtualization Manager Agent can be run on a managed system at a time.

  Virtualization Manager Agent can provide support only for features that are provided by the virtualization application. For example, when Virtualization Manager Agent for VMware VirtualCenter is used, you can dynamically migrate virtual machines from one VMware ESX Server host to another. When Virtualization Manager Agents for VMware ESX Server, VMware GSX
Server, and Microsoft Virtual Server are used, only static migration is supported.

Each Virtualization Manager Agent can perform the following functions:

– Discover virtualization environments and create Virtualization Manager objects.
– Relay communication between Virtualization Manager Server and the virtualization environment.
– Translate events that are provided by the virtualization environment into events that can be used in IBM Director event action plans.

### 10.2.1 Components required for supported environments

The Virtualization Manager Server component and at least one instance of Virtualization Manager Console are required for all installations. This section describes other Virtualization Manager components and vendor software that needs to be installed for each supported virtualization environment.

**Microsoft Virtual Server environment**

If you want to use Virtualization Manager to manage a Microsoft Virtual Server environment, you will need to install the following on each Microsoft Virtual Server system to be managed:

- IBM Director Agent
- Virtualization Manager Agent for Microsoft Virtual Server

No additional components need to be installed.

**VMware ESX Server environment**

If you want to use Virtualization Manager to manage a VMware ESX Server environment, you will need to install the following on each VMware ESX Server system to be managed:

- IBM Director Agent
- Virtualization Manager Agent for VMware ESX Server

No additional components need to be installed.
VMware GSX Server environment
If you want to use Virtualization Manager to manage a VMware GSX Server environment, you will need to install the following on each VMware GSX Server system to be managed:

- IBM Director Agent
- Virtualization Manager Agent for VMware GSX Server

The VMware Virtual Machine Console should also be installed on any management console from which an administrator will remotely access the management server and perform Virtualization Manager tasks. This allows IBM Director to invoke the Virtual Machine Console against a managed GSX virtual machine.

VMware VirtualCenter environment
If you want to use Virtualization Manager to manage a VMware VirtualCenter environment, you will need to install the following on each VMware VirtualCenter Server system to be managed:

- IBM Director Agent
- Virtualization Manager Agent for VMware VirtualCenter Server

**Important:** For any VirtualCenter Server Version 1.x in your environment, you must install VMware VirtualCenter Web Services prior to installing the Virtualization Manager Agent.

The VMware VirtualCenter Client should also be installed on any management console from which an administrator will remotely access the management server and perform Virtualization Manager tasks. This allows IBM Director to open the VirtualCenter management interface to perform tasks that cannot be performed from within IBM Director Console.

For each VMware ESX Server and GSX Server managed by VirtualCenter, install IBM Director Agent, but do not install any Virtualization Manager component on these systems.

**Note:** For VMware ESX and GSX environments, we recommend that you do not install the Virtualization Manager Agent on the ESX Servers or GSX Servers. Management is performed through VirtualCenter and not directly against the hosts.
Xen Virtualization environment
If you want to use IBM Virtualization Manager to manage a Xen Virtualization environment, you will need to install the following on each managed system running Xen Virtualization:

- IBM Director Core Services (The full Level-2 Agent is not required.)
- Virtualization Manager Xen CIM provider

Hardware Management Console environment
If you want to use IBM Virtualization Manager to manage System i or System p servers under the control of a Hardware Management Console (HMC), ensure that your environment is configured correctly.

When you install Virtualization Manager Server, the Hardware Management Console extension for IBM Director Server and IBM Director Console is installed automatically. The HMC extension enables the discovery of HMCs in your environment. Then you can view the servers and associated virtual servers that are managed by the HMC.

The managed servers do not require that IBM Director Agent be installed, because IBM Director communicates with the HMC through the HMC extension.
10.3 Installation and configuration

Installation of Virtualization Manager itself is very simple. The Virtualization Manager installer detects which virtualization environment is present on the system and automatically displays the proper installation choices for the corresponding Virtualization Manager components, as shown in Figure 10-1.

![Figure 10-1  Virtualization Manager installer detects what to install](image)
When installing the Virtualization Manager Server, you can select a pair of TCP/IP ports to use for the Web server that is part of the product, as shown in Figure 10-2. The default ports (8421 and 8422) should work in most situations.

![Figure 10-2 Virtualization Manager installer allows choice of TCP/IP port pair](image)

You will need to open these two ports in firewalls between remote management consoles and the management server in order to use the browser-based portion of the Virtualization Manager user interface.
Once Virtualization Manager Server installation is complete, you can launch the Web interface directly from the installer, as shown in Figure 10-3. Alternatively, you can open the Web interface by pointing your browser to the following URL:

http://System_Name:Port_Number/ibm/console

Where System_Name is the name of the management server and Port_Number is the lower of the two consecutive port numbers you specified for the Web server to use.

Figure 10-3  Launch the Virtualization Manager Web interface from the installer
On the initial launch of the Virtualization Manager Web interface, you are presented with a welcome window, as shown in Figure 10-4. Since this is the first time Virtualization Manager has been started, there is an alert letting the user know that discovery and monitoring need to be set up.

![Initial welcome window in Virtualization Manager (with setup reminder)](image-url)
This is easily accomplished by clicking the **Set up discovery and monitoring** link on the Welcome page to open the Setup Advisor, as shown in Figure 10-5.

The Setup Advisor walks the user through initial setup, including IBM Director Console installation, system discovery and monitoring, and setup of the Virtualization Manager health summary and dashboard.
The IBM Director Console window helps get the management console installed properly. In order to launch IBM Director Console from the Virtualization Manager Web interface, the Java Runtime Environment (JRE™) must be installed. If it is not, you will see an alert box, shown in Figure 10-6, that includes a link to the Java Web Start resources page. You can download the JRE and install it without closing Virtualization Manager.
The Discovery page (shown in Figure 10-7) allows you to double-check that you have installed all of the proper Virtualization Manager components. You can click the **IBM Director Console** link to open the management console and test that Java Web Start is installed and working properly.

<table>
<thead>
<tr>
<th>Discovery</th>
</tr>
</thead>
<tbody>
<tr>
<td>To manage certain resources through Virtualization Manager, you must prepare the resources to be discovered. After you have prepared those resources, you can start to discover them.</td>
</tr>
</tbody>
</table>

Complete the following steps:

1. Ensure that you have installed the components of IBM Virtualization Manager that are required to enable discovery.
2. Discover resources by using the following instructions:
   a. Open **IBM Director Console**
   b. Complete the instructions to set up discovery preferences that enable automatic discovery of resources.
   c. Complete the instructions to manually discover any additional resources in your environment.
   d. Complete the instructions to request access to locked resources after they have been discovered.

Click Next to continue.

*Figure 10-7   Virtualization Manager Setup Advisor - Discovery*

You can also click the other links on this page to see instructions that relate to setting up system discovery and requesting access to managed systems and other resources in the management console.
The Thresholds page (shown in Figure 10-8) provides links to instructions for setting up resource monitor thresholds in IBM Director. Setting proper thresholds for CPU, memory, storage, and network utilization are important, since these will be the basis for the Virtualization Manager Health Summary window and Dashboard area. Of course, they will also be used for alerting and automated corrective actions provided by event action plans.

---

**Figure 10-8 Virtualization Manager Setup Advisor - Thresholds**

<table>
<thead>
<tr>
<th>Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Welcome</strong></td>
</tr>
<tr>
<td><strong>IBM Director Console</strong></td>
</tr>
<tr>
<td><strong>Discovery</strong></td>
</tr>
<tr>
<td><strong>Thresholds</strong></td>
</tr>
<tr>
<td><strong>Health Summary</strong></td>
</tr>
</tbody>
</table>

Complete the following steps:

1. Open *IBM Director Console*

2. Set the resource-monitor thresholds for the recommended metrics by using the following instructions:
   - CPU Usage
   - Memory Usage
   - Storage Usage
   - Network Usage

3. Verify the thresholds that you set in IBM Director Console on the *All Available Thresholds* window.

Click Next to continue.

< Back  Next >  Finish  Cancel
The Health page (shown in Figure 10-9) introduces the Virtualization Manager Health Summary view. You can click the **Health Summary** link to open this view, or access the other links for help configuring resource and threshold favorites, as well as adding performance metrics to the Virtualization Manager Dashboard view.

![Virtualization Manager Setup Advisor - Health](image)

**Figure 10-9** Virtualization Manager Setup Advisor - Health
The Summary page (shown in Figure 10-10) is the final page in the Setup Advisor and contains links to two key Virtualization Manager views. You can click one of these links to begin working in Virtualization Manager immediately, or click Finish to complete the Setup Advisor and return to the Welcome window.

Figure 10-10  Virtualization Manager Setup Advisor - Summary
Once discovery and monitoring has been set up in IBM Director, the Welcome window shows that this important initial process has been accomplished, as seen in Figure 10-11.

![IBM Virtualization Manager Welcome window](image)

**Figure 10-11  Virtualization Manager Welcome window showing initial configuration has been completed**

10.4 One tool, two interfaces

IBM Virtualization Manager provides two interfaces from which to view and manage physical and virtual resources, the IBM Director Console interface and the Virtualization Manager Web interface. This section describes each interface.
and provides examples for how you might leverage them to manage your virtualized environment.

## 10.4.1 IBM Director Console

The IBM Director Console interface provides the familiar management console view of managed systems. Use it to quickly see which resources are available and how they are related. Set up resource monitors and thresholds, along with event action plans, just as you would for other managed systems.

Several items get added to IBM Director Console when Virtualization Manager is installed. Refer to Figure 10-12 on page 531 as we discuss these additions:

- The box in the Groups (left) pane highlights the addition of the Virtualization Groups category. This is a set of groups that allow you to display any of the following in the Group Contents pane:
  - **Guest operating systems**
    A guest operating system object is a managed system that represents an operating system that is running on a virtual server and that is running IBM Director Agent. A guest operating system object is a particular type of managed system. The standard IBM Director discovery process for managed systems can discover guest operating systems. However, if a guest operating system is not running IBM Director Agent, it is not recognized as a guest operating system object in IBM Director.
  - **Hosts**
    In an Virtualization Manager environment, a host object is a system that contains resources from which virtual servers are constructed. A host object can manage multiple virtual servers and their guest operating systems.
  - **Platform Managers**
    A platform manager object can manage multiple Virtualization Manager farms (when virtual farms are supported in a particular platform manager environment). Additionally, a platform manager can manage multiple hosts and their associated virtual servers and operating systems.
  - **Virtual servers**
    A virtual server object represents a virtual server that is associated with a host system that is a supported virtualization environment on Virtualization Manager. A virtual server is the logical equivalent of a physical platform: it can be powered on and turned off through Virtualization Manager. After Virtualization Manager discovers a host, it continues the discovery process to create virtual server objects for all of the virtual servers that are associated with the host.
Virtualization systems

Describes all of the components associated with a managed system and its virtualized resources. This group is a combination of all of the above object types and is used to find and display all object types that relate to any supported virtualization environment. Displaying this group while the Virtual Systems Membership association is selected shows the hierarchy of all managed objects in all supported virtualization environments.

![IBM Director Console with boxes highlighting Virtualization Manager additions](image)

Figure 10-12  IBM Director Console with boxes highlighting Virtualization Manager additions

- The box in the Group Contents (center) pane shows an example of a managed system that is recognized as being part of a supported virtualization environment. This is evident by the Virtualization Manager icon ( ) placed immediately next to the managed system object. Any objects that are
recognized by Virtualization Manager as platform managers or hosts will
display this icon.

- The box in the Tasks (right) pane shows the Virtualization Manager task and
  its subtasks:

  - Create Virtual Farm

    A virtual farm is a container within which you can migrate virtual servers
    between hosts. A virtual farm can contain multiple hosts and their
    associated virtual servers. A Virtualization Manager virtual farm is allowed
    to contain only hosts that are being managed with the same type of
    Virtualization Manager Agent. For example, a virtual farm that contains a
    host running Virtualization Manager Agent for GSX can only contain other
    hosts that are also running Virtualization Manager Agent for GSX.

  - Create Virtual Server

    You can use the Create Virtual Server wizard in Virtualization Manager to
    create virtual servers on your host systems. The wizard guides you
    through the virtual server creation process. The wizard prompts you to
    provide information such as the system name, number of CPUs, memory,
    and storage to allocate to the virtual server. The information it requests is
    specific to the virtualization environment in which the virtual server is
    being created. In most cases, the Create Virtual Server task does not
    install an operating system. You install the appropriate operating system
    after the virtual server is created.

  - Help

    Provides access to Virtualization Manager online help and the
    Virtualization Manager Information Center (working Internet connection
    required for the latter).

  - Migrate All Virtual Servers

    You can use Virtualization Manager to migrate a single virtual server or all
    of the virtual servers on a host. You can migrate a virtual server between
    different hosts within the same virtual farm to optimize resource utilization.
    Ensure that you meet the following migration requirements:

    - Migration of virtual servers is only possible between hosts within the
      same virtual farm.

    - Both the source and the destination host must have access to a shared
      storage area network (SAN). This restriction does not apply when
      migrating virtual servers on GSX hosts with the IBM Virtualization
      Manager Agent for VirtualCenter.

    - Both the source and the destination host must have access to a shared
      communications network.
• The destination host must have enough memory to support the virtual server.

• The destination host must support the configuration version of the virtual server.

• Migration of clustered virtual servers is not supported.

• Migration of virtual servers that are suspended or in a transition state is not supported.

• Source and destination hosts must have a virtual network device with the same label.

• Virtual servers to be migrated cannot be connected to a removable device such as a CD drive or diskette drive.

• The version of a configuration file for a virtual server must be supported by the virtualization application that IBM Virtualization Manager Agent communicates with. Otherwise, the virtual server cannot be migrated.

– Migrate Virtual Server

You can use Virtualization Manager to migrate a single virtual server or all of the virtual servers on a host. The same requirements hold for migrating a single virtual server as listed above for migrating all virtual servers.

– Start Vendor Software

You can use the Start Vendor Software subtask to start the virtualization application for the targeted Virtualization Manager object. Examples of vendor software that can be started include the following:

• VMware VirtualCenter Client for a VMware VirtualCenter 1.x environment

• VMware Management Interface for a VMware ESX Server 2.x environment

• VMware Virtual Machine Console interface for a VMware GSX Server environment

• VMware Virtual Infrastructure Client for a VMware VirtualCenter 2.x and VMware ESX Server 3.x environment

• Administration Web site for a Microsoft Virtual Server environment

– View Virtual Servers and Hosts

Opens the Virtualization Manager Web interface to the Virtual Servers and Hosts page. This view enables you to see additional details about your virtual servers and hosts, such as CPU utilization, processor allocation, and memory allocation. You can toggle between the topology map view, the resource table view, or the relationship table view. You also have full
access to the other views available in the Virtualization Manager Web interface.

Notice the padlock on the system named Neptunium in Figure 10-12 on page 531. This system is our VMware VirtualCenter Server, which is considered a platform manager by IBM Director. Until we supply valid credentials to connect to the platform manager, we will not see information relevant to our virtualized environment from this system. To do this, right-click the platform manager and select **Platform Manager Management → Connect**.

Figure 10-13 shows the Connect window, where we enter a valid User ID and Password for access to the platform manager, which is a VMware VirtualCenter Server in our case. If we have changed the port over which the platform manager communicates, we must enter the proper port number as well.

![Figure 10-13 Platform manager Connect window](image)
One of the most useful features of the management console interface for Virtualization Manager is its ability to graphically represent the relationships between physical and virtual managed objects. Virtualization Manager shows at a glance the relationship between the platform manager, farms (groupings of physical hosts), physical hosts (the System x or BladeCenter servers running the hosting operating system), virtual machines, and guest instances running on the virtual machines. All of these pieces can be seen in Figure 10-14.

Figure 10-14  IBM Virtualization Manager display of virtual environments
The IBM Director Console interface is also useful in seeing status changes in real
time, such as a virtual server migration from one host to another. Figure 10-15
shows such a migration in progress, which is indicated by the migration icon ( )
in the management console.

![IBM Director Console](image)

Figure 10-15  IBM Director Console showing virtual server migration in progress (highlighted)

10.4.2 Virtualization Manager Web interface

The Web interface for Virtualization Manager adds a whole new dimension to
managing virtualization resources with IBM Director. There are a number of
views that can be displayed, depending on your requirements.

To open the Virtualization Manager Web interface from IBM Director Console,
open the IBM Virtualization Manager task in the tasks pane of the management
console, right-click View Virtual Servers and Hosts, and select Open.
To open the Virtualization Manager Web interface without IBM Director Console, point your browser to the following URL:

http://System_Name:Port_Number/ibm/console

Where System_Name is the name of the management server and Port_Number is the lower of the two consecutive port numbers that you specified for the Web server to use.

Health Summary

The Virtualization Manager Health Summary provides the ability to monitor and manage systems across multiple platforms from a single interface. The Health Summary displays a consolidated view of the health of your system resources, storage resources, and thresholds.

Specifically, the Health Summary displays information about the resources and thresholds that you select for your resource favorites and threshold favorites. In addition, you can view detailed real-time data by adding your threshold metrics to the dashboard.

The Health Summary provides the following functions:

- Checks, displays, and analyzes the status and health of resources that you specify in resource favorites and thresholds that you specify in threshold favorites.
- Displays gauges that indicate real-time data for resources and thresholds.
- Enables you to run tasks against resources in response to status changes or systems management needs.

Figure 10-16 shows the Scoreboard area of the Health Summary page. The Scoreboard displays the current health status of your favorite resources and thresholds. By viewing the overall health status in the Scoreboard, you can determine at a glance if any of your resources or thresholds need attention.
Figure 10-17 shows the Dashboard area of the Health Summary page. The Dashboard displays a real-time, graphical representation of resource usage based on IBM Director thresholds you have set. You can display this data in a variety of formats to aid in the monitoring of your resources.

![Dashboard Image]

*Figure 10-17  Virtualization Manager Dashboard*

In our example, we have chosen to use the *Dial* format to display host CPU utilization as a percentage. Each of the two dials in the display represents one of our VMware ESX Server hosts. It is very easy to see that one of the hosts is working much harder than the other, but they are both well within acceptable limits for CPU utilization.

We have chosen to use a *Bar Chart* graph to display the amount of available memory remaining on each of our two host systems. We can determine at a glance that there is substantial memory available to our virtual servers.

We have chosen to use a *Capacity Graph* to represent disk space remaining on our two hosts. Again, it is quick and easy to see exactly how much disk space has been used and how much space remains on that particular host. If you are interested in more precise information, click the Dashboard monitor of interest to activate it, and then hover the mouse over areas of interest.
Figure 10-18 shows details regarding the amount of host memory available on our host named Plutonium. By hovering the mouse over the green bar in the chart, the detail pane shows that Plutonium currently has over 9 GB of uncommitted memory.

Figure 10-18  Dashboard showing memory available on Plutonium host

Figure 10-19 shows details regarding the amount of host memory available on our host named Uranium. This host is using more memory than the other, but still has adequate uncommitted memory available.

Figure 10-19  Dashboard showing memory available on Uranium host
Figure 10-20 shows the Resource Favorites area of the Health Summary page. Resource Favorites displays selected resources that you have chosen to watch closely. You can perform actions against a resource by using the context menu. Click the resource to find details about the resource.

![Virtualization Manager Resource Favorites](image)

**Figure 10-20   Virtualization Manager Resource Favorites**

Figure 10-21 shows the Threshold Favorites area of the Health Summary page. Threshold Favorites displays selected thresholds that you have chosen to watch closely. Click the threshold to find details about the threshold. For example, you can see the metrics (real-time data) that the IBM Director threshold is currently monitoring.

![Virtualization Manager Threshold Favorites](image)

**Figure 10-21   Virtualization Manager Threshold Favorites**

For group thresholds, you can graph the metrics for all of the members in the group as well as drill down into the threshold to see which member of the group
has triggered the threshold. There are a variety of graphing methods to choose from.

**Resource Monitors**

Another useful feature of the Threshold Favorites area is to provide a way to graph IBM Director Resource Monitors that have been configured on managed systems. Clicking the symbol next to any threshold name takes you to Display Chart. Several options for charting are available.

Figure 10-22 shows a *Line Chart* that graphs CPU utilization on all six of our virtual servers. The longer we let the graph display, the more data we collect. To choose a different type of display, click one of the graph icons in the upper left corner of the display (highlighted by the box) in the figure.
Figure 10-23 shows an *Area Chart* that graphs CPU utilization on all six of our virtual servers. In this figure, you can see that hovering the mouse over a data point provides details for that particular point in the graph.
Figure 10-24 shows a *Scatter Chart* that graphs CPU utilization on all six of our virtual servers.

*Figure 10-24  Scatter chart of CPU utilization for a group of virtual servers*
Figure 10-25 shows a Table View of the data recorded for CPU utilization on all six of our virtual servers. This is data that comes out of IBM Director Resource Monitors that have been configured for each of the virtual servers.

```
<table>
<thead>
<tr>
<th>Timestamp</th>
<th>1: Antimony</th>
<th>2: Iodine</th>
<th>3: Tellurium</th>
<th>4: Xenon</th>
<th>5: Caesium</th>
<th>6: Barium</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/18/06 8:14PM</td>
<td>0%</td>
<td>1%</td>
<td>9%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>12/18/06 8:13PM</td>
<td>0%</td>
<td>1%</td>
<td>8%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>12/18/06 8:12PM</td>
<td>1%</td>
<td>1%</td>
<td>9%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>12/18/06 8:11PM</td>
<td>0%</td>
<td>1%</td>
<td>8%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>12/18/06 8:10PM</td>
<td>0%</td>
<td>1%</td>
<td>7%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>12/18/06 8:09PM</td>
<td>1%</td>
<td>1%</td>
<td>7%</td>
<td>0%</td>
<td>12%</td>
<td>1%</td>
</tr>
<tr>
<td>12/18/06 8:08PM</td>
<td>0%</td>
<td>2%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>12/18/06 8:07PM</td>
<td>59%</td>
<td>11%</td>
<td>90%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>12/18/06 8:06PM</td>
<td>18%</td>
<td>100%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>12/18/06 8:05PM</td>
<td>0%</td>
<td>1%</td>
<td>100%</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
</tr>
</tbody>
</table>
```

**Resource views**

The Virtualization Manager Web interface offers three different resource views for examining your virtualization resources: the resource table view, the topology map view, and the relationship table view.
Figure 10-26 shows the resource table view, which provides a list of the resources in your environment and offers a fully accessible view of your resources. You can see the status, type, and description of each resource. For virtual servers and hosts, the resource table view provides additional information about your resources, such as IP address, CPU usage, processor capacity or allocation, and memory capacity or allocation.
Figure 10-27 shows the topology map view, which is a graphical view of your resources and their relationships.

Figure 10-27  Virtualization Manager topology map view of virtualization resources
Figure 10-28 shows the relationship table view, which shows the relationships between the resources in your environment and offers a fully accessible view of your resource relationships. You can see the name of each resource, its type of relationship to another resource, and the related resource.

![Figure 10-28   Virtualization Manager relationship table view of virtualization resources](image)

From any of these views, you can examine the properties of any resource. Figure 10-29 on page 548 shows the properties of a platform manager—the VMware VirtualCenter Server in our environment.
### Properties for Neptunium

| Name:       | Neptunium                         |
| Status:     | OK                                |
| Type:       | Platform Manager                  |
| Description:| A platform manager manages hosts, which might be in a virtual farm. |
| System Factory IDs: | Level 2: IBM Director Agents |
| System Status: | Online                   |
| System Presence Check Setting (minutes): | 30                       |
| Granted License: | true                  |
| Secure/Unsecure supported: | true                |
| Agent Unsecured: | true                    |
| Access Denied: | false                        |
| Encryption Enabled: | false                     |
| Agent time zone offset (GMT+minutes): | GMT-500                 |
| Parents:    | Neptunium                        |
| Virtualization Object Type: | Platform Manager |
| Virtualization State: | Authenticated               |
| Virtualization ChildIds: | ITSO Farm, Production Farm |
| Preferred IPC Path: | TCP/IP: 192.168.0.93         |
| Unique System ID: | 756967a1aca21e60          |
| Available IPC Paths: | {'TCP/IP': '192.168.0.93', '192.168.0.93'} |
| TCP/IP Hosts: | {'Neptunium'}                 |
| Operating System: | Microsoft Windows Server 2003™ |
| OS Major Version: | 5                                 |
| OS Minor Version: | 2                                 |
| Agent Type:  | Agent                            |
| Agent Version: | 5.20                         |
| Agent Build Date: | December 7, 2006      |
| Agent Unsecured: | true                     |
| Access Denied: | false                        |
| Encryption Enabled: | false                     |
| Agent time zone offset (GMT+minutes): | GMT-500                 |
| Parents:    | Neptunium                        |
| Virtualization Object Type: | Platform Manager |
| Virtualization State: | Authenticated               |
| Virtualization ChildIds: | ITSO Farm, Production Farm |
| Preferred IPC Path: | TCP/IP: 192.168.0.93         |
| Unique System ID: | 756967a1aca21e60          |
| Available IPC Paths: | {'TCP/IP': '192.168.0.93', '192.168.0.93'} |
| TCP/IP Hosts: | {'Neptunium'}                 |
| Operating System: | Microsoft Windows Server 2003™ |
| OS Major Version: | 5                                 |
| OS Minor Version: | 2                                 |
| Agent Type:  | Agent                            |
| Agent Version: | 5.20                         |
| Agent Build Date: | December 7, 2006      |
| System UUID: | 459D7E5F-F0E8-8213-909A-5CD9B7C328C8 |
| Computer Name: | Neptunium                      |
| MAC Address: | {'00000080010D'}             |
| Agent Architecture: | 1a32                  |

**Figure 10-29** Virtualization Manager properties view of a platform manager
There are many other views and ways to manage virtualization resources available in the Virtualization Manager Web interface. Our recommendation is to explore liberally and configure favorites when you find views that are particularly interesting to you.

**Standard management tasks**
The Virtualization Manager Web interface offers more than management of your virtualization resources. From this interface you can see and manage your entire IBM Director managed environment.

All groups and discovered objects can be viewed, and many of the standard management tasks can be performed from the Web interface. This can be very useful if you find yourself needing to access the management console from a workstation that does not have IBM Director Console installed.

Figure 10-30 on page 550 through Figure 10-38 on page 558 provide examples of the views and tasks that can be accomplished from the Virtualization Manager Web interface that really have nothing to do with the virtualization environment.
Figure 10-30 shows the Web interface displaying all of the groups that have been configured in IBM Director Console, as well as how many objects are contained in each group. This view is equivalent to the All Groups view in IBM Director Console.
Figure 10-31 shows the Web interface displaying all managed objects that have been discovered by IBM Director Server, as well as the status, object type, and description of each object. This view is equivalent to the All Managed Objects view in IBM Director Console.

Figure 10-31  Web interface showing all managed objects
Figure 10-32 shows the Web interface displaying all of the IBM BladeCenter chassis, blade servers, and switches that have been discovered by IBM Director Server, as well as the status, object type, and description for each device. This view is equivalent to the Chassis and Chassis Members view in IBM Director Console.

*Figure 10-32  Web interface showing IBM BladeCenter chassis and chassis members*
Figure 10-33 shows the Web interface displaying all managed systems that are running IBM Director Agent. Again, this view also shows status, object type, and description for each system. This view is equivalent to the Level 2: IBM Director Agents view in IBM Director Console.

![Table showing managed systems](image)

*Figure 10-33  Web interface showing all Level-2 managed systems*
Figure 10-34 shows the Web interface again displaying all managed systems that are running IBM Director Agent. Clicking the symbol next to any managed system opens a right-click menu that can be used to perform various management tasks. This is very similar to the context-sensitive list of functions available when you right-click a managed system in IBM Director Console.
Figure 10-35 through Figure 10-38 on page 558 provide an example of using this right-click method to request access to a managed system.

Figure 10-35 shows a list of managed systems, including a locked system named Chlorine. We can use the Web interface to request access to this system, just as we can perform this task from IBM Director Console.

Figure 10-35   The managed system Chlorine is shown as locked in this view
Implementing IBM Director 5.20

Figure 10-36 shows that the symbol has been clicked for the managed system named Chlorine, displaying the management options for this particular system. We select Request Access, exactly as we would from IBM Director Console.
Figure 10-37 shows a Resource Navigator window, into which we enter credentials for an account that has administrative rights on the managed system named Chlorine. We enter these credentials exactly as we would if requesting access from IBM Director Console.

![Resource Navigator window in which credentials are entered](image)

**Figure 10-37** Resource Navigator window in which credentials are entered
Figure 10-38 shows the resulting Web interface view that indicates that we have successfully gained access to the managed system named Chlorine. Note that the status column now indicates that this system is OK, as opposed to the earlier view (Figure 10-35 on page 555), in which the status was listed as locked.
10.5 Event filters

IBM Virtualization Manager is capable of generating a number of events that can be logged or acted upon by event action plans. The events that are provided by Virtualization Manager are for Virtualization Manager objects. These events are grouped under the VSM event type in the Event Filter Builder. See Figure 10-39.

![Simple Event Filter Builder: Virtualization Manager Filters](image)

Figure 10-39  Simple Event Filter Builder showing Virtualization Manager event types

See “Virtualization Manager filters (VSM type)” on page 712 for a complete description of these event types in the Event Filter Builder.

10.6 Event actions

Virtualization Manager adds several event action templates to IBM Director Event Action Plan Builder. Virtualization Manager event actions are easily identified by the Virtualization Manager icon they use ( ), as highlighted in
Implementing IBM Director 5.20

Figure 10-40. To use these templates, from the Event Action Plan Builder window, right-click the template name and select Customize to create a custom event action.

![Event Action Plan Builder](image)

**Figure 10-40** Event Action Plan Builder showing event actions added by Virtualization Manager

### 10.6.1 Customizable event actions

Virtualization Manager provides the following event actions:

- **Add a Host to a Virtual Farm**: used to add a host to a farm by specifying the name or IP address of the host to be added and the farm name.

- **Add a Host to VirtualCenter**: used to add a host to VMware VirtualCenter by specifying the name or IP address of the host to be added, as well as login credentials (user ID and password) and port number for communicating with the VirtualCenter Server.
Manage a Host: used to perform power management actions on virtual hosts by specifying the name or IP address of the virtual host to be managed and the action to be performed. Supported actions are the following:

- **Start (Microsoft Virtual Server only):** starts Microsoft Virtual Server services on the host. You can use this event action only for hosts that are currently stopped.
- **Stop (Microsoft Virtual Server only):** stops Microsoft Virtual Server services on the host. You can use this event action only for hosts that are currently started.
- **Power off all virtual servers:** turns off all running virtual servers that are associated with a single host without an orderly shutdown of any guest operating systems.
- **Power on all virtual servers:** turns on all stopped virtual servers that are associated with a single host.
- **Resume all virtual servers:** resumes all suspended virtual servers that are associated with a single host.
- **Suspend all virtual servers:** suspends all running virtual servers that are associated with a single host.

Manage a Virtual Server: used to perform power management actions on virtual servers by specifying the name or IP address of the virtual server to be managed and the action to be performed. Supported actions are the following:

- **Power on:** The virtual server is turned on.
- **Shut down and power off (Microsoft Virtual Server only):** If the guest operating system is a Windows operating system and if Microsoft Virtual Server Additions is installed on the guest operating system, action performs an orderly shut down of the guest operating system and then turns off the virtual server.
- **Power off now:** The virtual server is turned off without an orderly shut down of its guest operating system. This will immediately stop all applications that are in use on that guest operating system.
- **Suspend:** The virtual server remains turned on, but is suspended from use.
- **Resume:** The virtual server resumes operation and is no longer suspended.
- **Restart now:** The virtual server is restarted immediately, which means that it is restarted without an orderly shut down of its guest operating system. This will immediately stop all applications that are in use on that guest operating system.
- Remove a Host from a Virtual Farm: used to remove a host from a virtual farm by specifying the name or IP address of the host to be removed and the farm name.

### 10.6.2 Migration tasks as event actions

In addition to the event actions listed above and easily identified in the Event Action Plan Builder window, the migration tasks that you create with Virtualization Manager are also available in the Event Action Plan Builder window, under the *Start a Task on the “event” System* event action template.

Complete the following steps to access the saved migration tasks under this event action template:

1. In IBM Director Console, select **Tasks** → **Event Action Plan Builder**. The Event Action Plan Builder window opens.

2. In the Actions pane, double-click the **Start a Task on the “event” System** event action. The Customize Action window opens.

   The list on the Customize Action window contains several noninteractive IBM Director tasks that can be performed on the system for which the event is generated. Any saved migration tasks are in the formats shown in Example 10-1.

   **Example 10-1  Formats of the tasks available**

   | [Migrate All Virtual Server Tasks] [Virtualization Manager] [saved_task] [Execute] |
   | [Migrate Single Virtual Server Tasks] [Virtualization Manager] [saved_task] [Execute] |

   *saved_task* is the name of the saved migration task.

3. Select the desired migration task from the drop-down list, as shown in Figure 10-41.

   ![Customize Action window with virtual server migration task selected](image)
4. Select **File → Save As**, give the event action a name, and click **OK** to save it. The new event action now shows up in the *Start a Task on the “event” System* event action template, as shown in the highlighted box in Figure 10-42.

![Figure 10-42 Customized event action to migrate a virtual server](image)

*Figure 10-42 Customized event action to migrate a virtual server*
Regular IBM Director event actions can be used in conjunction with Virtualization Manager as well. For example, you can use the *Send an Event Message to a Console User* event action template to configure an event action that will open IBM Director Message Browser on the management console when a virtual system is migrated. The message itself can be very simple. Using the generic message &Text on &System provides all of the pertinent information about the migration, as seen in Figure 10-43 and Figure 10-44.

![Figure 10-43 Message Browser alert showing a virtual server migration has begun](image1)

Figure 10-43 and Figure 10-44 show the IBM Director Message Browser displaying two event notifications for a virtual server migration that was performed by the event action configured above. The first message is received when the migration is initiated. The second message is added to the Message Browser when the migration completes.

![Figure 10-44 Message Browser alert showing a virtual server migration has completed](image2)

Of course, you can add additional detail to the message, such as the time that the migration occurred (&Time) using IBM Director event data substitution.
variables. For more about these useful placeholders, see “Event data substitution variables” on page 732.

10.7  DIRCLI commands

The IBM Director command-line interface (DIRCLI) can be used with IBM Virtualization Manager to perform the following tasks without using IBM Director Console:

- List Virtualization Manager objects and their attributes
- Create and delete virtual farms.
- Start and stop hosts in a virtual farm (Microsoft Virtual Server only).
- Create, register, unregister, and delete virtual servers.
- Migrate one virtual server or migrate all virtual servers on a host.
- Change the attributes of a virtual server.
- Obtain or revoke credentials to a platform manager (VirtualCenter only).

DIRCLI provides command-line support for Virtualization Manager in two ways. There is a group of Virtualization Manager commands that have been added to DIRCLI through the vsm bundle. In addition, a group of noninteractive Virtualization Manager tasks can be executed via DIRCLI with the RunTask command.

10.7.1 Virtualization Manager commands

Virtualization Manager commands are provided in the vsm bundle of DIRCLI. Table 10-1 lists the commands that are supported.

<table>
<thead>
<tr>
<th>DIRCLI vsm command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>help</td>
<td>Lists all of the Virtualization Manager commands included in the vsm bundle in dircli, as well as their associated parameters.</td>
</tr>
<tr>
<td>list</td>
<td>Lists all of the Virtualization Manager commands included in the vsm bundle in DIRCLI, as well as their associated parameters.</td>
</tr>
<tr>
<td>lsvsm</td>
<td>Lists all Virtualization Manager objects defined in IBM Director.</td>
</tr>
<tr>
<td>chvsmauth</td>
<td>Enters or revokes credentials for a platform manager.</td>
</tr>
<tr>
<td>mkvsmfarm</td>
<td>Creates a virtual farm.</td>
</tr>
</tbody>
</table>
10.7.2 Noninteractive Virtualization Manager tasks

DIRCLI can be used to execute the Virtualization Manager noninteractive tasks that the Virtualization Manager extension provides. You can list all noninteractive IBM Director tasks, not just those supported by Virtualization Manager, with the DIRCLI server/ListNoninteractiveTasks command.

DIRCLI starts noninteractive tasks with the RunTask command. Use the DIRCLI server/ListNoninteractiveTasks command to see the status of a noninteractive task that you run with DIRCLI.

Table 10-2 lists the noninteractive tasks that Virtualization Manager adds to DIRCLI. Any of these actions can be executed using DIRCLI.

Note: Virtualization Manager does not add power operation tasks, but updates those listed in the table to work with virtual servers.

<table>
<thead>
<tr>
<th>DIRCLI vsm command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>chvsmfarm</td>
<td>Modifies a virtual farm by adding or removing a host.</td>
</tr>
<tr>
<td>chvsmhost</td>
<td>Changes the Virtualization Manager object attributes of a host.</td>
</tr>
<tr>
<td>mkvsmvs</td>
<td>Creates a virtual server with the specified attributes. The name must be less than or equal to 80 characters in length.</td>
</tr>
<tr>
<td>chvsmvs</td>
<td>Changes the Virtualization Manager object attributes of a virtual server.</td>
</tr>
<tr>
<td>chvsmvssreg</td>
<td>(Virtualization Manager Agent for ESX, GSX, and Microsoft Virtual Server only) Registers or unregisters a virtual server.</td>
</tr>
<tr>
<td>mkvsmmigratetask</td>
<td>Creates a task for migrating virtual servers. This task can migrate one virtual server or migrate all virtual servers on a host.</td>
</tr>
</tbody>
</table>

Table 10-2 Virtualization Manager noninteractive tasks in DIRCLI

<table>
<thead>
<tr>
<th>Virtualization Manager object for task</th>
<th>Command name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform manager</td>
<td>[Platform Manager Management][Discover Virtual Farms] [Platform Manager Management][Disconnect]</td>
</tr>
<tr>
<td>Virtualization Manager object for task</td>
<td>Command name</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Virtual farm</td>
<td>[Start...]</td>
</tr>
<tr>
<td></td>
<td>[Stop...]</td>
</tr>
<tr>
<td></td>
<td>[Delete Permanently...]</td>
</tr>
<tr>
<td>Host</td>
<td>[Discover Virtual Servers]</td>
</tr>
<tr>
<td></td>
<td>[Power On All Virtual Servers...]</td>
</tr>
<tr>
<td></td>
<td>[Force Power Off All Virtual Servers...]</td>
</tr>
<tr>
<td></td>
<td>[Suspend All Running Virtual Servers...]</td>
</tr>
<tr>
<td></td>
<td>[Resume All Suspended Virtual Servers...]</td>
</tr>
<tr>
<td></td>
<td>[Remove From Virtual Farm...]</td>
</tr>
<tr>
<td></td>
<td>[Start...]</td>
</tr>
<tr>
<td></td>
<td>[Stop...]</td>
</tr>
<tr>
<td></td>
<td>[Migrate All Virtual Servers]</td>
</tr>
<tr>
<td>Virtual server</td>
<td>[Shutdown]</td>
</tr>
<tr>
<td></td>
<td>[Shutdown and Power Off]</td>
</tr>
<tr>
<td></td>
<td>[Power On]</td>
</tr>
<tr>
<td></td>
<td>[Power Off Now]</td>
</tr>
<tr>
<td></td>
<td>[Restart]</td>
</tr>
<tr>
<td></td>
<td>[Restart Now]</td>
</tr>
<tr>
<td></td>
<td>[Delete Permanently...]</td>
</tr>
<tr>
<td></td>
<td>[Migrate Virtual Server]</td>
</tr>
</tbody>
</table>

a. The two migration tasks are not always listed. They are displayed only after you have created and saved migration tasks, where saved_task is the name of the migration task.
IBM z/VM Center

The IBM z/VM Center extension for IBM Director allows you to manage and clone Linux guests running on z/VM. This chapter provides complete instructions for the z/VM System Programmer on how to enable a z/VM Version 5.2 system to be managed using IBM Director and the z/VM Center extension.

In this chapter we cover the following topics:

- 11.1, “Overview” on page 570
- 11.2, “Planning and preparation” on page 576
- 11.3, “z/VM customization” on page 578
- 11.4, “Installing the Management Access Point” on page 601
- 11.5, “Installing the z/VM Center extension” on page 612
- 11.6, “Verifying the installation and initial setup” on page 615
- 11.7, “General usage” on page 623
11.1 Overview

The z/VM Center extension for IBM Director consists of the following components:

- z/VM Management Access Point Agent extension
- z/VM Center Console extension
- z/VM Center Server extension

Figure 11-1 shows these components in green. The diagram also shows the relationship between the z/VM Center extension components, IBM Director management server, and the z/VM system. We describe these components in this section.

On System z, IBM Director and IBM Director extensions for Linux on System z are delivered as components of IBM Virtualization Engine and Infrastructure Services. IBM Director for System z is a no-charge download. However, the z/VM Center extension is a chargeable feature, product number 5648-DR1. Information about the extension plus a demo and links to downloads can be found at:

You can also read more about the z/VM Center extension in the IBM Director Information Center:

http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/zvmcenter_5.20/zvm0_main.html

11.1.1 z/VM Management Access Point

IBM Director uses CIM as the underlying management interface to interact with its managed endpoints. However, there is no implementation of a CIM server for z/VM. This is not a problem since Linux runs on z/VM, and there is a CIM server for Linux. The z/VM Management Access Point (MAP) package contains the CIM models and providers that IBM Director uses to communicate with z/VM. The MAP code gets installed into the cimserver that runs on Linux under z/VM, and then uses the following interfaces to communicate with z/VM:

- z/VM Systems Management API via RPC
- Native Directory Manager commands

**Note:** In our system we used DirMaint as the directory manager. Other directory managers are available. Contact the directory manager vendor to determine whether it supports IBM Director z/VM Center.

- Native CP commands

**Note:** The MAP can use either cpint or vmcp to issue CP commands from Linux. vmcp is the default on RHEL 4 U3 and higher, SLES 9 SP3 and higher, and SLES 10. cpint is only used if vmcp is not available. On RHEL 4 systems previous to U3, it may be necessary to build cpint from source.

11.1.2 z/VM Center server extension

The z/VM Center server extension installs on the management server running IBM Director Server. The server extension runs on all platforms that support IBM Director Server.

The z/VM Center server extension must have a valid license key to be functional. It will install, and the tasks will appear in the Director console, but an error message will be produced if the tasks are invoked without a valid license key.
For details on installing the license key, see the IBM Director Information Center for z/VM Center:

http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/zvmcenter_5.20/vsd0_t_install_key.html

There are three tasks that are available in z/VM Center:

► Virtual Server Deployment (VSD)
  VSD provides the ability to request access to a z/VM system, view its disk pool utilization, create virtual server templates, and create operating system templates. It also provides the ability to create new virtual servers based on the virtual server templates, as well as new operating systems within those virtual servers based on the operating system templates.

► Server complexes (SC)
  SC provides the ability to create a container called a server complex. The server complex can have properties assigned to it such as network settings, VMRM settings, shared minidisk settings, and entry and exit scripts. These settings are applied when virtual servers enter the server complex.

  SC also provides the ability to create multiple new Linux systems from an existing set of virtual server templates and operating system templates with a single drag-and-drop action. The new systems will inherit the properties that have been assigned to the SC that they will be a part of.

► Utility Service Configuration Manager
  The Utility Service Configuration Manager provides an interface to configure Linux Utility applications that have been provisioned to Linux systems on System z hardware using Software Distribution.

  See the following for more information about Linux Utilities for IBM System z:
  http://www.ibm.com/zseries/os/linux/utilities

11.1.3 z/VM Center Console extension

The z/VM Center console extension installs on each management console running IBM Director Console. The console extension runs on all platforms that support IBM Director Console. It provides the graphical components and code needed to invoke the z/VM Center functions on IBM Director Server with the z/VM Center extension installed.
11.1.4 How it all works

In Figure 11-2 the following sequence of events happens:

1. The z/VM Center extension in the console issues a command to Director Server (for example, deactivate LNXRH4).

2. The z/VM Center extension in the management server receives the command from the console, and contacts the imbedded SBLIM client.

3. The SBLIM client on the management server invokes the System_Deactivate process within the cimserver running on the Linux system installed on the MAPSERVE guest.

4. The cimserver on MAPSERVE uses the code installed with the z/VM MAP package to communicate with the z/VM Systems Management API, which runs in the VSMSERVE service machine. The z/VM SM API then deactivates LNXRH4.

Figure 11-2 z/VM Center to z/VM SM API
In Figure 11-3 a similar process happens, but this time z/VM center is looking for the list of OS templates available on the z/VM system. The z/VM MAP code issues a scan command against the directory management system since this function is not available from the z/VM SM API.
Lastly, in Figure 11-4 the z/VM MAP issues CP commands via vmcp or cpint. CP commands are used to query the current status of guests, storage, service levels, or system names.

vmcp and cpint are both Linux kernel modules that can be used to issue commands directly to CP and get the response back to the Linux user who issued the command.

vmcp is automatically included in Linux systems with kernel levels equal to or higher than 2.6.13. It has also been backported to RHEL 4 U3 and higher, as well as SLES 9 SP3 and higher.

cpint is included with all versions of SLES 9, but the package is not part of the default install.

Notice that in no case does IBM Director Server ever contact the z/VM system directly through the TCP/IP stack. IBM Director only communicates with the z/VM system through the MAP system’s CIM services.
11.2 Planning and preparation

Before attempting to install z/VM Center or configure the z/VM system, the resources that will be used for provisioning new Linux systems should be found and made available.

11.2.1 Questions to answer

As with anything on System z, the outcome of a project depends highly on the quality of the planning done before implementing it.

In the following questions, we have provided answers related to our test environment in the lab. Of course your answers will be different.

► What DASD volumes will be used to contain the Linux systems?
  – We have devices CB31-CB49 available to our z/VM system.
  – CB31 - CB36 and CB 49 are in use by the z/VM system.
  – CB37 and CB 38 are the master Linux images LNXRH4 and LNXS10.
  – We will use CB37-CB48 as a DASD pool. This will include the master Linux images.

► What OSA devices are available for network connectivity?
  – We have OSA devices 2E20-2E2F available to our z/VM system.
  – Devices 2E20-2E22 are in use by z/VM TCP/IP.
  – Devices 2E24-2E26 are in use by VSWITCH1.
  – Device 2E2F is an OSA agent.
  – This leaves devices 2E28-2E2E available for use, enough for two systems.

► What IP addresses are available for use by new Linux systems?

► How large should the MAP guest be?
  – The MAP requires 512 MB of memory and 215 MB of disk space.
  – We use a single 3390-3 volume for our Linux systems. It is still possible to run Linux on a single 3390-3 in a minimal install without the complete GNOME or KDE environments installed. Our two pre-existing Linux systems both have at least 900 MB of free space on their 3390-3.
What will the network layout look like?
Since we have a limited number of real OSA devices available, our network could consist of only two Linux systems connected to real OSA devices. The rest of our Linux systems will connect to the existing vswitch.

Is DirMaint enabled and running?
The z/VM Center Extension requires a directory management tool. We use DirMaint.

If you are using DirMaint, are the following APARs installed?
– VM63948, VM64022, VM64089.
– These APARs address problems with DirMaint’s use of FlashCopy® that can lead to hung work units if they are not applied.

11.2.2 The initial configuration

Figure 11-5 on page 578 illustrates the starting configuration for the examples in this chapter.

z/VM 5.2 is running at RSU 0602.
TCP/IP is enabled and working with a single OSA interface.
DirMaint is enabled and working with MAINT as an authorized user.
A Vswitch is defined and working.
Two Linux guests are running and using the Vswitch for their network connections.
IBM Director is installed and running in the network where it can reach the z/VM System. IBM Director is perfectly capable of running on a Linux guest under z/VM, even on the same z/VM system that it is managing. We chose to use the same Director server as was used for the rest of the book (named Lithium in the diagrams).
11.3 z/VM customization

For the z/VM Center extension to function correctly, resources need to be defined in DirMaint, the VSMSERV guest needs to be enabled, a guest to run the MAP defined, and a new user class must be defined.

11.3.1 DirMaint customization

DirMaint should be enabled and running on the z/VM system. Refer to the following for details:

- DirMaint 520 Program Directory:
  

- Product publication Directory Maintenance Facility Tailoring and Administration Guide:
  

We chose to use the default single DATAMOVE machine. It is possible to define multiple DATAMOVE machines so that disks can be copied in parallel, but the
z/VM Center extension only dispatches one guest cloning operation at a time. If the system to be cloned has multiple disks to be copied, then multiple DATAMOVE machines may help the cloning operation go faster.

See Chapter 4 of *Directory Maintenance Facility Tailoring and Administration Guide* for more information about setting up multiple DATAMOVE machines:


**Define tagged comments for z/VM Center**

The z/VM directory allows the system programmer to imbed comments into the directory control files. Special comments called *tagged comments* can be defined to the directory management tool so that they are easily searchable.

The z/VM Center extension makes use of these tagged comments to help keep track of data pertaining to the Linux guests. At least three tagged comments must be defined:

- **CIMGOS01**
  The CIMGOS01: tag is used to store information describing the OS instance that is installed on this guest.
  
  *CIMGOS01: DATE 20061204105758.000000-300 TYPE 36 HOST lnxrh4
  *CIMGOS01: DISK 0201 BOOT 0201 PORT C200 IN eth0 IP 9.12.4.161

- **CIMIMG**
  The CIMIMG: tag is used to store image information in an OS template—mainly the name of the guest it was created from.
  
  *CIMIMG: DATE 20061204172257.000000-300 TYPE 36 GOS
  *CIMIMG: VMLINUX4.LNXRH4.CIMGOS01

- **CIMNIC01**
  The CIMNICxx: tags are used to store the configuration of the network devices in an OS template. Any guest that is provisioned through the Virtual Server Deployment task using this OS template will connect to the same networks as the original system.
  
  *CIMNIC01: C200 TYPE QDIO LAN SYSTEM VSWITCH1 DATA IN eth0 IP 9.12.4.161

Define enough *CIMNICxx: tags so that each network interface on the Linux guests can be accounted for. For example, if the Linux systems will never have more than four network interfaces, define *CIMNIC01: through *CIMNIC04:
See Example 11-1 for an example of defining enough tagged comments to cover the OS instances, OS templates, and eight network adapters per Linux image.

---

**Example 11-1  Defining tagged comments to DirMaint**

```
Q USERID
MAINT AT VMLINUX4
Ready; T=0.01/0.01 15:48:15
DIRM DEFINESTAG ? ALL
DVHXMT1191I Your DEFINESTAG request has been sent for processing.
Ready; T=0.03/0.03 15:48:53
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHDST3404I There are no local tags currently defined in your local
DVHDST3404I installation.
DVHREQ2289I Your DEFINESTAG request for MAINT at * has completed; with
DVHREQ2289I RC = 0.
DIRM DEFINESTAG CREATE *CIMGOS01: 100
DVHXMT1191I Your DEFINESTAG request has been sent for processing.
Ready; T=0.02/0.03 15:50:49
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHREQ2289I Your DEFINESTAG request for MAINT at * has completed; with
DVHREQ2289I RC = 0.
DIRM DEFINESTAG CREATE *CIMG: 101
DVHXMT1191I Your DEFINESTAG request has been sent for processing.
Ready; T=0.02/0.03 15:51:04
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHREQ2289I Your DEFINESTAG request for MAINT at * has completed; with
DVHREQ2289I RC = 0.
DIRM DEFINESTAG CREATE *CIMNIC01: 102
DVHXMT1191I Your DEFINESTAG request has been sent for processing.
Ready; T=0.02/0.03 15:51:30
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHREQ2289I Your DEFINESTAG request for MAINT at * has completed; with
DVHREQ2289I RC = 0.
DIRM DEFINESTAG CREATE *CIMNIC02: 103
DVHXMT1191I Your DEFINESTAG request has been sent for processing.
Ready; T=0.02/0.03 15:51:36
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHREQ2289I Your DEFINESTAG request for MAINT at * has completed; with
DVHREQ2289I RC = 0.
DIRM DEFINESTAG CREATE *CIMNIC03: 104
DVHXMT1191I Your DEFINESTAG request has been sent for processing.
Ready; T=0.02/0.03 15:51:43
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHREQ2289I Your DEFINESTAG request for MAINT at * has completed; with
```
DIRM DEFINESTAG CREATE *CIMNIC04: 105
DVHRQ2289I RC = 0.
DVHREQ2288I Your DEFINESTAG request has been sent for processing.
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHREQ2289I Your DEFINESTAG request for MAINT at * has completed; with
DVHREQ2289I RC = 0.

DIRM DEFINESTAG CREATE *CIMNIC05: 106
DVHREQ2288I Your DEFINESTAG request has been sent for processing.
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHREQ2289I Your DEFINESTAG request for MAINT at * has completed; with
DVHREQ2289I RC = 0.

DIRM DEFINESTAG CREATE *CIMNIC06: 107
DVHREQ2288I Your DEFINESTAG request has been sent for processing.
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHREQ2289I Your DEFINESTAG request for MAINT at * has completed; with
DVHREQ2289I RC = 0.

DIRM DEFINESTAG CREATE *CIMNIC07: 108
DVHREQ2288I Your DEFINESTAG request has been sent for processing.
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHREQ2289I Your DEFINESTAG request for MAINT at * has completed; with
DVHREQ2289I RC = 0.

DIRM DEFINESTAG CREATE *CIMNIC08: 109
DVHREQ2288I Your DEFINESTAG request has been sent for processing.
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHREQ2289I Your DEFINESTAG request for MAINT at * has completed; with
DVHREQ2289I RC = 0.

DIRM DEFINESTAG ? ALL
DVHREQ2289I Your DEFINESTAG request has been sent for processing.
DVHREQ2288I Your DEFINESTAG request for MAINT at * has been accepted.
DVHST3404I The current settings are listed below, the format is:
DVHST3404I tagname sortorder.
DVHST3404I *CIMGOS01: 100
DVHST3404I *CIMIMG: 101
DVHST3404I *CIMNIC01: 102
DVHST3404I *CIMNIC02: 103
DVHST3404I *CIMNIC03: 104
DVHST3404I *CIMNIC04: 105
DVHST3404I *CIMNIC05: 106
DVHST3404I *CIMNIC06: 107
Check the DirMaint CONFIGxx DATADVH file

Do the following:

1. Ensure that the following two statements are defined in the CONFIGxx DATADVH file:

   ```
   ALLOW_ASUSER_NOPASS_FROM= VSMERVE *
   ASYNCHRONOUS_UPDATE_NOTIFICATION_EXIT.UDP= DVHXNE EXEC
   ```

   ALLOW_ASUSER_NOPASS_FROM allows the listed user to issue commands to the Directory Manager using the ASUSER modifier without having to know the password of that user. This is needed so that the MAP can work with the directory entries of other users.

   ASYNCHRONOUS_UPDATE_NOTIFICATION_EXIT.UDP activates an exit that will notify the MAP of any changes that are made to the directory by other parties. For example, if MAINT alters a Linux guest's directory entry by adding another minidisk, this exit will notify the MAP so that the z/VM Center does not get out of sync with the actual directory contents.

   Example 11-2 shows how to retrieve the CONFIGxx DATADVH file from DirMaint.

---

**Example 11-2   Retrieving CONFIGxx DATADVH from DirMaint**

```plaintext
Q USERID
MAINT AT VMLINUX4
Ready; T=0.01/0.01 15:58:15
DIRM SEND CONFIGA DATADVH
DVHMT1191I Your SEND request has been sent for processing.
Ready; T=0.02/0.03 16:15:39
DVHREQ2288I Your SEND request for MAINT at * has been accepted.
RDR FILE 0133 SENT FROM DIRMAINT PUN WAS 0011 RECS 0014 CPY 001 A NOHOLD NOKEEP

DVHREQ2289I Your SEND request for MAINT at * has completed; with RC = 0.
RECEIVE 133 = = A
File CONFIGA DATADVH A1 created from CONFIGA DATADVH A1 received from DIRMAINT at VMLINUX4
Ready; T=0.01/0.01 16:15:48
```
2. Edit the CONFIGxx DATADVH file to add the two new configuration statements, or verify that they are already there.

Example CONFIGxx DATADVH

```
00000 * * * Top of File * * *
00001 RUNMODE= OPERATIONAL
00002 ONLINE= IMMED
00003 DASD_ALLOCATE= EXACT_FF
00004 DATAMOVE_MACHINE= DATAMOVE * *
00005 DVHDXD_FLASHCOPY_BEHAVIOR= 2
00006 DVHDXD_FLASHCOPY_COMPLETION_WAIT= 0 0
00007 MAXIMUM_UNASSIGNED_WORKUNITS= 100
00008 ALLOW_ASUSER_NOPASS_FROM= VSMServe *
00009 ASYNCHRONOUS_UPDATE_NOTIFICATION_EXIT.UDP= DVHXNE EXEC
00010 * * * End of File * * *
```

3. Send the CONFIGxx DATADVH file back to DirMaint and activate its changes.

Example 11-3 Replacing CONFIGxx DATADVH from DirMaint and making it active

```
DIRM FILE CONFIGA DATADVH
PUN FILE 0134 SENT TO DIRMAINT RDR AS 0012 RECS 0018 CPY 001 0 NOHOLD NOKEEP

DVHXMT1191I Your FILE request has been sent for processing.
Ready; T=0.03/0.03 16:23:44
DVHREQ2288I Your FILE request for MAINT at * has been accepted.
DVHRCV3821I File CONFIGA DATADVH A1 has been received; RC = 0.
DVHREQ2289I Your FILE request for MAINT at * has completed; with RC = 0.

DIRM RLDC
DVHXMT1191I Your RLDCODE request has been sent for processing.
Ready; T=0.03/0.03 16:23:58
DVHREQ2288I Your RLDCODE request for MAINT at * has been accepted.
DVHREQ2289I Your RLDCODE request for MAINT at * has completed; with RC = DVHREQ2289I 0.

DIRM RLDD
DVHXMT1191I Your RLDDATA request has been sent for processing.
Ready; T=0.03/0.03 16:24:01
DVHREQ2288I Your RLDDATA request for MAINT at * has been accepted.
DVHREQ2289I Your RLDDATA request for MAINT at * has completed; with RC = DVHREQ2289I 0.

DIRM RLDE
DVHXMT1191I Your RLDEXTN request has been sent for processing.
Ready; T=0.03/0.03 16:24:04
DVHREQ2288I Your RLDEXTN request for MAINT at * has been accepted.
DVHILZ3510I Starting DVHINITL with directory: USER DIRECT E
```
Create a directory prototype

A directory prototype will allow the system programmer to make guests that all share common statements. It is also the only way to get the z/VM Center to create certain directory statements such as CRYPTO settings.

Multiple directory prototypes can be created to support as many configurations as are needed.

Example 11-4  CRPTPROT directory prototype

```
00000 * * * Top of File * * *
00001 USER CRPTPROT NOLOG 5M 5M G
00002 CRYPTO APVIRT
00003 SPOOL 000C 2540 READER *
00004 SPOOL 000D 2540 PUNCH A
00005 SPOOL 000E 1403 A
00006 CONSOLE 009 3215 T
00007 LINK MAINT 0190 0190 RR
00008 LINK MAINT 019D 019D RR
00009 LINK MAINT 019E 019E RR
00010 MDISK 0299 FB-512 V-DISK 256000
00011 * * * End of File * * *
```

Use the DirMaint FILE command to tell DirMaint to keep a copy of this prototype for future use, as shown in Example 11-5.

Example 11-5  Sending the directory prototype to DirMaint

```
Ready; T=0.01/0.01 16:58:54
DIRM FILE CRPTPROT PROTODIR
PUN FILE 0136 SENT TO DIRMAINT RDR AS 0013 RECS 0018 CPY 001 0 NOHOLD NOKEEP
DVHXT1191I Your FILE request has been sent for processing.
Ready; T=0.03/0.03 16:59:04
DVHREQ2288I Your FILE request for MAINT at * has been accepted.
DVHRCV3821I File CRPTPROT PROTODIR A has been received; RC = 0.
DVHREQ2289I Your FILE request for MAINT at * has completed; with RC = 0.
```
NOLOG ID for OSA devices
The z/VM Center only consults the z/VM directory to determine which OSA devices are in use. OSA devices that are dynamically attached to machines such as 2E20 - 2E22 for TCP/IP and 2E24 - 2E26 for VSWITCH1 are not recognized as unavailable by z/VM Center.

Unfortunately, z/VM Center does not have a way to maintain this directory entry, so it must be kept up to date manually.

1. Create a dummy user ID to mark dynamically allocated OSA devices as in use.

   Example 11-6   Dummy ID for OSA adapters
   
   00000 * * * Top of File * * *
   00001 USER $DEVICE$ NOLOG 1M 1M G
   00002 * This user is only used to mark dynamically attached OSA
   00003 * devices as in use for z/VM Center
   00004  DEDICATE 2E20 2E20
   00005  DEDICATE 2E21 2E21
   00006  DEDICATE 2E22 2E22
   00007  DEDICATE 2E24 2E24
   00008  DEDICATE 2E25 2E25
   00009  DEDICATE 2E26 2E26
   00010 * * * End of File * * *

2. Add the new user to the z/VM system using the ADD command.

   Example 11-7   Adding the $DEVICE$ user
   
   DIRM ADD $DEVICE$
   
   PUN FILE 0137 SENT TO DIRMAINT RDR AS 0014 RECS 0017 CPY 001 0
   NOHOLD NOKEEP
   DVHXMT1191I Your ADD request has been sent for processing.
   Ready; T=0.03/0.03 17:18:28
   DVHREQ2288I Your ADD request for $DEVICE$ at * has been accepted.
   DVHBIU3450I The source for directory entry $DEVICE$ has been updated.
   DVHBIU3424I The next ONLINE will take place immediately.
   DVHDC3451I The next ONLINE will take place via delta object directory.
   DVHBIU3428I Changes made to directory entry $DEVICE$ have been placed
   DVHBIU3428I online.
   DVHREQ2289I Your ADD request for $DEVICE$ at * has completed; with RC
Allocation groups
z/VM Center relies on the Directory Management tool to automatically allocate minidisks out of a predefined pool of volumes. With DirMaint, these pools are defined in the EXTENT CONTROL file:

1. Retrieve the EXTENT CONTROL file from DirMaint (Example 11-8).

Example 11-8  Retrieve the EXTENT CONTROL file

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIRM SEND EXTENT CONTROL</td>
<td>DVHXMT1191I Your SEND request has been sent for processing.</td>
</tr>
<tr>
<td></td>
<td>Ready; T=0.03/0.03 17:20:21</td>
</tr>
<tr>
<td>DVHREQ2288I</td>
<td>Your SEND request for MAINT at * has been accepted.</td>
</tr>
<tr>
<td>RDR FILE 0138 SENT FROM DIRMAINT PUN WAS 0015 RECS 0030 CPY 001 A NOHOLD NOKEEP</td>
<td>DVHREQ2289I Your SEND request for MAINT at * has completed; with RC = 0.</td>
</tr>
<tr>
<td>RECEIVE 138 = = A</td>
<td>File EXTENT CONTROL A2 created from EXTENT CONTROL E2 received from DIRMAINT at VMLINUX4</td>
</tr>
<tr>
<td></td>
<td>Ready; T=0.01/0.01 17:20:29</td>
</tr>
</tbody>
</table>

2. Edit the extent control file to include the available DASD to be used by z/VM Center as a DASD pool. On our system the VolSer is LX<device number>

The extent control file can define multiple pools, but we chose to define all of our DASD in one pool. Each pool is made up of a set of regions. A region is an empty extent on a volume where DirMaint is allowed to allocate minidisks. Regions should never include cylinder 0 of the real volume.

The default behavior when DirMaint is allocating minidisks among the regions in a pool is to fill each region sequentially. This is fine for minidisks that will not have heavy I/O requirements placed on them. In our case, we chose to use the ALLOCATE ROTATING allocation method. This tells DirMaint to place each new minidisk on a new region in a round-robin fashion. This allows the regions to be more equally utilized as they fill. It is not especially important for 3390-03 volumes since entire volumes are usually used at once for Linux systems, but it is important for -09, -27, or -56 where a single volume may contain minidisks for multiple Linux systems.

Attention: Despite what the z/VM V5R2.0 Directory Maintenance Facility Tailoring and Administration Guide says, blank lines do seem to cause problems in the extent control file. We had to remove a blank line from between the end of our POOL0 definition and the :END. tag to get the z/VM Center to recognize POOL0.
Example 11-9  Customizing the EXTENT CONTROL file

*  ********************************************************************
:REGIONS.
  *RegionId  VolSer    RegStart      RegEnd  Dev-Type  Comments
  000001     LXCB37    0001          3338    3390-03
  000002     LXCB38    0001          3338    3390-03
  000003     LXCB39    0001          3338    3390-03
  000004     LXCB3A    0001          3338    3390-03
  000005     LXCB3B    0001          3338    3390-03
  000006     LXCB3C    0001          3338    3390-03
  000007     LXCB3D    0001          3338    3390-03
  000008     LXCB3E    0001          3338    3390-03
  000009     LXCB3F    0001          3338    3390-03
  000010     LXCB40    0001          3338    3390-03
  000011     LXCB41    0001          3338    3390-03
  000012     LXCB42    0001          3338    3390-03
  000013     LXCB43    0001          3338    3390-03
  000014     LXCB44    0001          3338    3390-03
  000015     LXCB45    0001          3338    3390-03
  000016     LXCB46    0001          3338    3390-03
  000017     LXCB47    0001          3338    3390-03
  000018     LXCB48    0001          3338    3390-03

:END.
:GROUPS.
  *GroupName RegionList
  POOL0   (ALLOCATE ROTATING)
  POOL0   000001 000002 000003 000004 000005 000006 000007 000008
  POOL0   000009 000010 000011 000012 000013 000014 000015 000016
  POOL0   000017 000018

:END.

3. Send the EXTENT CONTROL file back to DirMaint, and make it active.

Example 11-10  Replacing and reactivating the EXTENT CONTROL file

DIRM FILE EXTENT CONTROL A
PUN FILE 0139 SENT TO  DIRMAINT RDR AS  0016 RECS 0047 CPY  001 0 NOHOLD NOKEEP
DVXMTT1191I Your FILE request has been sent for processing.
Ready; T=0.03/0.03 17:32:43
  DVHREQ2288I Your FILE request for MAINT at * has been accepted.
  DVHRCV3821I File EXTENT CONTROL E2 has been received; RC = 0.
  DVHREQ2289I Your FILE request for MAINT at * has completed; with RC = 0.

DIRM RLDE
DVXMTT1191I Your RLDEXTN request has been sent for processing.
Ready; T=0.03/0.03 17:32:49
11.3.2 Define a custom user class

The MAP Linux system needs to be able to get the status of the z/VM system and the devices it is managing, as well as set access privileges on virtual network devices. These privileges by default are bundled in with other privileges that the MAP does not need to do its work. Here we define a new privilege class for the MAP guest that only contains the extra set of commands that it needs.

To define a custom user class T so that we can avoid giving the MAP full B and E authority, execute the following commands as MAINT:

```
#CP MODIFY CMD SET SUBC VSWITCH IBMCLASS B PRIVCLASS BT
#CP MODIFY CMD QUERY SUBC * IBMCLASS B PRIVCLASS BT
#CP MODIFY CMD IND IBMCLASS E PRIVCLASS ET
#CP MODIFY CMD QUERY SUBC * IBMCLASS G PRIVCLASS GT
#CP MODIFY CMD LINK IBMCLASS G PRIVCLASS GT
```

Add the section shown in Example 11-11 to SYSTEM CONFIG so that the custom user class is available after an IPL.

```
Example 11-11   Custom user class in SYSTEM CONFIG

 /*********************************************************************/
 /*                     IBM Director Privclass setup                  */
 /*********************************************************************/
 MODIFY CMD SET      SUBC VSWITCH IBMCLASS B PRIVCLASS BT
 MODIFY CMD QUERY SUBC * IBMCLASS B PRIVCLASS BT
 MODIFY CMD IND IBMCLASS E PRIVCLASS ET
 MODIFY CMD QUERY SUBC * IBMCLASS G PRIVCLASS GT
 MODIFY CMD LINK IBMCLASS G PRIVCLASS GT

At this point, we have defined resources to DirMaint and made changes to the z/VM Privilege Class structure.
11.3.3 Create IDs for MAPSERVE and MAPAUTH

The MAPSERVE guest will be used to contain the Linux system that will serve as the Management Access Point (MAP). Recall that the MAP runs the cimserver that the z/VM Center extension uses to communicate with z/VM.

To do this:

1. Create the MAPSERVE user.

Example 11-12 shows the directory entry we used to define the MAP Linux system. Ensure that the directory entry provides the new privilege class that was defined in 11.3.2, “Define a custom user class” on page 588.

Note that NICDEF C300 is for the MAPLAN guest LAN, which we have not created yet. We will create the guest LAN in Example 11-19 on page 595.

Example 11-12 MAP guest definition

```
00000 * * * Top of File * * *
00001 USER MAPSERVE EVRESPAM 512M 1G GT
00002   INCLUDE IBMDFLT
00003   OPTION LNKNOPAS LANG AMENG
00004   NICDEF C200 TYPE QDIO LAN SYSTEM VSWITCH1
00005   NICDEF C300 TYPE QDIO LAN SYSTEM MAPLAN
```
2. Add the new MAPSERVE user to the z/VM directory, as shown in Example 11-13.

Example 11-13   Adding MAP guest to DirMaint

```
DIRM ADD MAPSERVE
PUN FILE 0147 SENT TO   DIRMAINT RDR AS 0024 RECS 0014 CPY 001 0 NOHOLD NOKEEP
DVHXMT1191I Your ADD request has been sent for processing.
Ready; T=0.03/0.03 10:40:04
DVHREQ2288I Your ADD request for MAPSERVE at * has been accepted.
DVHBIU3450I The source for directory entry MAPSERVE has been updated.
DVHBIU3424I The next ONLINE will take place immediately.
DVHDRC3451I The next ONLINE will take place via delta object directory.
DVHBIU3428I Changes made to directory entry MAPSERVE have been placed
DVHBIU3428I online.
DVHSCU3541I Work unit 01104005 has been built and queued for processing.
DVHSHN3541I Processing work unit 01104005 as MAINT from VMLINUX4,
DVHSHN3541I notifying MAINT at VMLINUX4, request 38.1 for MAPSERVE
DVHSHN3541I sysaffin *; to: AMDISK 0191 3390 156 10 LX4USR MR
DVHBIU3450I The source for directory entry MAPSERVE has been updated.
DVHBIU3424I The next ONLINE will take place immediately.
DVHDRC3451I The next ONLINE will take place via delta object directory.
DVHBIU3428I Changes made to directory entry MAPSERVE have been placed
DVHBIU3428I online.
DVHSHN3430I AMDISK operation for MAPSERVE address 0191 has finished
DVHSHN3430I (WUCF 01104005).
DVHSCU3541I Work unit 01104006 has been built and queued for processing.
DVHSHN3541I Processing work unit 01104006 as MAINT from VMLINUX4,
DVHSHN3541I notifying MAINT at VMLINUX4, request 38.2 for MAPSERVE
DVHSHN3541I sysaffin *; to: AMDISK 0201 3390 AUTOG 3338 POOLO MR
DVHBIU3450I The source for directory entry MAPSERVE has been updated.
DVHBIU3424I The next ONLINE will take place immediately.
DVHDRC3451I The next ONLINE will take place via delta object directory.
DVHBIU3428I Changes made to directory entry MAPSERVE have been placed
DVHBIU3428I online.
DVHSHN3430I AMDISK operation for MAPSERVE address 0201 has finished
DVHSHN3430I (WUCF 01104006).
DVHREQ2289I Your ADD request for MAPSERVE at * has completed; with RC
DVHREQ2289I = 0.
```
3. Create a z/VM user named MAPAUTH.

   The purpose of MAPAUTH is to separate the authority that the MAP Linux system needs to do its work from the Linux system itself. This provides a separation of privileges between the Linux system that does the work (MAPSERVE) and the user who is authorized to do the work (MAPAUTH). This separation is a safety net in the event of software errors or security breaches.

   The definition of the MAPAUTH id is shown in Example 11-14.

   **Example 11-14  MAPAUTH guest definition**
   
   ```
   00000 * * * Top of File * * *
   00001 USER MAPAUTH  HTUAPAM  32M 32M G
   00002  INCLUDE IBMDFLT
   00003  MDISK 191 3390 166   10   LX4USR  MR
   00004 * * * End of File * * *
   ```

4. Add the MAPAUTH user to the z/VM Directory, as shown in Example 11-15.

   **Example 11-15  Adding MAPAUTH guest to DirMaint**
   
   ```
   DIRM ADD MAPAUTH
   PUN FILE 0148 SENT TO   DIRMAINT RDR AS  0025 RECS 0011 CPY 001 0 NOHOLD NOKEEP
   DVHXT1191I Your ADD request has been sent for processing.
   Ready; T=0.03/0.04 10:48:54
   DVHREQ2288I Your ADD request for MAPAUTH at * has been accepted.
   DVHBIU3450I The source for directory entry MAPAUTH has been updated.
   DVHBIU3424I The next ONLINE will take place immediately.
   DVHDCRC3451I The next ONLINE will take place via delta object directory.
   DVHBIU3428I Changes made to directory entry MAPAUTH have been placed
   DVHBIU3428I online.
   DVHCSN3541I Work unit 01104856 has been built and queued for processing.
   DVHSHN3541I Processing work unit 01104856 as MAINT from VMLINUX4,
   DVHSHN3541I notifying MAINT at VMLINUX4, request 39.1 for MAPAUTH
   DVHSHN3541I sysaffin *; to: AMDISK 0191 3390 166 10 LX4USR MR
   DVHBIU3450I The source for directory entry MAPAUTH has been updated.
   DVHBIU3424I The next ONLINE will take place immediately.
   DVHDCRC3451I The next ONLINE will take place via delta object directory.
   DVHBIU3428I Changes made to directory entry MAPAUTH have been placed
   DVHBIU3428I online.
   DVHSHN3430I AMDISK operation for MAPAUTH address 0191 has finished (WUCF
   DVHSHN3430I 01104856).
   DVHREQ2289I Your ADD request for MAPAUTH at * has completed; with RC =
   DVHREQ2289I 0.
   ```
5. Logged in as MAINT (or any other user with sufficient DirMaint privileges), allow the MAPAUTH user to issue DirMaint commands using the commands shown in Example 11-16.

**Attention:** We are authorizing MAPAUTH to issue DirMaint commands, not MAPSERVE.

**Example 11-16  Granting MAPAUTH authority to issue DirMaint commands**

```plaintext
DIRM FOR ALL AUTHFOR MAPAUTH CMDLEVEL 140A CMDSET ADGHMOPS
DVHXMT1191I Your AUTHFOR request has been sent for processing.
Ready; T=0.03/0.03 13:45:56
DVHREQ2288I Your AUTHFOR request for ALL at * has been accepted.
DVHREQ2289I Your AUTHFOR request for ALL at * has completed; with RC =
DVHREQ2289I 0.

DIRM FOR ALL AUTHFOR MAPAUTH CMDLEVEL 150A CMDSET ADGHMOPS
DVHXMT1191I Your AUTHFOR request has been sent for processing.
Ready; T=0.03/0.03 13:46:01
DVHREQ2288I Your AUTHFOR request for ALL at * has been accepted.
DVHREQ2289I Your AUTHFOR request for ALL at * has completed; with RC =
DVHREQ2289I 0.
```

### 11.3.4 VSMSERVE enablement

VSMSERVE is the machine that runs the z/VM Systems Management API interface. The z/VM Systems Management API is an RPC interface, and as such is not encrypted. All traffic entering or exiting the z/VM Systems Management API is in plain text, including z/VM system passwords.

For security reasons we set the network environment up such that the only system that can communicate with the z/VM Systems Management API is the MAP system. This is done by creating a restricted guest LAN that only allows the z/VM TCP/IP stack and MAP systems to couple to it.

In addition to the private guest LAN, the z/VM TCP/IP stack is configured to only expose the z/VM Systems Management API to the private guest LAN.
To configure VMSERVE, do the following:

1. Log on to the VMSERVE machine. Be sure to press keys before pressing Enter to prevent the server from starting, as shown in Example 11-17. If the server does start, enter #CP I CMS to get another chance.

Example 11-17  Logging in to VMSERVE

LOGON VMSERVE
z/VM Version 5 Release 2.0, Service Level 0601 (64-bit),
built on IBM Virtualization Technology
There is no logmsg data
FILES:  NO RDR,  NO PRT,  NO PUN
LOGON AT 12:18:28 EST FRIDAY 12/01/06
z/VM V5.2.0  2006-06-01 12:22

DMSACP723I C (193) R/O
DMSACP723I E (591) R/O
DMSACP723I F (592) R/O
Ready; T=0.01/0.01 12:18:30
DTCRUN1022I Console log will be sent to default owner ID: TCPMAINT
DTCRUN1022I Console log will be sent to redefined owner ID: VMSERVE
File DIRMAINT NEWMAIL B2 sent to * at VMLINUX4 on 12/01/06 12:18:30
DVHELD1190I Command EXECLOAD complete; RC= 0.
DVHGLB1190I Command DEFAULTS complete; RC= 0.
DVHGLB1190I Command DEFAULTS complete; RC= 0.
DTCRUN1021R To cancel Virtual System Management API server startup, type any
non-blank character and press ENTER. To continue startup, just
press ENTER.

asdf
DTCRUN1098I Server startup cancelled at user request
CON FILE 0001 SENT **** PURGED **** AS 0001 RECS 0011 CPY 001 T NOHOLD NOKEEP
Ready; T=0.11/0.12 12:18:38

2. Edit the VSMSERVE AUTHLIST file on the A disk.
   The configuration statements in this file are column sensitive. There must be
   a user ID at column 1, ALL at column 66, and ALL at column 131. See
   Example 11-18.
   Repeat the existing line for VSMSERVE, and replace VSMSERVE with
   MAPAUTH on the new line. By repeating an existing line and replacing the ID,
   it is easy to maintain the correct column alignment,

   **Attention:** We are authorizing MAPAUTH to issue z/VM SM API
   commands, not MAPSERVE.

*Example 11-18  VSMSERVE AUTHLIST file (split in two chunks)*

```
|...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....|
|DO.NOT.REMOVE                                                   DO.NOT.REMOVE|
|MAINT                                                             ALL|
|VSMSERVE                                                          ALL|
|MAPAUTH                                                           ALL|
|**End of File**                                                  **End of File**|
```

3. Save the file and log off VSMSERVE.
TCP/IP configuration

Now create the MAPLAN guest LAN and set up z/VM TCP/IP to use it to allow MAPSERVE to communicate with the z/VM SM API.

To do this:

1. As MAINT, define the guest LAN that MAPSERVE will use to communicate with VSMSERVE. Grant MAPSERVE and TCP/IP authority to connect to it. Also grant MAPSERVE authority to connect to VSWITCH1 if you have not already. See Example 11-19.

Example 11-19  Create the guest LAN and grant access

```
DEFINE LAN MAPLAN OWNERID SYSTEM MAXCONN 2 RESTRICTED TYPE QDIO IP
LAN SYSTEM MAPLAN is created
Ready; T=0.01/0.01 11:15:08
SET LAN MAPLAN OWNERID SYSTEM GRANT TCPIP
Command complete
Ready; T=0.01/0.01 11:16:14
SET LAN MAPLAN OWNERID SYSTEM GRANT MAPSERVE
Command complete
Ready; T=0.01/0.01 11:16:19
SET VSWITCH VSWITCH1 GRANT MAPSERVE
```
2. Add the definitions in Example 11-20 to the z/VM SYSTEM CONFIG so that they will be there after an IPL.

*Example 11-20  Add guest LAN settings to SYSTEM CONFIG*

```
DEFINE LAN MAPLAN OWNERID SYSTEM MAXCONN 2 RESTRICTED TYPE QDIO IP
MODIFY LAN MAPLAN OWNERID SYSTEM GRANT TCPIP
MODIFY LAN MAPLAN OWNERID SYSTEM GRANT MAPSERVE
```

3. Also make sure that MAPSERVE is authorized to connect to the VSWITCH after an IPL by adding the following (Example 11-21) to SYSTEM CONFIG if you have not already.

*Example 11-21  Grant MAPSERVE access to VSWITCH1*

```
MODIFY VSWITCH VSWITCH1 GRANT MAPSERVE
```

4. As MAINT or TCPMAINT, add a .vnic statement to SYSTEM DTCPARMS on TCPMAINT’s 198 disk. This will define the virtual NIC that will allow z/VM TCP/IP to couple to the MAPLAN guest LAN.

*Example 11-22  vnic statement added to SYSTEM DTCPARMS*

```
00000 * * * Top of File * * *
00001 :************************************************************
00002 :* SYSTEM DTCPARMS created by DTCIPWIZ EXEC on 2 Jun 2006
00003 :* Configuration program run by MAINT at 13:55:50
00004 :************************************************************
00005 :nick.TCPIP    :type.server
00006                :class.stack
00007                :attach.2E20-2E22
00008                :vnic.C300 to system maplan
00009 * * * End of File * * *
```

5. Make the following changes to the TCP/IP config file on TCPMAINT’s 198 disk:

   a. Add an AUTOLOG section for PORTMAP and VSMSERVE.
   b. Uncomment the PORTMAP entries in the PORT section.
   c. Add a VSMSERVE entry in the PORT section.
   d. Note the IP address in the first column. The syntax of the PORT section allows IP addresses before the port number. (Yes, this does ruin the alignment, but that is okay.) The presence of an IP address before the port
number indicates that the service should only bind to that IP address. If there is no IP address before the port number, the service binds to all available IP addresses. This is how we are limiting VSMSERVE to only listen on the MAPLAN guest LAN.

e. Add DEVICE and LINK statements for the vnic that couples to the MAPLAN guest LAN.

f. Add the new vnic device’s IP information to the HOME section.

g. Add a START command for the new device.

Example 11-23  Enable PORTMAP and VSMSERVE in the TCP/IP config

```
* * * Top of File * * *

; - PROFILE TCPIP created by DTCIPWIZ EXEC on 2 Jun 2006
; - Configuration program run by MAINT at 13:55:48

ASSORTEDPARMS
PROXYARP
ENDASSORTEDPARMS

AUTOLOG
  PORTMAP 0  ; Portmap Server
  VSMSERVE 0  ; VM SMAPI Server
ENDAUTOLOG

OBEY
OPERATOR TCPMAINT MAINT MPROUTE ROUTED DHCPD REXECD SNMPD SNMPQE
ENDOBEY

PORT
  20  TCP FTPSERVE  NOAUTOLOG  ; FTP SERVER
  21  TCP FTPSERVE  ; FTP SERVER
  23  TCP INTCLIEN  ; TELNET Server
  25  TCP SMTP  ; SMTP Server
  53  TCP NAMESRV  ; Domain Name Server
  53  UDP NAMESRV  ; Domain Name Server
  67  UDP BOOTPD  ; BootP Server
  67  UDP DHCPD  ; DHCP Server
  69  UDP TFTP  ; TFTP (Trivial FTP) Server
  111 TCP PORTMAP  ; Portmap Server
  111 UDP PORTMAP  ; Portmap Server
```
; 143  TCP IMAP                      ; IMAP Server
; 161  UDP SNMPD                    ; SNMP Agent
; 162  UDP SNMPQE                   ; SNMPQE Agent
; 512  TCP REXECD                   ; REXECD Server (REXEC)
; 514  TCP REXECD                   ; REXECD Server (RSH)
; 515  TCP LPSERVE                  ; LP Server
; 520  UDP MPRROUTE NOAUTOLOG       ; Multiple Protocol Routing Server
; 520  UDP ROUTED                   ; RoutED Server
; 608  TCP UFTD                     ; UFT Server
; 750  TCP VMKERB                   ; Kerberos Server
; 750  UDP VMKERB                   ; Kerberos Server
; 751  TCP ADMSERV                  ; Kerberos Database Server
; 751  UDP ADMSERV                  ; Kerberos Database Server
172.16.0.1  845 TCP VSMSERVE       ; VM SMAPI Server
; 2049 UDP VMNFS                    ; NFS Server
; 2049 TCP VMNFS NOAUTOLOG          ; NFS Server
; 9999 TCP SSLSERVER                ; SSL Server - Administration

---------------------------------------------------------------------
DEVICE DEV@2E20  OSD 2E20 PORTNAME OSA2E20 NONROUTER
LINK OSA2E20D QDIOETHERNET DEV@2E20  MTU 1500

DEVICE NIC@C300  OSD C300 PORTNAME NICC300 NONROUTER
LINK NICC300D QDIOETHERNET NIC@C300  MTU 1500

; (End DEVICE and LINK statements)
---------------------------------------------------------------------
HOME
9.12.4.17  255.255.254.0 OSA2E20D
172.16.0.1  255.255.255.0 NICC300D
; (End HOME Address information)
---------------------------------------------------------------------
GATEWAY
; Network Subnet First Link MTU
; Address Mask Hop Name Size
---------------------------------------------------------------------
DEFAULTNET  9.12.4.92 OSA2E20D 1500
; (End GATEWAY Static Routing information)
---------------------------------------------------------------------
START DEV@2E20
START NIC@C300
; (End START statements)
---------------------------------------------------------------------
6. Restart the TCP/IP stack to make the changes take effect. Check that VSMSERVE and PORTMAP are automatically started when TCP/IP starts.

### 11.3.5 VMRM enablement

VM Resource Manager (VMRM) allows z/VM to dynamically adjust to changing workload priorities. VMRM will adjust the share settings of guests so that the guests under its control can meet their response time goals. This can be used to insure that a production environment is always given sufficient system resources even while a test environment is making demands on the z/VM system.

![VM Resource Manager Diagram](image)

VMRM uses a config file to describe the users that make up a workload and the resources that workload requires. In order for z/VM Center to make changes to this config file it must reside in the z/VM Shared File System. z/VM Center does not directly edit the file from the MAP system. Rather, it retrieves the file through a z/VM SM API call, makes changes, and then replaces the file with another
z/VM SM API call. This means that the VSMSERVE guest who runs the z/VM SM API must have access to the SFS space where the config file is kept.

1. Give z/VM Center access to the VMRM config file by running these commands as MAINT:

   ENROLL USER VSMSERVE
   GRANT AUTH VMSYS:VMRMSVM. TO MAPAUTH (WRITE NEWWRITE
   GRANT AUTH VMSYS:VMRMSVM. TO VSMSERVE (WRITE NEWWRITE

   **Attention:** We are authorizing MAPAUTH to issue alter the VMRM config file, not MAPSERVE.

2. Set up VMRMSVM so that it can access its config file in the SFS pool. Log on to VMRMSVM and add the following two lines to PROFILE EXEC on the A disk:

   "SET FILEPOOL VMSYS:
   "ACCESS VMSYS:VMRMSVM. C"

3. Save and then execute the PROFILE EXEC.

4. Create a new file VMRM CONFIG C that will contain the workload definitions. The file must have a syntactically correct set of statements for VMRM to be functional, even if there is no workload to define at this point. We create the file with dummy data so that we can modify it dynamically later with z/VM Center. See Example 11-24.

   **Example 11-24**   dummy VMRM CONFIG

   ADMIN MSGUSER VMRMADMN NEWCFG VMRM CONFIG VMSYS:VMRMSVM.
   WORKLOAD FWORK1 USER DUMMY
   GOAL FGOAL1 VELOCITY CPU 10 DASD 10
   MANAGE FWORK1 GOAL FGOAL1 IMPORTANCE 5

5. Save the file on the C disk.

6. Run the following commands to give VSMSERVE and MAPAUTH permission to alter the config file:

   GRANT AUTH * * C TO MAPAUTH ( WRITE
   GRANT AUTH * * C TO VSMSERVE ( WRITE

7. Issue #CP I CMS to check that VMRM starts correctly.

8. Log off VMRMSVM.

9. From MAINT run the following commands:

   XAUTOLOG VMRMADMN
   XAUTOLOG VMRMSVM
10. Add VMRMADMN and VMRMSVM to AUTOLOG1’s PROFILE EXEC (Example 11-25) so that they start automatically when the system IPLs.

**Example 11-25  AUTOLOG1’s PROFILE EXEC**

```
/****************************
/* Autolog1 Profile Exec */
/****************************

'CP XAUTOLOG VMSERVS'
'CP XAUTOLOG VMSERVU'
'CP XAUTOLOG VMSERVR'
'CP XAUTOLOG GCS'
'CP XAUTOLOG TCPIP'
'CP XAUTOLOG VSWCTL1'
'CP XAUTOLOG VSWCTL2'
'CP XAUTOLOG PVM'
'CP XAUTOLOG DIRMAINT'
'CP XAUTOLOG DATAMOVE'
'CP SLEEP 10 SEC'
'CP XAUTOLOG VMRMADMN'
'CP XAUTOLOG VMRMSVM'
'CP XAUTOLOG RSCS'
'CP ENA ALL'
'CP LOGOFF'
```

At this point, z/VM has been customized for z/VM Center.

### 11.4 Installing the Management Access Point

In this section we describe installing the following on the Management Access Point (MAP) server:

- IBM Director Agent for Linux on System z (including cimserver)
- z/VM MAP agent

Both components can be found on the IBM Director for Linux on System z server CD, which you can download in ISO format from the following URL (select **IBM Director 5.20** from the list):


Linux should be installed on the system that will host the MAP server. If both SLES and RHEL systems will be provisioned by the MAP, the MAP should be a SLES system. If the MAP is a RHEL system, then all SLES systems should have
ext2 or ext3 boot partitions. This is because RHEL does not support the Reiser file system at all, and the MAP system must be able to LINK and mount the boot partition of the systems that it provisions so that it can customize their IP address and host name.

**Attention:** SLES 9 and SLES 10 both ship with slpd enabled by default. This slpd will conflict with the one that the IBM Director agent will install and try to use, so it must be disabled through YaST's runlevel editing tool.

The installation steps are as follows:

1. Verify that the MAP should have two network interfaces. One network interface should be reachable by the IBM Director Server and the other interface should be on the MAPLAN guest LAN.

   In Example 11-26, eth0 is coupled to the VSWITCH with access to the outside world and the IBM Director server. eth1 is coupled to the MAPLAN guest LAN and is only used to interact with the z/VM SM API.

**Example 11-26  MAP network configuration**

```
mapserve:~ # ifconfig
eth0      Link encap:Ethernet  HWaddr 02:00:00:00:00:01
          inet addr:9.12.4.96  Bcast:9.12.5.255  Mask:255.255.254.0
          inet6 addr: fe80::200:0:300:1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1492  Metric:1
          RX packets:90199 errors:0 dropped:0 overruns:0 frame:0
          TX packets:43002 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16455002 (15.6 Mb)  TX bytes:27160343 (25.9 Mb)
eth1      Link encap:Ethernet  HWaddr 02:00:00:00:00:04
          inet addr:172.16.0.2  Bcast:172.16.0.255  Mask:255.255.255.0
          inet6 addr: fe80::200:0:300:4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1492  Metric:1
          RX packets:1270 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1194 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:289443 (282.6 Kb)  TX bytes:88028 (85.9 Kb)
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16365 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16365 errors:0 dropped:0 overruns:0 carrier:0
```
2. Add an entry to /etc/hosts so that when MAPSERVE contacts VMLINUX4 it will automatically use the MAPLAN guest LAN connection. The MAP system also needs to be able to resolve the IP address used to communicate with the z/VM SM API by the name of the VM system.

**Example 11-27   The modified /etc/hosts file**

```bash
mapserve:~ # vmcp q userid
MAPSERVE AT VMLINUX4
mapserve:~ # cat /etc/hosts
#
# hosts         This file describes a number of hostname-to-address
# mappings for the TCP/IP subsystem. It is mostly
# used at boot time, when no name servers are running.
# On small systems, this file can be used instead of a
# "named" name server.
# Syntax:
#
# IP-Address       Full-Qualified-Hostname   Short-Hostname
#
127.0.0.1       localhost

# special IPv6 addresses
::1             localhost ipv6-localhost ipv6-loopback
fe00::0         ipv6-localnet
ff00::0         ipv6-mcastprefix
ff02::1         ipv6-allnodes
ff02::2         ipv6-allrouters
ff02::3         ipv6-allhosts
9.12.4.96       mapserve.itso.pok.ibm.com mapserve
```
3. Once the network is working correctly, copy the following two files to mapserve:

   - IBM Director Agent for Linux on System z:
     dir5.20_agent_linux_s390_packagedIU.zip
   - IBM Director z/VM MAP Agent:
     dir5.20_zvmmapagent_linux_s390_packagedIU.zip

Both files can be found on IBM Director Agents and Consoles CD 1 as well as the IBM Director for Linux on System z server CD. You can download the latter in ISO format from the following URL (select IBM Director 5.20 from the list):


The Director Agent package contains the cimserver that will be needed on the MAP system. It also contains the Java agent for full IBM Director management support.

It is also acceptable to install the IBM Director Core Services package from the agents CD (cs5.20_agent_linux_s390_packagedIU.zip) instead of the full IBM Director Agent package.
Figure 11-10 shows how the cimserver and z/VM MAP agent reside on mapserve.

4. If necessary, unzip the Agent package on mapserve.

5. View the contents of the diragent.rsp response file in director/agent/Linux/s390/FILES. The response file settings indicate the components that will be installed by default.

*Example 11-28*  Unpack the agent

```bash
cat
mapserve:~ # unzip dir5.20_agent_linux_s390_packagedIU.zip
Archive: dir5.20_agent_linux_s390_packagedIU.zip
  creating: director/agent/linux/
  creating: director/agent/linux/s390/
  creating: director/agent/linux/s390/FILES/
  inflating: director/agent/linux/s390/FILES/dir5.20_agent_linz.sh
  inflating: director/agent/linux/s390/FILES/diragent.rsp
  creating: director/agent/linux/s390/META-INF/
  inflating: director/agent/linux/s390/META-INF/dir5.20_agent_linz_de.xml
  inflating: director/agent/linux/s390/META-INF/dir5.20_agent_linz_en.xml
  inflating: director/agent/linux/s390/META-INF/dir5.20_agent_linz_es.xml
  inflating: director/agent/linux/s390/META-INF/dir5.20_agent_linz_fr.xml
```
inflating:
director/agent/linux/s390/META-INF/dir5.20_agent_linz_installArtifact.xml
inflating: director/agent/linux/s390/META-INF/dir5.20_agent_linz_ja_JP.xml
inflating: director/agent/linux/s390/META-INF/dir5.20_agent_linz_ko.xml
inflating: director/agent/linux/s390/META-INF/dir5.20_agent_linz_packagedIU.xml
inflating: director/agent/linux/s390/META-INF/dir5.20_agent_linz.xml
inflating: director/agent/linux/s390/META-INF/dir5.20_agent_linz_zh_CN.xml
inflating: director/agent/linux/s390/META-INF/dir5.20_agent_linz_zh_TW.xml

mapserve:~ # cd director/agent/linux/s390/FILES/
mapserve:~/director/agent/linux/s390/FILES # cat diragent.rsp

# IBM Director Agent (Linux for zSeries) Install Response File
#    A '#' in the first column indicates a comment statement
#    This response file is used by invoking Setup in one of the
#    following ways:
#
#     dir5.10_agent_linz.sh
#     Installs with the defaults. This response file
#     is ignored.
#     dir5.10_agent_linz.sh -r "filename"
#     Installs using the options in the given file.
#
#===============================================================================
#
# SRCDIR = the location where the Director RPMs can be
#    found. If the RPMs are in the same directory as
#    this script, leave SRCDIR as is.
#
# SRCDIR=`pwd`
#
# LogFile = the location for a file that captures the
#    results of the installation; if LogFile line starts
#    with a #, no log will be created
#
# LogFile=/var/log/dirinst.log
#
# DebugInstall = set to 1 to obtain very verbose logging
#    information from the installation
#
# DebugInstall=0
#
# The following components are required. However, if the
# current version is already installed, you may specify
# 0 to not install them.
#
# DirectorCimCore=1
zSeriesCoreservices=1
ITDAgent=1
zSeriesAgentExt=1

# CIM Repository upgrade
CIMRepositoryUpgrade=0
mapserve:~/director/agent/linux/s390/FILES #

6. Run the install script to install the IBM Director Agent with all of the defaults.

Example 11-29  Install the agent

mapserve:~/director/agent/linux/s390/FILES # ./dir5.20_agent_linz.sh

./dir5.20_agent_linz.sh self-extracting installation program... Please wait...

******************************************************************************
This Program is licensed under the terms of the agreement located in the license file in the Program's installation license folder or in the license folder on the source media. By installing, copying, accessing, or using the Program, you agree to the terms of this agreement. If you do not agree to the terms, do not install, copy, access, or use the Program.
******************************************************************************

Attempting to install ITDAgent-5.20-1.s390.rpm
Preparing...  ################################################################
ITDAgent  ################################################################

Interprocess communications data are encrypted by default. Run /opt/ibm/director/bin/cfgsecurity to remove this setting.

To start the IBM Director Agent manually, run /opt/ibm/director/bin/twgstart

Attempting to install IBMCimCore-5.20-1_SLES9.s390.rpm
Preparing...  ################################################################
IBMCimCore  ################################################################

Creating SSL certificate and private key
Compiling MOF files...

Finished compiling MOF files.
Starting SLP ....
Starting IBM SLP SA:
please wait ......
..done
Starting Pegasus CIM Listener ..done
Starting Pegasus CIM Object Manager ..done
Attempting to install IBMCimExt-5.20-1_SLES9.s390.rpm
Preparing...                                                     ##########################################
IBMCimExt                                                        ##########################################
Compiling MOF files...

Subscribing default handlers ...
Finished subscribing default handlers.
Attempting to install DirectorCimCore-5.20-1_SLES9.s390.rpm
Preparing...                                                     ##########################################
DirectorCimCore                                                  ##########################################
Compiling MOF files...

Shutting down Pegasus CIM Object Manager ..done
Starting Pegasus CIM Object Manager ..done
Starting SLP Attributes
Attempting to install zSeriesCoreServices-level1-5.20-1_SLES9.s390.rpm
Preparing...                                                     ##########################################
zSeriesCoreServices-level1                                       ##########################################
Configuring registration MOF files...
Finished configuring registration MOF files.
Compiling mof files ...

Attempting to install zSeriesAgentExt-5.20-1.s390.rpm
Preparing...                                                     ##########################################
zSeriesAgentExt                                                  ##########################################

No repository backup has been created during this script run.

Installation of selected components is successful.
mapserve:~:/director/agent/linux/s390/FILES #

7. Once the installation completes, use the `ps axf` command, which should show the four new processes shown in Example 11-30 running.

```
Example 11-30    Output of ps axf

<table>
<thead>
<tr>
<th>PID</th>
<th>State</th>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>8517</td>
<td>Ss</td>
<td>0:00</td>
<td>/opt/ibm/icc/cimom/../slp/bin/slp_srvreg</td>
</tr>
<tr>
<td>8533</td>
<td>Ssl</td>
<td>0:00</td>
<td>./cimlistener -D ..</td>
</tr>
<tr>
<td>8670</td>
<td>Ssl</td>
<td>0:00</td>
<td>./cimserver -D ..</td>
</tr>
<tr>
<td>8691</td>
<td>Ss</td>
<td>0:00</td>
<td>/opt/ibm/director/cimom/bin/tier1slp</td>
</tr>
</tbody>
</table>
```

These processes are the cimserver itself, a listener process for the cimserver, and the SLP registration daemons for the cimserver.
8. Start the Java portion of the IBM Director agent with the following command:
   
   /opt/ibm/director/bin/twgstart

9. Run `ps axf` again, which should now show the Java threads of the IBM Director Agent:

   **Example 11-31  Output of ps axf**

<table>
<thead>
<tr>
<th>PID</th>
<th>Status</th>
<th>Time</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>8960</td>
<td>Ss</td>
<td>0:00</td>
<td>/opt/ibm/director/bin/daemonize /opt/ibm/director/jre</td>
</tr>
<tr>
<td>8961</td>
<td>Sl</td>
<td>0:04</td>
<td>_ /opt/ibm/director/jre/bin/java -Xms8m -Djava.home</td>
</tr>
</tbody>
</table>

10. If necessary, unzip the z/VM MAP agent.

11. View the contents of the zvmmagent.rsp response file. The response file indicates the default setting that will be applied for the install.

   **Example 11-32  Unpack the z/VM MAP agent**

   ```bash
   mapserve:~ # unzip dir5.20_zvmmagent_linux_s390_packagedIU.zip
   Archive:  dir5.20_zvmmagent_linux_s390_packagedIU.zip
     creating: director/zvmmagent/linux/
     creating: director/zvmmagent/linux/s390/
     creating: director/zvmmagent/linux/s390/FILES/
   inflating: director/zvmmagent/linux/s390/FILES/dir5.20_zvmmagent_linz.sh
   inflating: director/zvmmagent/linux/s390/FILES/zvmmagent.rsp
     creating: director/zvmmagent/linux/s390/META-INF/
   inflating: director/zvmmagent/linux/s390/META-INF/dir5.20_zvmmagent_linz_de.xml
   inflating: director/zvmmagent/linux/s390/META-INF/dir5.20_zvmmagent_linz_en.xml
   inflating: director/zvmmagent/linux/s390/META-INF/dir5.20_zvmmagent_linz_es.xml
   inflating: director/zvmmagent/linux/s390/META-INF/dir5.20_zvmmagent_linz_fr.xml
   inflating:
   director/zvmmagent/linux/s390/META-INF/dir5.20_zvmmagent_linz_installArtifact.xml
   inflating:
   director/zvmmagent/linux/s390/META-INF/dir5.20_zvmmagent_linz_ja_JP.xml
   inflating: director/zvmmagent/linux/s390/META-INF/dir5.20_zvmmagent_linz_ko.xml
   inflating:
   director/zvmmagent/linux/s390/META-INF/dir5.20_zvmmagent_linz_packagedIU.xml
   inflating: director/zvmmagent/linux/s390/META-INF/dir5.20_zvmmagent_linz.xml
   inflating:
   director/zvmmagent/linux/s390/META-INF/dir5.20_zvmmagent_linz_zh_CN.xml
   inflating:
   director/zvmmagent/linux/s390/META-INF/dir5.20_zvmmagent_linz_zh_TW.xml
   mapserve:~ #
   mapserve:~/director/zvmmagent/linux/s390/FILES # cat zvmmagent.rsp
   # z/VM MAP-Agent (Linux for zSeries) Install Response File
   #   A '#' in the first column indicates a comment statement
# This response file is used by invoking Setup in one of the following ways:
#
# dir5.10_zvmmagent_linz.sh
#       Installs with the defaults. This response file is ignored.
# dir5.10_zvmmagent_linz.sh -r "filename"
#       Installs using the options in the given file.
#
#=================================================================================
#
# SRCDIR = the location where the Director RPMs can be found. If the RPMs are in
#     the same directory as this script, leave SRCDIR as is.
#
# SRCDIR=`pwd`
#
# LogFile = the location for a file that captures the results of the installation;
#     if LogFile line starts with a #, no log will be created
#
# LogFile=/var/log/dirinst.log
#
# DebugInstall = set to 1 to obtain very verbose logging information from the
#     installation
#
# DebugInstall=0
#
# The following components are required. However, if the current version is
#     already installed, you may specify 0 to not install them.
#
# zVMMAP=1
#
# CIM Repository upgrade
# CIMRepositoryUpgrade=1
# mapserve:~/director/zvmmagent/linux/s390/FILES #
12. Run the z/VM MAP agent install script to install the z/VM MAP code into the cimserver.

Example 11-33  Install the z/VM MAP agent
mapserve:~/director/zvmmapagent/linux/s390/FILES # ./dir5.20_zvmmapagent_linz.sh

./dir5.20_zvmmapagent_linz.sh self-extracting installation program... Please wait...

Attempting to install zVMMAP-5.20-1_SLES9.s390.rpm
Preparing...  #################################################################
+-----License information--------------------------------------------+
In order to execute a z/VM Center Director task against the z/VM Manageability Access Point, you must purchase a license with sufficient authorizations to the z/VM Center feature of the IBM Director for Linux on System z and accept the applicable license agreement.
+--------------------------------------------------------------------+
zVMMAP  #################################################################
Planned value for the property providerDir is set to "/opt/ibm/icc/cimom/lib:/opt/ibm/director/cimom/lib:/opt/ibm/zvmmap/lib" in CIMServer.
Shutting down Pegasus CIM Object Manager ..done
Starting Pegasus CIM Object Manager ..done
zvm-mgmtslp  0:off 1:off 2:off 3:on 4:on  5:on  6:off
Starting z/VM Management SLP registration daemon: zvm-mgmtslpd.
No repository backup has been created during this script run.

Installation of selected components is successful.

mapserve:~/director/zvmmapagent/linux/s390/FILES #

13. Run the ps axf command, which should now show the following new process (Example 11-34).

Example 11-34  Output of ps axf command
9490 ? Ss 0:00 /usr/bin/perl /usr/sbin/zvm-mgmtslpd -f /etc/zvm-mgmt

This process is the SLP daemon for the z/VM MAP agent.

Since our MAP has two network interfaces, we need to guarantee that the z/VM MAP code will recognize which interface it uses to talk to the IBM Director server. By adding the VMLINUX4 entry to /etc/hosts, it already knows how to talk to the z/VM system.

14. Open file /etc/zvm-mgmtslp/daemon.conf on mapserve and change the slp.service.interfaces setting to list the IP address that is used to contact the IBM Director server. In our case, this is eth0’s IP address.
Implementing IBM Director 5.20

### Example 11-35 Edit /etc/zvm-mgmtslp/daemon.conf

```bash
# slp.service.interfaces = <ipaddress[:port][,ipaddress[:port]][, ...]>
#
# This setting contains a list of ipaddress and port information.
# These address information is used to compose the SLP service: URL
# host part. For each ipaddress:[port] entry a SLP service will be
# registered.
#
# Default:
# slp.service.interface
# slp.service.interfaces = 9.12.4.96
```

15. Restart the zvm-mgmtslp daemon with the command shown in Example 11-36.

### Example 11-36 Restarting the zvm-mgmtslp daemon

```bash
mapserve:/etc/zvm-mgmtslp # /etc/init.d/zvm-mgmtslp restart
Restarting z/VM Management SLP registration daemon: zvm-mgmtslpd.
mapserve:/etc/zvm-mgmtslp #
```

The z/VM MAP is now configured to talk to both z/VM and the z/VM Center on the IBM Director server.

### 11.5 Installing the z/VM Center extension

Now you need to install the z/VM Center extension on your management server (running IBM Director Server) and each of your management consoles (running IBM Director Console).

You can download the code as described below, but you will need to purchase a license before you can use it. You can order z/VM Center, product number 5648-DR1, via ShopzSeries:

http://www.ibm.com/software/ShopzSeries
Figure 11-11 illustrates the installation location of the z/VM Center extensions on the IBM Director management server and console.

The z/VM Center extension is available for download from the following page. Select **IBM Director 5.20** from the list, sign in using your IBM registration ID, then select the appropriate operating system:


Do the following for your IBM Director Server system and each management workstation where you have IBM Director Console installed:

1. Copy the z/VM Center extension package to the IBM Director management server, or make it available through a network share.

2. Unpack the package and run the install file. (For IBM Director Server on Windows, this installer is zVMCenterServerExt_5.20_windows.exe.)

The z/VM Center extension for IBM Director on Windows platforms uses the standard InstallShield packaging and windows. There are no configuration decisions to make during installation other than the installation directory (it should detect and install in the IBM Director installation directory).
3. If you are installing the code on the management server, then when the installation is finished and you are prompted to reboot, click **No**. Do **not** reboot at this point, as we first need to supply a license key for the z/VM Center extension.

4. Edit the file `ZvmCenter.properties` with a text file. This file is in the IBM Director proddata directory (on Windows, this directory is by default, `c:\Program Files\IBM\Director\proddata`). If the file does not exist, then create it, but be sure that the name is correct and has the correct case (Linux and AIX are case sensitive).

5. Add the line `VSDandSC.Task.Licence =` followed by your z/VM Center license key. See Figure 11-12.

```
VSDandSC.Task.Licence = YOURLICENSE#
```

*Figure 11-12  License key file*

6. Save the changes.

**Tip:** Ensure that you spell the file name (`ZvmCenter.properties`) correctly, and for Linux and AIX systems ensure that the case is correct as well. Check it and the contents of the file if you get any licensing errors.

Also check that Windows Explorer is not hiding the file extensions. The file that was created may have been named `ZvmCenter.properties.txt`, and the `.txt` extension may be hidden.

7. Reboot the server after saving the license file.
8. Once the server is back, log in to the IBM Director Console and check for the z/VM Center tasks at the bottom of the tasks pane.

![Figure 11-13  z/VM Center tasks](image)

9. Repeat the installation on any other management consoles you have running IBM Director Console.

11.6 Verifying the installation and initial setup

Now that the components are installed, the next step is to add the appropriate systems to IBM Director Console:

1. Discover or manually add mapserve as a normal managed server object. It is a Linux Server running a cimserver, so it will be at least a Level-1 managed object. If you chose to install the full Director agent, it will be a Level-2 managed object.

2. To gain access to the mapserve, right-click the object and click **Request Access**. Enter the root user ID and password.
3. Discover the z/VM system that it represents. Discovery can be problematic when there are many network hops between Director Server and the MAP system. It may be necessary to manually add the z/VM system using **Console ➔ New ➔ Managed Objects ➔ z/VM Systems**, as shown in Figure 11-14.

![Add z/VM Systems](image)

*Figure 11-14  Add z/VM system to IBM Director Console manually*

4. Enter the IP address of mapserve and the name of the z/VM system, then click **OK**.

5. Once the z/VM system is in IBM Director Console, right-click the icon and click **Request Access** to access the system.
6. Drag and drop the z/VM Virtual Server Deployment task to the VM system object, as shown in Figure 11-15.

Figure 11-15   Launch the Server Deployment task on the z/VM system
The UI for the Server Deployment task appears (Figure 11-16).

7. Check the specifics of the system to ensure connectivity. If the Memory field matches the total amount of main storage that is available to the z/VM System, and the Computer System field contains the correct processor ID, then the z/VM MAP is able to query the z/VM system itself for status.

If the Memory field displays the memory size of the MAPSERVE guest itself rather than the memory size of the entire z/VM System, then the custom privilege class settings are not allowing the MAPSERVE guest to issue the query command with the system level authority that it needs. From the root user on MAPSERVE, issue `vmcp q v store` and compare the response with `vmcp q store`. If the storage sizes indicated are equal, then go back to 11.3.2, “Define a custom user class” on page 588, check that the indicated changes were made correctly in the system config file, and re-issue the CP commands as MAINT.
8. Expand the z/VM system (VMLINUX04 in our example), as shown in Figure 11-17, and click **z/VM Profile**.
9. Click **Configure**. Figure 11-18 appears.

![Set User ID and Password](image)

**Figure 11-18** Set the z/VM MAP system credentials

10. Change the user ID to MAPAUTH.
11. Enter the password for MAPAUTH.
12. Ensure that the VSMSERVE Server field points to the z/VM system by name (VMLINUX4 in our example).
13. Click **Finish**. The z/VM Profile is now displayed, as shown in Figure 11-19.

![z/VM Profile disk pool setting](image)

**Figure 11-19**  z/VM Profile disk pool setting

14. Specify the correct disk pool. Select **POOL0** from the Disk Pool drop-down selection box (see Figure 11-19). This setting will let z/VM Center pre-populate any field for choosing a disk pool with POOL0.

15. Click **Save**.
16. In the z/VM System tree pane, expand **z/VM Virtual Servers**. z/VM Center will query mapserve to get the list of all of the users on the z/VM system.

*Figure 11-20  Virtual servers on your z/VM system*
17. Scroll down in the list until you find **VMLINUX4.MAPSERVE** and select it. Figure 11-21 appears.

![z/VM Virtual Server Deployment: VMLINUX4](image)

**Figure 11-21** MAPSERVE properties

18. Check the status icon. If mapserv is a green triangle then the system is active. Active in z/VM Center terms means that the guest is logged on to the z/VM system.

If the status is showing green for mapserv and all the guests are browseable, then z/VM Center is correctly installed and configured.

### 11.7 General usage

There are two main tasks:

- The z/VM Center Virtual Server Deployment task allows you to capture the operating system running on a virtual server (VS) as an OS template, create
virtual server templates, create new virtual servers from those templates, and provision OS templates into the new virtual servers.

- The z/VM Center server complexes task allows you to create groups of virtual servers known as server complexes and manage their properties at the group level.

The server complexes task makes use of the VS and OS templates that are defined in the virtual server deployment task. The server complexes task also provides the ability to create a new virtual server, provision an OS template into the virtual server, and set the properties of that virtual server with one drag-and-drop action.

Furthermore, this action can be repeated as many times as there are resources available—providing the ability to provision an entire farm of Linux systems with a single drag-and-drop action.

### 11.7.1 Virtual Server Deployment

Virtual Server Deployment (VSD) provides the ability to define the following resources to z/VM Center for use in managing Linux systems:

- **Virtual server template**
  
  A virtual server template is a set of common definitions that are applied when defining a new virtual server. Memory size, number of virtual CPUs, user class, password, directory prototype, and user ID pattern are the fields that can be set in the virtual server template.

  There are many more options that can be set in a z/VM directory entry than are available in the virtual server template. To set these options, a directory prototype must be created and stored on DirMaint. This directory prototype can then be used in a virtual server template.

- **Virtual server**

  In VSD terms, a virtual server is analogous to a z/VM user. It correlates to the z/VM directory entry for a Linux guest. z/VM Center reads the z/VM directory entry for a given user to populate the properties fields within VSD when a system is selected.

  Virtual servers are created from virtual server templates. Once a virtual server is created, VSD does not have the ability to make changes to its virtual hardware configuration in the z/VM directory.

- **Operating system**

  An operating system is associated with a virtual server. It defines the disks that contain the OS, the network devices and settings for that server, and the server's host name.
An operating system is created in VSD manually by registering the OS properties of a virtual server system that already has an OS installed, or automatically when an OS template is applied to an empty virtual server.

**Operating system template**

An operating system template is a copy of the disks that contain an operating system. These disks are defined to a NOLOGed user ID on the z/VM system, and information regarding the IPL device and network devices is kept in a tagged comment in the directory entry.

**Virtual server template**

Before creating new virtual servers, there must be a virtual server template. To create a virtual server template, do the following:

1. From VSD, select the **Virtual Server Templates** item in the Provisioning Resources panel on the bottom left pane, then click **New**.

![Figure 11-22  Select virtual server template](image-url)
Figure 11-23 appears.

![Create Virtual Server Template on z/VM System: VMLINUX4]

Figure 11-23  Virtual server template specifics

2. Review the fields in Figure 11-23.

The user ID that is created as a result of using this template is created according to the pattern in the User ID Pattern field. All text up to the asterisk (*) is taken as is, and the asterisk is converted to a number counting up from 1 and padded to fill the ID to eight characters.

In the above example, the first ID created will be lnxz0001. The next would be lnxz0002, lnxz0003, and so on. The ID can also be completely specified, in which case this VST will only be useful one time.

The Prototype field is used to specify which directory prototype file to copy statements from. This is the only way to get directory entries for things like CRYPTO APVIRT or IUCV settings.

The rest of the fields are input directly into their corresponding places in the z/VM Directory. Click Next.
3. Choose a name for the Virtual Server template and fill in some description text. Good things to include here are CPU and memory settings, as well as the directory prototype that was used, if any.

![Create Virtual Server Template on z/VM System: VALinux4](image)

**Figure 11-24  VST Name and Description**

4. Click **Finish**.
The Virtual Server Template is now saved on the MAP server in the CIM repository. There is no entry in the z/VM directory for the Virtual Sever Template.

**Figure 11-25  Available Virtual Server Templates**

**Note:** If the CIM repository on the MAP server is damaged, the Virtual Server Templates will be lost. Make sure to back up the CIM repository in /opt/ibm/icc/cimom/repository before upgrading software on the MAP system. Instructions for this are available in the IBM Director Information Center.
Virtual server

Now that there is a virtual server template, create a new virtual server using that template, as follows:

1. Select z/VM Virtual Servers in the z/VM System pane on the top left. z/VM Center will query the MAP server to get a list of all of the IDs on the z/VM system and display them as a list of virtual servers in the right side of the window. See Figure 11-26.

![Figure 11-26 Select Virtual Servers](image-url)
2. Click **New**. Figure 11-27 appears.

![Figure 11-27 Choose the template](image1)

3. z/VM Center displays a list of all of the available Virtual Server templates on the z/VM MAP. Choose a Virtual Server template and click **Next**. Figure 11-28 appears.

![Figure 11-28 Override some settings](image2)
Virtual Server Deployment (VSD) shows the UserID pattern that will be used to create the new virtual server. The UserID pattern as well as the password and description can be overridden in this panel. The z/VM Virtual Server field can be used to name this virtual server something other than the default `<vmsystem>.<userid>`.

4. Make any necessary changes and click **Finish**.

5. VSD will build a new directory prototype based on the settings chosen in the panels and the settings that exist in the prototype that was specified in the virtual server template.

6. VSD then scans the z/VM directory to see what the next available ID is in the sequence defined by the User ID Pattern field in the virtual server template. In this example, this is the first virtual server based on this template, so it chooses LNXZ0001, as shown in Figure 11-29.

![z/VM Virtual Server Deployment: VMLINUX4](image)

*Figure 11-29  An empty virtual server*
7. VSD creates the virtual server in the z/VM directory. VSD does not allocate any minidisks or network devices when creating a virtual server, as shown in Figure 11-30.

**Note:** The only fields that can be changed in VSD’s display for a virtual server are the Description field and the Virtual Server name field. All of the other fields are read only. VSD cannot make changes to a virtual server once it has been created.

Adding network devices and minidisks is done as part of provisioning an OS template into the virtual server. LNXZ0001 has no operating system yet, so it is not very useful at this point.

**Operating system**

The operating system for an existing virtual server must be defined to z/VM Center before an operating system template can be captured. The process of defining an operating system to z/VM Center is called *registration*.
We will register the operating system properties for an existing guest that is already running Linux in the following steps. This guest will be the master Linux image.

1. In the z/VM System pane, select the guest that will be used as the master image and expand it to display Operating Systems.
2. Select the **Operating Systems** group, then click **Action → Register Operating System**. Figure 11-32 appears.

![Registration System Disks panel](image)

*Figure 11-32  OS Registration System Disks panel*

3. In the System Disks panel, check the disks that are needed by the operating system. This includes any disks for the operating system itself, user data, or application data.

Any disks that are checked here will be copied to the OS template when it is created later. There is no need to check disks that are used for swap devices or other data that is created anew when the server starts. Swap disks can be created by the DirMaint Directory Prototype when the VS is created.
4. Click **Next**.

   If multiple disks were selected, the Boot Disk panel will appear where you select which volume is the boot volume. If only one disk was selected, the boot menu is skipped and the IP Addresses panel appears.

*Figure 11-33  OS Registration IP addresses panel*
5. Fill in the interface name and IP address for the devices listed in the IP Addresses panel. If either the interface name or IP address is entered, the other must also be entered. Leaving both blank is allowed if you do not want this port to be defined as in use by this OS. Click Next.

![OS Registration Hostname panel](image)

Figure 11-34 OS Registration Hostname panel

6. Fill in the fully qualified host name, and enter a description of this OS if desired. Click Finish.
The operating system is now registered and appears under Operating Systems in Figure 11-35.

![z/VM Virtual Server Deployment: VMLINUX4](image)

**Figure 11-35  A registered OS**

**Tip:** z/VM Center takes the information entered in the panels and stores it in the z/VM directory entry for the virtual server as a *CIMGOS01: tagged comment.

### Operating system template

Now that the master image has its OS registered with z/VM Center, we can create an OS template from it.

One last item to check before creating the OS template is to ensure that the Personalization package zVMPersonalization-5.20-1.s390.rpm is installed on the master system. This package is available on the director server as part of the z/VM Center extension, under the main IBM Director install directory in proddata/zVMCenter.
Copy the personalization package to the master image and install it as shown in Example 11-37.

**Example 11-37  Installing the personalization rpm**

```bash
[root@lnxrh4 ~]# rpm -ivh zVMPersonalization-5.20-1.s390.rpm
Preparing...  #################################### [100%]
  1:zVMPersonalization  #################################### [100%]
[root@lnxrh4 ~]#
```

The personalization package is a shell script that will be used by newly cloned virtual servers to configure their host names and network interfaces the first time they are started.

Once the personalization package is installed, create the OS template from the master image, as follows:

1. Select the **Operating System Templates** object in the Provisioning Resources pane (Figure 11-36).
2. Click **New**. Figure 11-37 appears.

![Available servers](image)

*Figure 11-37  Available servers*
3. The list of available virtual servers appears in the right pane. Scroll to the virtual server that is running the master Linux image, expand it, and select the OS that is registered on that system. Click **Next**. Figure 11-38 appears.
4. The list of disks that were selected as essential disks when the OS was registered appears. Select any disk that is to be shared read-only among all virtual servers to be provisioned from this OS template. Do not select the boot volume to be shared as read only.

Click **Next**. Figure 11-39 appears.

![Create Operating System Template on z/VM System: VMLINUX4](image)

*Figure 11-39  OS template name*
5. Name the OS template. This is the name that will appear in the Operating System Templates list in VSD.

You also have the option of choosing the user ID that will be created to contain this OS template. If this is not specified, then VSD will automatically choose an ID based on the ID of the master system.

You may also optionally enter some description text.

Click **Next**.
6. Choose a disk pool to contain the OS template. Click **Next**.

![Create Operating System Template on z/VM System: VMLINUX4](image)

Figure 11-41  Active check

7. Before creating a copy of the disks for the OS template, the master image must be shut down and logged off z/VM. If the server is active, click the **Deactivate** button. z/VM Center will issue a command to have z/VM shut down the master image, and the icon will change its status.

8. When the master image status changes to inactive, click **Finish**.
9. z/VM creates a user ID and minidisks using DirMaint to contain the OS template. It then uses the DirMaint clonedisk command to copy the master image’s disks to the OS template’s disks. This process can take some time if the master image has many large disks and the storage subsystem does not support a fast copy mechanism. DirMaint must also be configured to take advantage of the fast copy services provided by the storage subsystem. If FastCopy services are not available, or DirMaint is not configured to use them, it will use DDR instead.

Figure 11-42  New OS template
Once the copy processing is complete, the new operating system template will appear in the OS Templates list under Provisioning resources, as shown in Figure 11-42 on page 644.

The OS template is a NOLOGed z/VM guest with some minidisks attached to it and a special tagged comment in its z/VM directory entry. The minidisks are copies of the master image’s minidisks.
Provision an OS template to the empty virtual server

Now that we have an OS template, the next step is to provision it into an empty virtual server:

1. Select the virtual server that was created previously (for us, VMLINUX4.LNXZ0001) and expand it to show the operating systems group object.
2. There is no operating system on this Virtual Server yet, so the list is empty. Click **New**. Figure 11-45 appears.

3. Select the OS template to be provisioned into this virtual server and click **Next**.

4. Fill in the IP addresses for the new virtual server. All IP addresses must be filled in. It is not possible to change anything but the IP address when using
VSD to provision a new operating system using an operating system template. All clones will be connected to the same network devices as the master image.

If the master image is using dedicated OSA or HiperSocket devices, VSD will choose available OSA or HiperSocket devices and dedicate them to the new clones. VSD only checks if an OSA or HiperSocket device is available by scanning the z/VM directory for it. If it is not in the z/VM directory, VSD considers it available.

This is why we had to create the $DEVICE$ user who has DEDICATE statements for all of the dynamically attached OSA devices for TCP/IP and VSWITCH1.

If the master image was using a virtual NIC coupled to a vswitch or guest LAN, the clones will have a NIC with the same device numbers on the same virtual networks.

Click **Next**. Figure 11-47 appears.

5. Choose the disk pool that will contain the new disks for the virtual server.
Click **Next**.

**Note:** A minidisk must be allocated as contiguous chunk on a single volume. Even if the remaining managed space value is large enough to contain a minidisk, the max allocatable space value is the one that determines the largest single minidisk that can be allocated. It is possible to have tens of GBs of free space, but have it so fragmented across so many volumes that it is not possible to allocate a single 2.5 GB minidisk. The only way to resolve this is to add more volumes to the pool or to shut down systems and manually defragment the volumes by moving the minidisks around.

6. Set the fully qualified host name of the new virtual server. Click **Finish**. The OS template copy now begins.

An error may occur if a network device or minidisk exists at the virtual address specified by the OS template. This can happen if a previous clone operation failed before completing, or if you try to clone multiple OS templates into the same virtual server.
**Tip:** If the OS template was created just minutes ago, and the storage subsystem uses a fast copy technology, it is possible that the disks for the OS template are still being copied in the background even though the fast copy command completed. If this is the case, the creation of the new virtual server will use DDR since a new fast copy operation is not able to copy from the OS template disk that has not finished the previous fast copy operation.

Figure 11-49  The new virtual server and its operating system

7. The new virtual server now has an operating system, and it can be activated by selecting the virtual server and clicking **Action → Activate**.

You are able to log in to the new virtual server in a few moments once it has completed its personalization process and started its network interfaces.
Once activated, the status indicator for the virtual server indicates that it is up and running, as shown in Figure 11-50.

*Figure 11-50  After Activation*
The overall layout of the system as it is now is shown in Figure 11-51.

11.7.2 Server complexes

The server complexes task provides the ability to define a container called a server complex that has properties associated with it. All virtual servers in a server complex inherit these properties. In addition, a server complex can consist of up to four sub groups called tiers. The use of tiers allows some default properties to apply to all systems within a server complex and more specific properties to apply to some systems within a tier in the server complex. There is no predefined relationship or hierarchy between tiers, other than that they are part of the same server complex.

All properties can be set with the scope of a whole server complex or a specific tier within a server complex. Settings made at a specific tier take precedence over settings made for the whole server complex.

The properties that can be set in a server complex are:

- **VMRM**
  
The VM Resource Manager (VMRM) property allows a server complex or a tier to have an entry made within the VMRM config file. The entry will define
all of these systems as part of the same workload with the same CPU, DASD, and importance settings.

VMRM will then monitor the CPU and DASD utilization data from the z/VM Monitor stream to determine whether the goals are being met. If it determines that the goals are not being met, VMRM will dynamically change the z/VM relative share values for the guests under its control until the workload is meeting its goals.

**Important:** Changing property values can lead to unexpected behavior, since VMRM manages the CPU and DASD performance of a workload as a whole.

If multiple systems are in the same workload for VMRM, their CPU and DASD throughput are aggregated together for comparison against the defined goals. If the goals are not met, VMRM adjusts the share value of one system at a time per adjustment interval until the goals are met. This can lead to strange min/max issues where one system in a workload gets a share value of 3 while another gets a share value of 10000. The workload as a whole may be meeting its defined goals, but the individual systems are not balanced relative to each other.

If the VMRM support is going to be used, it may be best to limit the configuration to one virtual server per tier and define an explicit set of goals for each tier.

- **Scripts**

  The scripts property allows a server complex or a tier to have a particular script run on virtual servers when they enter or leave a server complex or tier.

  If a system is moved into the group, the *On the Entering Guest* script is run after the guest enters the server complex. This script can reside either on the guest or on the server. If the script resides on the server it is copied to the guest before it is run.

  If a system is moved out of the group, the *On the Leaving Guest* script is run before the guest leaves the server complex. This script can reside either on the guest or on the server. If the script resides on the server it is copied to the guest before it is run.

- **Network**

  The network property provides the ability to define up to four network interfaces per virtual server. The definition is common to all guests within an server complex or tier.
The network properties of the z/VM System itself must be defined to the SC task before the setting can be made within a particular server complex.

- Minidisks

The minidisks property provides the ability to define a shared minidisk that all systems within an server complex or tier will have access to.

**z/VM server complex networking properties**

In this section we describe how to define the network resources that will be used by the server complex.

1. Open the server complexes task.
2. Click **Action → z/VM Networking Properties** to open the server complexes Network configuration panel. The panel that opens has tabs for the three network device types supported by z/VM Center.

---

*Figure 11-52  z/VM Networking Properties*
3. Click **Action → Refresh from z/VM** to acquire the list of network devices from z/VM. The result will be similar to Figure 11-53.

![Figure 11-53 Populated z/VM networking properties](image)

4. Entries are made for each network device that z/VM Center can find on the z/VM system. Select the **VSWITCH** tab.

![Figure 11-54 Vswitch tab in z/VM Networking Properties](image)
5. Double-click the VSWITCH1 entry in the list to open the properties window for VSWITCH1. Figure 11-55 appears.

![Connection Properties](image)

**Figure 11-55  VSWITCH1 properties**

6. In the properties window, define the base address to be used when allocating systems on VSWITCH1. This is the first address that will be used. Then define the IP address range. This is how many addresses are available in sequence. For example, to define the IP address pool 9.12.4.156 - 9.12.4.161, we defined a base address of 9.12.4.156 and a range of 6.

**Note:** It is not possible to define multiple ranges to a network device. One workaround for this issue is to define a range large enough to cover all the ranges, and then mark the forbidden IPs as in use by creating occupied IP entries.

7. Fill in values for the MTU, netmask, and default gateway, and click **OK**.

8. From the Networking Properties window, click **Action → Scan for Occupied IP Addresses** to search the director console for IP addresses that are
currently in use. This does not actually scan the network. Rather, it searches the IBM Director server for managed systems that are in the IP ranges defined to the z/VM devices.

![Connection Properties](image)

**Figure 11-56  VSWITCH1 properties with occupied IP addresses**

In our example, scanning for occupied IPs found the two master Linux images that were discovered by the director server. These two IPs are marked as in use on VSWITCH1, even if they are not actually using VSWITCH1 for network connectivity.

z/VM Center now has a pool of four IP addresses available on VSWITCH1 for use by systems in server complexes.
Defining a server complex
In this section we describe how to define a server complex named nucleus and set VSWITCH1 as the network connection for all its systems.

1. From the server complexes task, click **Action → New Server Complex**.

![Create a Server Complex](image)

*Figure 11-57  Name the server complex*

2. In the window that opens, name the server complex and choose how many tiers it will contain. Name the tiers by overwriting the default tier names. Click **OK**.

   A progress window opens that will display a green check mark once the server complex has been created.

3. Click **Close**.

![Server complex creation](image)

*Figure 11-58  Creation complete message*
The new server complex is now available (Figure 11-59), but before systems can be added to it, it must have network properties defined. Network properties are the only properties that must be set for a server complex to be usable.

1. Click the title bar of the server complex where the name nucleus is, and the server complex will be highlighted.

Figure 11-59  The new server complex
2. With the server complex selected, click **Action → Edit Properties**. The properties for nucleus will be displayed (Figure 11-60).

![Figure 11-60 Properties overview](image1)

3. Click the **VMRM** tab.

![Figure 11-61 VMRM properties](image2)
There are three goal values in the VMRM tab:

- **CPU**
  Define the CPU allocation of this workload to VMRM. The number here is the percent of time that the workload runs when it is ready to run, from 1 to 100.

- **DASD**
  Define the DASD I/O priority of this workload to VMRM. DASD I/O priority changes must be allowed by the hardware for this setting to be effective. This setting is made on the HMC in the activation profile for the processor.

- **Importance**
  Set the importance of this workload relative to other defined workloads in VMRM. This is an integer from 1 to 10. 10 is important, 1 is unimportant. VMRM will take the values entered here and define a workload that contains all of the systems in this server complex. This may lead to strange behavior, as noted on page 653.
4. Click the **Scripts** tab.

![Scripts properties](image)

The scripts property allows scripts to be run on the guest when it enters a server complex, exits a server complex, or both. The script may be assumed to reside on the guest being moved or on the director server. If the script resides on the director server, it will be copied to the moving guest by IBM Director before being executed.
5. Click the **Network** tab.

![Network properties](image)

**Figure 11-63  Network properties**

It is possible to define up to four network interfaces and a default gateway in the Network tab.
6. Click the **Minidisks** tab.

![Minidisks properties](image)

**Figure 11-64  Minidisks properties**

Minidisks that are defined here are linked and mounted to all systems in the server complex. This is valuable to share common data read only among several systems.

7. Go back to the Network tab.
8. Choose VSWITCH1 for interface #1, and select the default gateway.

9. Click **OK** to apply the properties to the server complex.
The properties have been applied successfully when the green check mark appears in the progress box (Figure 11-66).

Figure 11-66  properties saved

10. Click Close.
Provisioning systems into the server complex
Once the server complex is defined and its network properties set, it is a simple matter to provision multiple systems into the server complex. This section describes how to provision four systems into the server complex:

1. Open the server complexes task.

2. Click **Refresh** to get the most current set of virtual server templates, operating system templates, and disk pools from virtual server deployment.
3. Select the appropriate virtual server template and disk pool, then drag the operating system template on to the server complex that you wish to create new systems in.

4. Enter the number of clones you wish to create. Enter 4 and click **OK**.

![Number of clones](image1.png)

*Figure 11-68  Number of clones*

![Cloning new guests](image2.png)

*Figure 11-69  Cloning new systems*

5. The server complexes task then executes the following tasks. Progress is shown in Figure 11-70 on page 669.

   a. Creates a new virtual server using the chosen template
   b. Provisions an operating system into the virtual server using the chosen template
c. Applies the network settings for the server complex

d. IPLs the Linux Virtual Server

Figure 11-70  Finished cloning new systems

6. Once server complexes has cloned all the Linux systems, click Close to exit
the status window.
7. The server complex is then shown with the four new systems in it, as shown in Figure 11-71.

![Figure 11-71   New systems in nucleus](image)

The new systems appear in the nucleus server complex. They are currently in status unknown, and marked by a question mark (?) since they have not been accessed by the director server.
8. Go to the main window of IBM Director Console. Optionally, set the association to be z/VM server complexes Membership, as shown in Figure 11-72.

![IBM Director Console](image)

*Figure 11-72   The new systems are initially locked*

The systems are discovered automatically as part of the server complexes cloning process if their IP address range is listed in the director server discovery preferences. However, the four new systems appear as locked objects, as indicated by the padlock icon.

9. Select and request access to the four new systems.

It is possible to request access to all four at once by selecting the first one, then shift selecting the last one. Requesting access to multiple systems at the same time works fine as long as the same credentials can be used for each system. Since these systems are all clones, this will work.
10. Once all of the new systems are unlocked, they will be inventoried. If the console is set to use the z/VM Server Complexes Membership association then the new systems will move into the free systems list for the z/VM system that they are running on, then move to the tier of the server complex they actually reside in.
11. Back in the Server Complexes window, the new systems are showing normal status in the nucleus server complex (Figure 11-74).

![z/VM Server Complexes: VM/LINUX4](image)

**Figure 11-74** unlocked new systems in nucleus

**Putting it all together**

The z/VM Center extension allows a system programmer to more efficiently provision new Linux systems and configure some of their properties at the server complex level.

The Virtual Server Deployment task provides these capabilities:

- Authenticate the z/VM MAP to the z/VM System Management API.
- Define virtual server templates.
- Register the operating system characteristics of a running Linux system.
- Create a new virtual server from a virtual server template.
- Capture an operating system template from a Linux guest with a registered operating system.
- Provision an operating system template to an empty virtual server.
The server complexes task provides these capabilities:

- Define the properties of the network resources that are available to z/VM.
- Create containers called server complexes that have the following properties:
  - VMRM allows the z/VM system to adjust resource allocations between server complexes as needed.
  - Scripts allow arbitrary actions to be run on Linux systems as they enter or leave server complexes.
  - Networks allow up to four network interfaces to be defined and connected to any network resources available within z/VM.
  - Minidisks allow Linux systems within a server complex to share access to read-only data.
- Move systems from the Free Linux guests list to a server complex and apply all the server complex properties to that system.
- Move Linux systems out of a server complex to the Free Linux Guests list.
- Provision new Linux systems with a single drag-and-drop action into a server complex.
Event management

Effective systems management requires more than just monitoring capabilities. You need to have some form of action take place when a monitored event occurs.

Event management is another differentiating element of IBM Director. This chapter discusses how you can create and maintain event action plans (EAPs).

This chapter covers the following topics:

- 12.1, “Introduction” on page 676
- 12.4, “Event filters” on page 687
- 12.5, “Event actions” on page 729
- 12.6, “Example: creating an event action plan” on page 740
- 12.7, “Event flow” on page 744
- 12.8, “Recommended EAPs” on page 747
- 12.9, “Exporting and importing EAPs” on page 758

We recommend that you also read Chapter 4 of the product publication IBM Director Systems Management Guide.
12.1 Introduction

The most powerful feature of IBM Director is probably its extensive ability to respond to events. There are 23 customizable actions, ranging from e-mail, paging, starting applications, to even posting to a newsgroup.

All event management is done through EAPs, which associate the actions that occur as a result of a specified event. EAPs can be applied to individual objects or groups, easing administration in large environments.

EAPs are comprised of two components:

- Event filters, which specify explicit criteria that the plan react on
- Actions, the tasks that are executed as a result of the event

There are six steps to successfully create, build, and maintain EAPs:

1. Plan for EAP implementation. Consider what event you want to monitor for, and what action should occur as a result of that alert.

2. Create any trigger points if necessary, such as resource monitors, process monitors, and so forth. This step is only required if you want to trigger your EAP on an event that does not normally occur. For example, a CPU utilization threshold or process termination.

3. Create any actions if necessary, such as process tasks, batch files, and so forth. This step is only required if you want to take an action that does not exist in the standard installation (for example, a Process Task that terminates a process or a batch file that executes a series of commands).

4. Create and name an empty EAP to contain the desired event filters and actions. The purpose of an EAP is to bind an event generated by one or more managed systems to one or more desired actions.

5. Create an event filter. Event filters can be configured to use an approach where the criteria is very broad (for example, any IBM Director Agent event), or a very specific approach (for example, an IBM Director Console login failure due to a bad password). An EAP can have one or more event filters associated with it.

6. Select and customize the actions. Most actions require some configuration in order to be used. For example, you must provide several pieces of information about the recipient and e-mail server in order to use the Send an Internet (SMTP) E-mail action. An event filter can have one or more actions associated with it.

7. Apply (associate) the completed EAP to a group or managed system.
Before beginning, it is useful to understand how the typical event message flows through IBM Director. A basic understanding of the process can help you build and troubleshoot an action plan efficiently.

When IBM Director receives an event message from a system, it performs the following steps to determine which actions must be taken:

1. The system generates an event and forwards the event to all IBM Director Servers that have discovered the system (except for some events, such as Resource Monitor thresholds, which are sent only to the management server where they were configured).
2. IBM Director Server examines the event and determines which system generated the event and to which groups the system belongs.
3. IBM Director Server checks to see if EAPs are associated with the system or its groups.
4. The associated EAPs are checked to determine whether any event filters match the event that was received.
5. The server carries out each associated action for each matching filter.

Definitions of terms:

- **Event**: A flag that identifies a change in a process or device, such that notification of that change can be generated and tracked. Examples include a server going offline, or CPU utilization exceeding a predefined percentage.
- **Event filter**: A set of characteristics or criteria that determine whether an incoming event should be acted upon.
- **Action**: A step that is taken in response to an event.
- **Event action plan**: An association of one or more event filters with one or more actions. EAPs become active when you apply them to a system or a group of systems.

In addition, if you have a service processor installed in your System x server and have installed the ASM device driver and IBM Director Agent, then IBM Director also receives all local service processor events.

## 12.2 The Event Action Plan Wizard

The IBM Director Event Action Plan wizard is used to create an initial set of EAPs, typically to provide event alerting. Some of the capabilities include:

- Choice of systems or groups to which it will apply
- Additional filters, including system offline, CPU, and memory utilization
- Time ranges in which the EAP will be applicable
- Actions including e-mail, paging, and starting a program on the event system, another system, or the IBM Director server

The EAP Wizard can be launched in any of four ways:

- If an Express installation of IBM Director Server is executed, the EAP Wizard is automatically launched during the first management console login process. Note that this version of the EAP Wizard is slightly different than the standard EAP Wizard. See 4.1, “Express installation” on page 150, for more about this.
- As shown in Figure 12-1, click the arrow to the right of the icon on the IBM Director console tool bar and click Event Action Plan Wizard.

![EAP Builder menu](image)

*Figure 12-1  EAP Builder menu*

- From the EAP Builder window, click the button.
- Right-click the Event Action Plans task in the Tasks column of the main console window and click Event Action Plan Wizard.

**Tip:** The IBM Director EAP Wizard is limited in which filters and actions you can use. For extensive filtering and alerting actions, use the Event Action Plan Builder.
The Event Action Plan Wizard dialog boxes are as follows:

1. When you start the wizard, you are first prompted to enter a name for the new EAP, as shown in Figure 12-2.

![Event Action Plan Wizard](image)

*Figure 12-2  EAP Wizard - Name*
2. Specify the systems or groups to which you want the EAP to apply. To select a group, select **All Groups** from the pull-down menu above the left-hand list. See Figure 12-3.

*Figure 12-3  EAP Wizard - Systems*
3. Specify the event filters that you want to use to restrict which events trigger the event actions. The text below the list box describes the selected filter and lets you specify additional parameters (such as a utilization percentage when you select CPU Utilization, as shown in Figure 12-4).

**Note:** Some event filters, such as CPU Utilization, can only be applied to individual systems, not groups.

*Figure 12-4  EAP Wizard - Event Filters*
4. Specify the actions that you want to perform if the filtered events occur on the specified systems or groups. See Figure 12-5.

![Event Action Plan Wizard](image)

**Figure 12-5  EAP Wizard - Actions**

You can select from three actions:

- Send an e-mail. Only one e-mail address can be specified.
- Send a page.
- Run a program on the system that generated the event, the management server, or any other managed system.

You can test your actions by clicking the **Test Action** button. This generates an event of severity Harmless and of type Director.Test.Action.
5. In the Time Range window (Figure 12-6), you can specify a range of times when you want the events to result in an action. The default is to not restrict the actions to a range of times.

Figure 12-6  EAP Wizard - Time Range
6. When completed, you are given an opportunity to review the configuration and make any changes desired. Figure 12-7 shows the review pane of a completed EAP.

![Event Action Plan Wizard](image)

**Figure 12-7  EAP Wizard - Summary**

7. Click **Finish** to exit the wizard.

If you later want to change the EAP that you created with the EAP Wizard, expand the **Event Action Plans** entry in the Tasks pane of the IBM Director Console, right-click the EAP, and click **Edit plan with wizard**.

**Note:** Only existing EAPs created with the wizard can be edited with the wizard.

12.3 **The Event Action Plan Builder**

The Event Action Plan Builder allows you to truly exploit the power and flexibility of IBM Director’s event handling capabilities. It enables you configure what you want to be alerted about and how to send the alert.
It is crucial that you understand the concepts of the Event Action Plan Builder before you start to configure your alerts. To start the Event Action Plan Builder, click the gear icon ( ). A new window with three panes opens, as seen in Figure 12-8.

**Figure 12-8  Event Action Plan Builder**

### 12.3.1 Event action plans

The left pane lists all of the configured EAPs. The initial install creates a default EAP of Log All Events, which is applied to the All Managed Objects group. As you create additional EAPs, they populate this left pane, as well as the EAPs item in the task pane on the IBM Director console.

Think of an EAP as a container for event filters and actions. You can choose to have one EAP for each event or, more likely, to create an EAP that contains several events within one category. An example is to create one EAP for critical hardware events and one EAP for software events. For easy recognition, you
should name your EAPs to reflect what they do and what types of systems they are designed for (for example, Resource monitors - mail servers).

After you have created your EAP, you must apply it to the selected managed systems or groups by dragging it onto a managed system or group in IBM Director Console.

In order to see which EAPs are associated with which managed systems or groups, click Associations → Event Action Plans in the IBM Director console.

To see all systems that have event action plans assigned to them, click the group All Systems and Devices (or any other group if you want to check only a subset of systems). The systems that have event action plans assigned can be expanded to show them, as in Figure 12-9.

![IBM Director Console](image)

*Figure 12-9  Showing event action plans assigned to systems*
To see the groups that have event action plans assigned, click the Groups category **All Groups**, as in the left pane of Figure 12-10.

![Figure 12-10  Showing event action plans assigned to groups](image)

To remove an EAP that has been applied to a system or group, right-click the EAP and click **Delete**. This removes the EAP from the system or group but does not delete the EAP outright.

## 12.4 Event filters

The middle pane of the Event Action Plan Builder (Figure 12-8 on page 685) contains the filters. When events are received by the management server, it is the filters that determine whether the actions specified in the EAP are to be executed.

In this section we discuss the types of filters and their uses:

- 12.4.1, “Event filter types” on page 688
- 12.4.2, “Event Type tab” on page 696
- 12.4.3, “Severity tab” on page 720
- 12.4.4, “Day/Time tab” on page 721
- 12.4.5, “Category tab” on page 723
- 12.4.6, “Sender Name tab” on page 723
- 12.4.7, “Event Text tab” on page 725
12.4.1 Event filter types

There are four different filter types:

- Simple event filter
- Exclusion event filter
- Threshold event filter
- Duplication event filter

Initially there are filters only in the simple filters. The other categories require you to configure filters. This section describes each of the filter types and provides examples of filter configuration.

Common attributes for all filter types

All four event filter types have common attributes. Right-click any of the event filter types and click New. You can see the Event Filter Builder window (Figure 12-11).

![Simple Event Filter Builder window](Figure 12-11)
All of the event filter builders have the following tabs:

- Event type
- Severity
- Day/Time
- Category
- Sender Name
- Event Text
- Extended Attributes
- System Variables

The Duplication and Threshold filters also have a Frequency tab, and the Exclusion filter has an Excluded Event Text tab.

**Simple event filter**

The simple event filter is the general-purpose filter type. Most of your filters will be this type. As Figure 12-8 on page 685 shows, there are many predefined filters in this group. These predefined filters are useful for creating generic EAPs.

Several of these filters use the severity of the event as criteria to allow events to pass through. The Critical Events filter is concerned only with events of \textit{critical} severity, the Fatal Events filter is concerned only with events of \textit{fatal} severity, and so on. The All Events filter passes through any events that occur on any managed system.

Carefully consider the use of the supplied Simple Event Filters. Many of these are quite broad regarding what events will be caught, leading to potentially numerous alerts being generated. For example, there could be a critical CPU utilization event and a critical storage event. If both of those systems have an EAP that filters for critical events, then the defined action would occur for both.

**Note:** The severity of each IBM Director event is provided in the \textit{IBM Director Events Reference} publication.

IBM Director provides you with the ability to create new filters, using more specific criteria, so that the filter will catch only specific events. The filter criteria check boxes are in a hierarchical format, meaning that the further into the tree the box is checked, the more granular the filter is. If two boxes in the same branch are checked, the higher level will be the effective filter.
Figure 12-12 illustrates this concept. A check in the Director box will catch all IBM Director events, including console, agent, inventory, topology, and so forth. Drilling down, you can set the criteria to be more specific, such as only Director Agent events; only monitored process event; only monitored processes starting; and finally only if Solitaire (sol.exe) starts. This allows you to create EAPs that will only respond to very specific events, and respond in different ways to different events, even if they have the same severity and category characteristics.

![Hierarchical filtering in IBM Director](image)

**Exclusion event filter**

This filter can be used to activate a whole subgroup of events, then exclude some subevents. An example of this is if you plan to monitor the Windows Security event log events, but you want to exclude security alerts 528, 551, and 552.
The two-step process to create the exclusion filter is:

1. In the Event Type tab, select the **Windows Event Log** entry. Selecting the parent entry also includes all child entries. See Figure 12-13.

2. Click the **Extended Attributes** tab and select the child entries that you want to exclude.
**Tip:** Your IBM Director Server might not have the event log entries selected in Figure 12-14. This is because the filter list is dynamically populated with entries such as these, so they only appear after one is added to the event log.

Use an exclusion event filter when you want to create an event based on severity or category for an entire filter subgroup (instead of picking one event and one event filter and creating custom actions for each one). You can do this with the other event filter types as well, but by using exclusion event filters it is easier to remove events that you do not want to monitor or that you want to create a custom action for without rearranging your whole EAP.

**Threshold event filter**

The threshold event filter can be used in scenarios when an event must meet the filter criteria several times within a time limit.
An event meeting the criteria defined in this filter triggers associated actions only after an event meets the criteria for the number of times specified in the Count field or only after the number of times specified in the Count field within the time range specified in the Interval field.

For example, if you want to be alerted if a user logs on with a bad password five times within five minutes, you would create this threshold filter:

1. In the Event Type tab, select the event type that you want to monitor. In Figure 12-15, we select 529.

![Figure 12-15 Step 1: Threshold event filter: create the event type](image_url)
2. In the Frequency tab, enter the minimum number of times this event must occur and the length of time within which this count must occur.

   In Figure 12-16, we enter 5 minutes and 5 occurrences.

![Threshold Event Filter Builder: New](image)

   Figure 12-16  Step 2: Configure the frequency

3. Click **File Save** (or the icon) to save the filter. For this example, we named it **Windows - Bad Passwd - 5/5**, and now this filter is listed under Threshold Event Filter.

**Duplication event filter**

A duplication event filter allows for duplicate events to be ignored. To use this filter, you must specify the number of times (count) the same event is ignored during a specified time range (interval). The two values are specified in the Frequency tab.

To trigger the associated actions a second time, one of these situations must occur:

- The event must occur more than the number specified in the Count field (not counting the first occurrence)
- The time range specified in the Interval field must elapse.
- The value specified in the Count field must be exceeded by 1 within the time range specified in the Interval field.
When the initial event is received, the actions defined in the EAP are performed. If the event occurs again (one or more times), and it is less than the count or interval specifications, it is ignored until the count or interval values are exceeded.

If the Count field or the Interval field are blank or 0, they are ignored. After actions are performed the second time, the counters for both count and interval are reset.

This is very useful if you want to trigger an action on an event, but the action you trigger (for example, a batch script or a fix) takes two minutes to execute. You do not want to start the batch file or fix several times on the same system even if the event occurs several times. If the event triggers in the example shown below, an action will execute. But if the event occurs (up to ten times) again within 5 minutes, the action will not execute, as displayed in Figure 12-17.

*Figure 12-17  Frequency settings for a Duplication event filter*
12.4.2 Event Type tab

The Event Type tab is the most important tab because it is here that you select the events upon which you want the event action plan to be activated. It is used to specify the sources of the events that are to be processed by this filter. See Figure 12-18.

**Tip:** The Event Type list is created dynamically and entries are added as new alerts are received.

![Simple Event Filter Builder: New
File Help

<table>
<thead>
<tr>
<th>Gender Name</th>
<th>Event Text</th>
<th>Extended Attributes</th>
<th>System Variables</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Type</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>By default,</td>
<td>Capacity Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the event</td>
<td>CIM</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter</td>
<td>Configuration Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>excludes</td>
<td>Director</td>
<td></td>
<td></td>
</tr>
<tr>
<td>none of the</td>
<td>MassConfig</td>
<td></td>
<td></td>
</tr>
<tr>
<td>event types,</td>
<td>MPA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>except for</td>
<td>PET</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows-specific</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>is/OS-specific events</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>To exclude</td>
<td>SNMP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>specific</td>
<td>Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>event types,</td>
<td>Windows Event Log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>clear the</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>None check</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>box</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 12-18  Event Type tab*

We address each of these filter categories in the following sections:

- “Capacity Manager filters” on page 700
- “CIM filters” on page 700
- “Configuration Manager filters” on page 702
- “Director filters” on page 703
- “Electronic Service Agent filters” on page 708
- “MassConfig filters” on page 708
- “MPA filters” on page 709
- “PET filters” on page 709
By default the Any check box is marked, meaning that most events will be monitored on the managed systems. (See the shaded box on this page for specifics.) If you want to change this to make your own specific event filter, clear the Any box. This gives you access to all of the options. To select an event, highlight the option you require. You can highlight more than one event by holding down the Ctrl or Shift keys.

Important: Checking Any in Event Types does not mean that all event types are selected. This includes some CIM event types and all Windows Event Log event types. These event types can generate significant network traffic in large IBM Director installations. Therefore, if you want to create an Event Filter with all CIM event types or any Windows Event Log event types, you must make sure to select the appropriate event types.

If you really want all event types selected, deselect Any and manually click all entries with the Ctrl key pressed (or click the first entry, then with Shift click the last entry).

Though you can right-click a child event type and click Delete to delete the event type, do not do this because the event type will be deleted immediately from all filters regardless of whether you save this filter. Since the list of event types is dynamic, the deleted event type may be restored automatically when another event of the same type is received by IBM Director Server.

The Filter Type tab lets you specify filters from specific hardware and software components, as described in the following subheadings.
Implementing IBM Director 5.20

Tip: To aid in determining which events you want to include or exclude in a filter, you can view the event log of a managed object, and then in the Event Type column is the filter tree in a dotted notation, which corresponds to the event tree. See Figure 12-19 on page 698 for an example.

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Event Type</th>
<th>Event Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/2/2005</td>
<td>3:57:22 PM</td>
<td>Director.Topology.Online</td>
<td>System 'kidd' is online</td>
</tr>
</tbody>
</table>

The event log entry displays a dotted representation of the corresponding Event Type. For example **Director.Topology.Offline** corresponds to **Director > Topology > Offline** in the tree view.

*Figure 12-19  Event type from the log*

As mentioned earlier in this section, some entries in the tree are dynamically populated. When you install your IBM Director Server, most of the filter types entries will be populated with events, except for Windows Event Log and SNMP. The list of events is built dynamically by enabling logging for all Windows event log and SNMP events.
We use the Windows Event log in this example (Figure 12-20).

The security subgroup contains seven definitions of events, which are collected from the discovery process when IBM Director discovers an agent with the Windows Security event log present. There are still no actual events in the event filter subgroup.

If you include the security events in an EAP, when a security event is triggered (such as logging on with auditing enabled), new events are added to the list, as shown in Figure 12-21.
To save these definitions of events, make a backup copy of Data\TWGType.ini. This file can be copied to a new IBM Director server, where you can keep all definitions for Windows event log events and SNMP events.

![Diagram of Alert Standard Format filters](image1)

**Figure 12-22  The Alert Standard Format filters**

### Capacity Manager filters

Capacity Manager can generate an event when a managed system has a bottleneck. This event is triggered by the Capacity Manager task, a fee-based extension. You can use this filter to schedule an automatic weekly Capacity Manager report and forward an event if one of the systems has a bottleneck.

This filter category (Figure 12-23) is only present if Capacity Manager is installed. Capacity Manager is described in 6.7.1, “Capacity Manager” on page 399.

![Diagram of Capacity Manager bottleneck filter](image2)

**Figure 12-23  The Capacity Manager bottleneck filter**

### CIM filters

The CIM events category works for both IBM and OEM hardware running Windows operating systems. We recommend that you use this filter for mobile
computers, desktops, and System x servers that do not have a service processor. There are seven categories of CIM filter types, as shown in Figure 12-24.

As you can see in Figure 12-24, the bottom three event filter types are related to Windows. If you want to filter on Windows event log entries, we recommend that you use the Windows event log filter described in “Windows event log events” on page 717, and not the one in the CIM filter subgroup. If you want to filter on Windows services, we recommend that you configure a service threshold under the Process Management task or use the Resource Monitors task to establish monitors for specific services. Likewise, we recommend using the Resource Monitors task to configure Windows Registry monitors, due to the granularity that can be achieved.

Note that the CIM events create generic events for all systems, and the event text sometimes can be very long. Therefore, we do not recommend that you send an SMS alert with the body of the event (&text) to a mobile phone, to avoid dividing an important SMS message.

Each time a system is started, the CIM events generate several events to report that hardware components are operating normally. Therefore, it is important to use the Severity tab (see page 720) and Category tab (see page 723) to prevent these messages from being sent as alerts when they really are information events. These events will be sent as a resolution event, and we recommend that you use the Add to Event Log action for those.
To receive an alert when a system has a problem, check the **Alert** box (Figure 12-25).

![Simple Event Filter Builder: New](image)

**Figure 12-25** Event action plan Category tab

After you have created the filters, select your desired actions and apply the plan (Figure 12-26) to the All Director Systems group.

![Event Action Plans](image)

**Figure 12-26** Event action plan for client systems

**Configuration Manager filters**

The Configuration Manager filter catches events generated when either a BladeCenter or a Server Configuration Manager manager task has been applied (Figure 12-27).

![Configuration Manager filter](image)

**Figure 12-27** Configuration Manager filter
Director filters
The Director filters tree (seen in Figure 12-28) picks up events that are generated inside IBM Director components, including IBM Director Server, Console, and Agent.

These filters also help to alert you in the event of issues or changes in the IBM Director database and inventory, as well as when managed systems come online and go offline. There is also an event filter used for testing event action plans. Finally, a new group of event filters has been added for Update Manager.

Director.Console events (seen in Figure 12-29) are related to logon, such as users logging on to the management server with bad passwords. We recommend that you monitor these events closely because a successful logon to the management server can grant powerful access to the whole infrastructure.
Director.Director Agent events (seen in Figure 12-30) are generated as output from monitors you can activate on managed systems. The Director.Director Agent subgroup is empty by default. You must activate one or more of the following monitors before you can filter for these events:

- Process monitor and monitor an application
- Process monitor and monitor a service
- Process monitor and monitor a device
- Resource monitor

After you have configured one of these monitors on at least one managed system, you can create filters based on the events the monitor sends. For example, if you monitor your Lotus Domino service and the service stops, an event is generated. Using this event as a trigger, you can configure your EAP to
automatically restart the service by using a `net send` command or start an executable file.

Another example is to use the resource monitor to monitor how many inactive sessions you have on a terminal server. If the number of inactive sessions you have configured as maximum is reached, the EAP can send an e-mail to the help desk and inform them that this requires attention.

Director.Inventory filters (seen in Figure 12-31) can be used to alert you in the event that IBM Director inventory data has changed or that inventory collection has succeeded or failed.

![Figure 12-31  IBM Director Inventory event filters](image)
Director.Topology (seen in Figure 12-32) is another important event filter. It monitors when managed systems come online and go offline. Keep in mind that a Director.Topology.Offline event does not necessarily mean that the managed system has been shut down or that it has lost connectivity to the network. Although these situations will certainly trigger this event, there is another explanation. This event is triggered by IBM Director Agent itself. If you stop IBM Director Agent on a managed system, the Director.Topology filter will treat this as though the managed system has gone offline.

![Diagram of IBM Director Test and Topology event filters]

*Figure 12-32  IBM Director Test and Topology event filters*
Director.Update Manager is a new filter (seen in Figure 12-33) introduced in IBM Director 5.20 that monitors various Update Manager events. Update Manager events occur after any of the following conditions:

- An update is downloaded successfully.
- An update fails to download.
- A profile setting changes.
- A profile is deleted.

![Figure 12-33 IBM Director Update Manager event filters](image-url)
Electronic Service Agent filters
Electronic Service is a new filter that is added when Electronic Service Agent (ESA) extension for IBM Director is installed. You can use ESA filters to e-mail you if any service requests are generated or scheduled inventory fails. See Figure 12-34.

MassConfig filters
The MassConfig filters (Figure 12-35) allows you to specifically monitor for changes to mass configuration items such as asset ID, SNMP, or network settings.

Figure 12-34  Event filters pane expanded to see Electronic Service filters

Figure 12-35  Event filters pane expanded to see MassConfig filters
MPA filters
These events (Figure 12-36) are generated by the service processor in a managed system. They will only work for servers that either have an onboard service processor, RSA, or a management module. MPA events provide more hardware events than CIM filters and are more detailed. We recommend that you use MPA events instead of CIM filters for System x servers that have a service processor.

![Figure 12-36  Event filters pane expanded to see MPA filters](image)

Use the Severity tab to differentiate fatal and critical events from warning and information events. MPA events can differ slightly from server to server, but if you create a filter that enables the whole subgroup and use severities to separate the events, you can be sure that you will not miss any events.

PET filters
Platform Event Trap (PET) events are generated by ASF-capable NICs and BMCs. Events can include environmentals (temperature, power, and so on) and hardware alerts.
Figure 12-37 shows the event log from a BMC on a system that incurred a fan failure. Notice that there is a PET event type, which is similar to SNMP dotted decimal, and not very readable.

IBM Director translates the native PET event to an MPA event, which can then be used for filtering and alerting purposes, with meaningful information. This is why there are multiple event log entries for a single PET event.

**SNMP events**

IBM Director has the ability to receive events from SNMP devices in your infrastructure. This is a very powerful feature for monitoring SNMP-capable devices such as printers, routers, switches, and SNMP-capable applications.
Chapter 12. Event management

There are some predefined events (Figure 12-38), but most SNMP devices have their own event definitions, stored in MIB files. To convert native SNMP dotted decimal notation into meaningful text you must compile the proper MIB files. For more information about compiling MIB files and the SNMP Browser task, see 6.3.18, “SNMP Browser” on page 346.

**Storage filters**

For IBM ServeRAID events, use the Storage.ServeRAID Controller subgroup (Figure 12-39). ServeRAID adapters generate very detailed events if a problem occurs, which can result in a very complex filter list. However, it is easy to pick out the right events because ServeRAID events are categorized with different severities.
If you are not familiar with ServeRAID adapters, we recommend selecting events based on their severity. In the case of a hard drive failure in a RAID-5 array with a hot spare, the following events happen:

1. An event is generated by the ServeRAID adapter, acknowledging that the logical drive is in a critical state. This is a critical event, but it is not fatal because the array is still functional and users can still access their data.
   
   Event=Storage.ServeRAID Controller.Logical Drive.State.Critical

2. An event is generated to inform that a physical drive has failed. If the drive was not part of an array or logical drive, this is the only event generated. This is categorized as a fatal event.
   
   Event=Storage.ServeRAID Controller.Physical Drive.State.Failed

3. An event is generated to inform that the rebuild process has started. This happens automatically if you have a hot spare drive in the system, or it happens when you replace the defunct drive. This is a harmless event.
   
   Event=Storage.ServeRAID Controller.Logical Drive.Rebuild.Started

4. An event is generated when the rebuild is complete. This is a harmless event.
   

If you have configured your EAP to send an SMS alert for fatal events and an e-mail for critical events, the hard drive failure event will be sent as an SMS alert and the Logical Drive critical event will be sent as an e-mail alert. This is by far the easiest way to configure ServeRAID event filters.

**Virtualization Manager filters (VSM type)**

IBM Virtualization Manager is capable of generating a number of events that can be logged or acted upon by event action plans. The events that are provided by Virtualization Manager are for Virtualization Manager objects. These events are grouped under the **VSM** event type in the Event Filter Builder. For more about Virtualization Manager see Chapter 10, “IBM Virtualization Manager” on page 513.
Figure 12-40 shows the Simple Event Filter Builder window with the Virtualization Manager event headings exposed. Details of these headings are described in this section.

Figure 12-40  Simple Event Filter Builder showing Virtualization Manager event types

Figure 12-41 shows a partial view of the event filter tree for Virtualization Manager. Details of the event filters shown are as follows:

► Agent Extension filters

– Status Changed - Virtualization Manager Agent detects a status change for the platform manager or the host. The following scenarios are examples of such events:

• Virtualization Manager Agent is not running or the virtualization application is not installed.

• Virtualization Manager Agent and the virtualization application are installed, but they are not communicating properly with each other.

• The platform manager or host is ready for use. For platform managers, this means that IBM Director has authenticated with VMware.
VirtualCenter server. For hosts, this means that Microsoft Virtual Server services are started.

► Host filters

– Started - Virtualization Manager Agent detects that Microsoft Virtual Server services have started on a host.

– Stopped - Virtualization Manager Agent detects that Microsoft Virtual Server services have stopped on a host.

► Virtual Farm filters

– Created - Virtualization Manager Agent for VirtualCenter detects that a virtual farm has been created. IBM Director Console displays the virtual farm object.

– Deleted - Virtualization Manager Agent for VirtualCenter detects that a virtual farm has been deleted. IBM Director Console no longer displays the virtual farm object.

– Host Added - Virtualization Manager Agent detects that a host has been added to a virtual farm. IBM Director Console displays a host object under a virtual farm object. For VMware VirtualCenter, when this event occurs, a host object is displayed only when the managed system that represents the host has already been discovered by IBM Director Server.

– Host Removed - Virtualization Manager Agent detects that a host has been removed from a virtual farm. IBM Director Console no longer displays the host object under its virtual farm object.

– Renamed - Virtualization Manager Agent for VirtualCenter detects that a virtual farm has been renamed. IBM Director Console displays the new name for the virtual farm object.
Figure 12-42 shows the portion of the event filter tree for Virtualization Manager associated with virtual servers. Events in this part of the tree originate from managed virtual servers. Details of the event filters shown are as follows:

- **Attribute Changed** - The value of the CPU Count or the Memory Size attribute for a virtual server object has changed. Virtualization Manager updates this attribute information in both IBM Director and the associated virtualization application.

- **Created** - A virtual server object has been created. IBM Director Console displays a virtual server object for a virtual server.
  - **Deleted** - A virtual server object has been deleted. IBM Director Console no longer displays a virtual server object for a virtual server.

- **Migration filters**
  - **Completed** - A virtual server has completed migration from one host to another.
  - **Started** - A virtual server has started migration from one host to another.

*Figure 12-42  Another set of Virtualization Manager event types*
- State filters
  - Pending - The state of a virtual server has changed to pending. The associated virtualization application requires the user to answer a question before the state change will continue. To resolve a pending state, use the Start Vendor Software task to start the management interface for the virtual server, then resolve any open questions.
  - Powered Off - The state of a virtual server has changed to turned off.
  - Powered On - The state of a virtual server has changed to turned on.
  - Reset - The state of a virtual server has changed to restarted.
  - Resumed - The state of a virtual server has changed from suspended to Turned On.
  - Suspended - The state of a virtual server has changed to suspended.
- Task Failed - An operation on a virtual server has failed to be completed successfully. A power or migration operation failed for a virtual server.
Figure 12-43 shows an IBM Director Event Log window that displays several Virtualization Manager events that have occurred on our environment that are related to virtual server migration. The IBM Director Event Log provides a historical record of notable events that have taken place in the virtualization environment.

![IBM Director Event Log](image)

**Windows event log events**

Two filter subgroups (Figure 12-38 on page 711) provide software events. The first one is the CIM events category discussed in “CIM filters” on page 700. Under the second one, the Windows Event Log subgroup, you see the available event log categories that are present in your infrastructure.
Normally, you see the application log, security log, and system log. However, there can be more event logs, depending on whether you have any Active Directory controllers, Windows DNS servers, and so on. Which event logs show up here is based on inventory collection from the managed systems.

If you have not configured any EAPs with the Windows Event Log filter yet, notice that there are several event sources under the event logs, but there are no real events. The reason for this is that IBM Director has to receive an event once before it can show up here.

To start the event, create an exclusion event filter and select the whole Windows event log subgroup. We recommend that you use an exclusion event filter because you probably will want to exclude some events fairly soon. This is described in “Exclusion event filter” on page 690. Set the action to log the event, and apply it to all IBM Director systems.

![Windows event log filter](image-url)
Either generate a Windows event (enable security auditing and logon or logoff), or wait a few minutes until the management server has received events from some of the managed systems. Now you can see that there are events in the filter subgroup (Figure 12-45).

![Figure 12-45  Windows event log events with events](image)

You can either use a simple event filter and create custom events for each event log entry you want to monitor, or you can create a generic filter based on severity. If you want to create a generic filter, use Table 12-1 to map Windows event log severities to IBM Director severities.

<table>
<thead>
<tr>
<th>Windows event log severity</th>
<th>IBM Director severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informational (Blue)</td>
<td>Harmless</td>
</tr>
<tr>
<td>Warning (Yellow)</td>
<td>Harmless</td>
</tr>
<tr>
<td>Error (Red)</td>
<td>Critical</td>
</tr>
</tbody>
</table>
12.4.3 Severity tab

The Severity tab is used to indicate the urgency of the events that are received. If an event is received and the severity level is not included in the action plan, the filter will ignore the event. See Figure 12-46 for a view of the Severity tab options. By default, the Any check box is checked, indicating that all severities are processed by the filter.

![Figure 12-46 The Severity tab (Any is checked by default)](image)

**Tip:** The severity of events is assigned by IBM Director and might not match your definition of the actual severity of the situation. Do not rely solely on the severity of events without performing tests. For example, when a server reboots, IBM Director typically generates two events (offline, then online). Both of these events have a severity of harmless.

When you select more than one severity, they are added together using logical OR. The source of the event determines what severity the alert is. Generally, the severity levels mean the following:

- Fatal: The event caused a failure and should be resolved before the program or component is restarted.
- Critical: The event could cause a failure and should be resolved immediately.
- Minor: The event should not cause immediate program failure, but should be resolved.
Warning: The event is not necessarily problematic, but can warrant investigation.

Harmless: The event is for information only. No potential problems should occur.

Unknown: The application that generated the event did not assign a severity level.

12.4.4 Day/Time tab

The Day/Time tab enables you to set the filter to accept and ignore events on certain days and at certain times of the day. This creates the flexibility for IBM Director to react differently based on the day and time of day an event is generated. By default, the Any check box is checked, indicating that events occurring 24x7 are processed by the filter.

The time zone that applies to the day/time filtering entries is the time zone in which the management server is located. If your management console is not in the same time zone as the server, the difference in time zones is displayed above the selections pane as an aid in determining the correct times.
Figure 12-47 shows a filter that responds to events occurring between 8:00 a.m. and 5:00 p.m., Monday to Friday.

By default, all events are passed through all filters. This includes events that had to be queued at the agent because the link between the agent and the server was unavailable. You can prevent these queued events from being processed by a filter by clicking **Block queued events**.

This option can be useful if the timing of the event is important or if you want to avoid filtering on multiple queued events that are sent all at once when the IBM Director Server becomes accessible. However, you may only block queued events if you filter the event based on time. If you leave the day and time set to any, you cannot block queued events.
12.4.5 Category tab

The Category tab, shown in Figure 12-48, enables you to react based on the alerting or resolution of a problem.

For information about the category of each event, refer to the *IBM Director Events Reference* publication.

**Note:** Not all events have resolutions.

![Figure 12-48  The Category tab](image)

12.4.6 Sender Name tab

The Sender Name tab enables you to specify the system to which the filter will apply. Events generated by all other systems will be ignored. By default, the Any check box is selected, indicating that events from all agents (including the IBM Director Server) are processed by the filter.

The list of systems is added to dynamically. Initially, only the management server is listed in the drop-down menu. At the time of installation, the management server is the only system that has registered an event. As other systems generate events, such as thresholds being exceeded, this list should grow dynamically. If you anticipate that other systems will generate alerts, you can type agent names into the field and click **Add** to add them.
Figure 12-49 shows a filter configuration that only catches events from Jafa RSA and Skyler RSA.
12.4.7 Event Text tab

The Event Text tab (Figure 12-50) is used when you want to filter on specific words in the body of the received event. You can specify that you want to filter on any words, all words, or the exact phrase you enter. You can also specify whether case should be considered.

**Note:** There was a bug in IBM Director Server 5.10 and 5.10.1 where you were unable to enter anything in the text entry field. This bug was fixed in Version 5.10.2.

![Figure 12-50   Event Text tab](image)
In addition, this field is also used if you create a filter based on an event in the event log. Figure 12-51 shows a new event filter being created based on a topology.online event.

Figure 12-51   Creating an event filter from an existing event

The resulting Event Filter Builder window has an active Event Text tab with the text of the event listed. You can then select text matching options from the window, as shown in Figure 12-52.

Figure 12-52   Event Text tab
12.4.8 Extended Attributes tab

The Extended Attributes tab enables you to specify additional filter criteria. This tab is available (that is, not greyed out) only when you clear the Any check box in the Event Type tab and select certain entries from that tab.

**Tip:** The Extended Attributes tab is active when you select event types that support extended attributes. If you select one that does not have extended attributes (even if others selected do support them), the tab is greyed out.

If the Extended Attributes tab is enabled for a specific event type but no keywords are listed, the IBM Director Server is not aware of any keywords that can be used for filtering.

The filter in Figure 12-53 is configured to receive only Windows security events categorized as Logon/Logoff.

![Extended Attributes tab](image)

*Figure 12-53  The Extended Attributes tab*

12.4.9 System Variables tab

Use the System Variables tab to further qualify the filtering criteria by specifying a system variable. You can set a system variable using the event action Set an Event System Variable, as defined in Appendix A, “Event actions” on page 891.
With this event action, you can set a new system variable or reset the value of an existing system variable. For example, you can create an event action plan with an action to set the variable DatabaseServerRebooted to true. After the action has been executed at least once, you are then be able to select that variable from the System Variables tab for a filter in another event action plan, as shown in Figure 12-54.

![Figure 12-54 System Variables tab](image)

You can use the value of this variable as a filter in this new event action plan.
12.5 Event actions

With the exception of Add Event to Event Log, each type of event must be customized by either double-clicking or right-clicking and selecting Customize. Event actions are used to specify which actions you would like IBM Director to take as a result of the occurrence of an event. The Event Actions pane, shown in Figure 12-55, lists the predefined action types.

![Figure 12-55 Predefined actions in Actions pane](image)
A list of the event actions supported in IBM Director and a brief description of each is provided in Table 12-2.

<table>
<thead>
<tr>
<th>Event actions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/remove event system to static group.</td>
<td>Adds a managed system to or removes a managed system from a specified static group when the managed system logs a specific event.</td>
</tr>
<tr>
<td>Add/remove source group members to a target static group.</td>
<td>Adds all managed systems in a source group to a target group or removes all specified managed systems from the target group.</td>
</tr>
<tr>
<td>Add a message to the console ticker tape.</td>
<td>Displays a message in red type that scrolls from right to left at the bottom of IBM Director Console.</td>
</tr>
<tr>
<td>Add to the event log.</td>
<td>Adds a description of the event to the event log.</td>
</tr>
<tr>
<td>Define a timed alarm to generate an event.</td>
<td>Generates an event only if IBM Director does not receive an associated event within the specified interval.</td>
</tr>
<tr>
<td>Define a timed alarm to start a program on the server.</td>
<td>Starts a program on the management server if IBM Director does not receive an associated event within the specified interval.</td>
</tr>
<tr>
<td>Log to textual log file.</td>
<td>Generates a text log file for the event that triggers this action.</td>
</tr>
<tr>
<td>Post to a newsgroup (NNTP).</td>
<td>Sends a message to a newsgroup using the NNTP protocol.</td>
</tr>
<tr>
<td>Resend modified event.</td>
<td>Creates or changes an event action that modifies and resends an original event.</td>
</tr>
<tr>
<td>Send an alphanumeric page (through TAP).</td>
<td>Sends a message to a pager using the Telocator Alphanumeric Protocol (TAP).</td>
</tr>
<tr>
<td>Send an event message to a console user.</td>
<td>Displays a pop-up message on the management console of one or more specified users.</td>
</tr>
<tr>
<td>Send an e-mail via SMTP.</td>
<td>Sends an e-mail message.</td>
</tr>
<tr>
<td>Send an SNMP inform to an IP Host.</td>
<td>Sends an SNMP inform request to a specified IP Host.</td>
</tr>
<tr>
<td>Send an SNMP trap to a NetView® host.</td>
<td>Generates an SNMP trap and sends it to a specified NetView host using a TCP/IP connection to the host. If delivery of the SNMP trap fails, a message is posted in the history log of the managed system.</td>
</tr>
</tbody>
</table>
Event actions | Description
---|---
Send an SNMP trap to an IP host. | Generates an SNMP trap and sends it to a specified IP address or host name.
Send a numeric page. | Sends a numeric-only message to the specified pager.
Send a TEC Event to a TEC Server. | Sends a Tivoli Enterprise Console® event to a TEC Server.
Set an event system variable. | Sets the managed system variable to a new value or resets the value of an existing system variable.
Start a program on a system. | Starts a program on any managed systems on which IBM Director Agent is installed.
Start a program on the event system. | Starts a program on the managed system that generated the event.
Start a program on the server. | In response to an event, starts a program on the management server that received the event.
Start a task on the event system. | In response to an event, starts a non-interactive task on the managed system that generated the event.
Update the status of the event system. | When the selected resource status generates an event, the status of the managed system associated with the resource is set or cleared according to your specification.

Event action right-click options
All event actions have right-click context menus. These menus include several tools for troubleshooting and maintaining the actions. See Table 12-3.

**Note:** Not all of these items apply to all actions.

<table>
<thead>
<tr>
<th>Menu</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize</td>
<td>Enables the creation of custom actions.</td>
</tr>
<tr>
<td>Add to Action Plan</td>
<td>Adds the action to the currently selected action plan.</td>
</tr>
<tr>
<td>Show Implementations</td>
<td>Shows which EAP the action is used in.</td>
</tr>
<tr>
<td>Rename</td>
<td>Enables you to rename the action.</td>
</tr>
<tr>
<td>Update</td>
<td>Enables you to modify or copy an action.</td>
</tr>
</tbody>
</table>
Event data substitution variables
Event actions can use event data substitution variables as a part of the actions. This allows you to personalize the actions to be specific to the event generated.

Table 12-4 lists the available substitution variables. See Event Data Substitution in the IBM Director help for more information.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;date</td>
<td>Specifies the date the event occurred.</td>
</tr>
<tr>
<td>&amp;time</td>
<td>Specifies the time the event occurred.</td>
</tr>
<tr>
<td>&amp;text</td>
<td>Specifies the event details, if supplied by the event.</td>
</tr>
<tr>
<td>&amp;type</td>
<td>Specifies the event type criteria used to trigger the event. For example, the event generated when a system goes offline is of type Director.Topology.Offline. This corresponds to the entry in the Event Type tab, shown in 12.4.2, “Event Type tab” on page 696.</td>
</tr>
<tr>
<td>&amp;severity</td>
<td>Specifies the severity level of the event.</td>
</tr>
<tr>
<td>&amp;system</td>
<td>Specifies the name of the system for which the event was generated. The system name is either the name of the IBM Director client, or in the case of SNMP devices, the TCP/IP address.</td>
</tr>
<tr>
<td>&amp;sender</td>
<td>Specifies the name of the system from which the event was sent. This keyword returns null if unavailable.</td>
</tr>
<tr>
<td>Variable</td>
<td>Meaning</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&amp;group</td>
<td>Specifies the group to which the target system belongs and is being monitored by. This keyword returns null if unavailable. Our testing showed that this field is blank for most events.</td>
</tr>
<tr>
<td>&amp;category</td>
<td>Specifies the category of the event, either Alert or Resolution. For example, if a system goes offline, the category is Alert. If the system comes online, the category is Resolution.</td>
</tr>
<tr>
<td>&amp;pgmtype</td>
<td>Specifies a dotted representation of the event type using internal type strings.</td>
</tr>
<tr>
<td>&amp;timestamp</td>
<td>Specifies the coordinated time of the event (milliseconds since 1/1/1970 12:00 AM GMT).</td>
</tr>
<tr>
<td>&amp;rawsev</td>
<td>Specifies the non-localized string of event severity (FATAL, CRITICAL, MINOR, WARNING, HARMLESS, UNKNOWN).</td>
</tr>
<tr>
<td>&amp;rawcat</td>
<td>Specifies the non-localized string of event category (ALERT, RESOLVE).</td>
</tr>
<tr>
<td>&amp;corr</td>
<td>Specifies the correlator string of the event. Related events, such as those from the same monitor threshold activation, will match this.</td>
</tr>
<tr>
<td>&amp;snduid</td>
<td>Specifies the unique ID of the event sender.</td>
</tr>
<tr>
<td>&amp;sysuid</td>
<td>Specifies the unique ID of the system associated with the event.</td>
</tr>
<tr>
<td>&amp;prop:filename#propname</td>
<td>Specifies the value of the property string propname from property file filename (relative to \TivoliWg\classes).</td>
</tr>
<tr>
<td>&amp;sysvar:varname</td>
<td>Specifies the event system variable varname. This keyword returns null if a value is unavailable.</td>
</tr>
<tr>
<td>&amp;slotid:slot-id</td>
<td>Specifies the value of the event detail slot with the non-localized ID slot_id.</td>
</tr>
<tr>
<td>&amp;md5hash</td>
<td>Specifies the MD5 hash code (CRC) of the event data (good event-specific unique ID).</td>
</tr>
<tr>
<td>&amp;hashtxt</td>
<td>Specifies a full replacement for the field with an MD5 hashcode (32-character hex code) of the event text.</td>
</tr>
<tr>
<td>&amp;hashtxt16</td>
<td>Specifies a full replacement for the field with a short MD5 hashcode (16-character hex code) of the event text.</td>
</tr>
</tbody>
</table>
Action: creating a pop-up message

The first action we create is a pop-up message on a system using the `net send` command.

**Tip:** When you use event data substituting variables, do not use punctuation after the variable:

- Good example:
  ```
  &system
  ```
- Bad example:
  ```
  &system.
  ```
  &system will not be correctly interpreted because of the period.

**Note:** NET SEND relies on the Windows Messenger service (not MSN IM). On Windows Server 2003 the Messenger service is disabled by default.

IBM Director has a standard action that opens a pop-up message on the window of any system currently running the console. However, because you cannot always be sure that the person who needs to receive the message is running IBM Director Console, we do a pop-up using another method. If you want to send a pop-up to a console, use the action described in “Send an Event Message to a Console User” on page 905.

To configure a `net send` action to send a pop-up window to user Martin, do the following:

1. Determine the IP address or host name of the system on which you want the pop-up to appear on.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>&amp;otherstring</td>
<td>Specifies the value of the detail slot with the localized label that matches otherstring. This keyword returns OTHERSTRING if unavailable.</td>
</tr>
</tbody>
</table>
2. In the Event Action Plan Builder window, right-click **Start a Program on the Server** in the Actions pane, and click **Customize**. The Customize Action window appears, as shown in Figure 12-56.

![Image of Customize Action](image-url)

**Figure 12-56  Customizing Start a program on the server action**

3. Enter the following line in the Program Specification field:

```
cmd /c net send martin "&severity - &text on &system"
```

You can leave the working directory blank because CMD.EXE is in the Windows path.

The `cmd /c` tells Windows on the IBM Director Server to close the window automatically when the command is completed. The remainder of the line is the command line that will be executed.

The event data substitution variables in the command line will be substituted with the name of the system that generated the event and some of the event details. See “Event data substitution variables” on page 732.

4. Select **File → Save As** to save the action.

5. Type the name of the action. We use **Net send message to Martin**.
6. The new action appears in the Actions pane, as shown in Figure 12-57.

![Event Action Plan Builder](image)

Figure 12-57   The Net send message is created

**Tip:** When you build other similar actions, also name them starting with *net send*. Because IBM Director sorts actions alphabetically, the actions will be grouped logically.

**Action: creating an e-mail notification**

The second type of action we demonstrate with our example is an e-mail notification. This is usually the first type of event that most IBM Director administrators set up. E-mail notification is very flexible because it can be used to generate standard e-mail messages, as well as to send messages to most pagers and mobile phones.

1. From the Action pane, right-click **Send an Internet (SMTP) E-mail**, and click **Customize**.
2. Fill in the fields using values similar to those in Figure 12-58.

![Customize Action: e-mail sysmons - generic](image)

**Figure 12-58  Customizing an e-mail action**

3. Select **File → Save As** to save the action and enter the name of the action. We entered `e-mail sysmons - generic` in our example. The advantage of using the data substitution variables is that the message will provide detailed event information, regardless of the event or system it is applied to.

If we were sending the message to a pager, we would start the name with `Pager`. If we were using a telephone, it would start with `Phone`. This ensures that entries are grouped in a convenient fashion.

4. The new action now appears as a child task listed under Send an Internet (SMTP) E-mail (Figure 12-59).

![Send an Internet (SMTP) E-mail](image)

**Figure 12-59  New e-mail action**
Tip: You can specify only one e-mail address in the Internet e-mail address field. If you need to send the events to more than one user, we recommend that you create mail-groups on the mail server in your infrastructure and address the events to the mail-groups. This method is more flexible, because you can add and remove e-mail addresses from the mail-group on the server instead of having to update several e-mail actions in your EAP.

The output of our example is shown in Figure 12-60.

![Figure 12-60](image-url)

Figure 12-60  The e-mail that was based on our action

Note: The e-mail action will always add the following event data substitution variables to the e-mail:

- Event Text (&text)
- Date (&date)
- Severity (&severity)
- Event Type (&type)
- System name (&system)
- Sender name (&sender)
Using action history
IBM Director can log the execution of the actions that are processed. This action history is useful in determining when events occurred, when actions were processed for the events, and whether the action was successful on completion. This can be helpful in troubleshooting the successful function of actions.

Action history must be enabled before logging of the action will begin. This must be done for each customized action for which you wish to capture a history. To enable action history on a customized action, follow these steps:

2. Find the customized action you wish to enable. Right-click the action, and click Action History → Enable.

To view the action history of an action, follow these steps:

2. Right-click the customized action you wish to view, and select Action History → Show from the menu.
3. The action history is displayed, as shown in Figure 12-61. Highlight the entry to view its associated information.

**Tip:** To make it easier to view the information click **View → Horizontal Split**. Then resize the window to view the information.

![Action History: e-mail sysmons - generic](image)

**Figure 12-61  Action history: Action Details**

To refresh the window, select **View → Refresh** from the menu or click ![refresh icon]. It can take several minutes for an action to complete running. When it is complete, the end status is displayed.

### 12.6 Example: creating an event action plan

In this section we create a new event action plan.
Successful implementation of EAPs requires planning and consideration of how they will be implemented and used. Developing and following strict naming standards is very important.

Actions should be as descriptive as possible to reflect the action that will take place. The Event Action Plan Builder sorts actions and sub-actions (those actions you create using the Customize menu option) alphabetically. Consequently, you should name your actions so that they are grouped together.

First, determine the goal of the action plan. You should consider which systems you intend to target with the action plan. This could be all systems, a subgroup of systems, or a specific system.

**Step 1: Create a new event action plan**

Follow these steps:

1. Open the Event Action Plan Builder from the main Console window.
2. Click **File → New → Event Action Plan** or right-click in the Event Action plan pane, and click **New**.
3. Enter a name for your event action plan, and click **OK**.

![Create Event Action Plan](image)

*Figure 12-62  Enter the name for the EAP*

4. The EAP is displayed in the Event Action Plans column of the Event Action Builder window (see Figure 12-63). If it does not appear, click the refresh icon ( ).

![Event Action Plans](image)

*Figure 12-63  New event action plan*
Step 2: Add filters
The next step is to add filters to the action plan to allow it to capture only specific events. You can use either predefined filters or create new ones.

1. From the Event Action Plan Builder window, select the **Fatal hardware event** filter.
2. Drag the filter to the action plan just created.
3. Select the additional filters you will include, and drag them to the action plan. We have included the agent offline filter as well as the default severity for agent offline, which is harmless. This will not change the severity, but if the agent goes offline it will be handled as part of the Fatal Events EAP.

**Note:** For steps 2 and 3, remember that filters cannot be added to other filters, only to action plans. Also, actions cannot be added to action plans, only to filters.

The new filters will be listed below your new action plan, as shown in Figure 12-64.

![Figure 12-64  Filters after being added to the New EAP](image)

Step 3: Add actions
Now that you have added the necessary filters to the action plan, the next step is to add the actions that IBM Director will take with each of these filters. Simply drag and drop the desired actions onto the filters.
In this example we added two actions to the Fatal Events filter and three actions to the Director Agent Offline filter. Events caught by either filter will start a ticker tape on the IBM Director console, and send an e-mail. In addition, the Director Agent Offline filter will execute a command that will try to restart the agent on the affected machine.

![Figure 12-65 Actions added to the New EAP](image)

**Step 4: Applying the event action plan to systems**

Now that we have an action plan, we must apply (or associate) that action plan to a system or a group. When an action plan is created, it is added as a task in the IBM Director Console main window.

![Figure 12-66 New event action plan listed as a task](image)

If your goal is to apply an action plan that is specific to a system, you should create a group, put the system into the group, then apply all monitors and action plans to the group. This makes it easier when you add new similar systems. Just add them to the group, and all of the same monitors and action plans are automatically applied to them.
12.7 Event flow

After you have installed your management server and your managed systems are discovered and appear in the console, then event handling is activated. All of the managed systems send events automatically to the management server. If they are managed by more than one management server, the managed systems send their events to all of the servers. The events are sent as a UDP packet on port 14247 to all trusted management servers.

If the managed system appears in the server console with a padlock (meaning that the server does not have the authority to access the managed system), events are not sent to this management server.

When a Level-2 managed system sends an event to the management server the following events happen, as shown in the network trace in Figure 12-67:

1. The managed system does a broadcast to check whether the management server is responding (line 1 in Figure 12-67). If the managed system already knows the IP and MAC address of the management server, it does not send this broadcast.

2. The management server responds with its IP address and MAC address (line 2).

3. The managed system sends the event on port 14247 as a UDP packet to the management server (line 3).

4. The management server responds with an acknowledgement (line 4).

5. The management server sends a packet back to the managed system verifying the event (line 5).

6. The managed system sends an acknowledge packet back to the management server (line 6).

<table>
<thead>
<tr>
<th>Src MAC</th>
<th>Dst MAC Ad Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>*BROADCAST ARP RARP ARP: Request, Target IP: 192.168.0.1</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>Agent A RARP ARP: Reply, Target IP: 192.168.0.2 Target Hdw Addr: 0004ACDEF84</td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td>Server UDP Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 172 (0xAC)</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>Agent UDP Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 11 (0xB)</td>
<td></td>
</tr>
<tr>
<td>Server</td>
<td>Agent UDP Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 105 (0x55)</td>
<td></td>
</tr>
<tr>
<td>Agent</td>
<td>Server UDP Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 11 (0xB)</td>
<td></td>
</tr>
</tbody>
</table>

Figure 12-67  Communication between the agent and server when an event is issued

By default, the event action plan Log All Events is applied to the group All Systems and Devices. (See Figure 12-10 on page 687.) This event action plan processes all events that IBM Director Server receives and logs them to the IBM Director event log. You can view this log using the Event Log task in IBM Director Console. In these cases, the event is sent by the managed system, and the filters
in the event action plans running on IBM Director Server determine whether to process or discard the event.

However, as described in 12.4.2, “Event Type tab” on page 696, when you select Any in the Event Type tab, not all event types are sent by IBM Director Agent to IBM Director Server. For example, the following event types are not sent to the management server unless they are specifically selected:

- CIM events
- Windows Event Log events

The reason for this is that these two event types could generate a significant network burden when there are large installations. If you do plan to enable these event types, be selective about the events that you want to monitor.

**Note:** When we use the term event log in this chapter, we mean the IBM Director event log. If we want to address the Windows event log or other event logs, we specifically use the term Windows event log.

### 12.7.1 Event queuing

By default, events are queued by IBM Director Agent when the link between the managed system and the management server is unavailable. You can prevent queuing of events at the filter level by enabling Block queued events, as described in 12.4.4, “Day/Time tab” on page 721.

Two scenarios in which this happens are:

- The management server is down or disconnected from the network.

  If the management server is not available in the network, the broadcast packet will not be replied to, and the event packet will not receive an acknowledgement packet.
The managed system will continue to send the packet until the management server comes back online, as in Figure 12-68:

- The network messages in the red box marked are where IBM Director Agent attempts to send the event to the server.
- In the server comes back online and some broadcasts are being sent by the management server to reestablish connectivity.
- In the management server receives the event packet, does a broadcast to determine the IP and MAC address of the managed system, and sends an acknowledge packet back.

<table>
<thead>
<tr>
<th>Src MAC...</th>
<th>Dst MAC Addr</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent</td>
<td>Server</td>
<td>UDP</td>
<td>Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 172 (0xAC)</td>
</tr>
<tr>
<td>Agent</td>
<td>Server</td>
<td>UDP</td>
<td>Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 172 (0xAC)</td>
</tr>
<tr>
<td>Agent</td>
<td>Server</td>
<td>UDP</td>
<td>Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 172 (0xAC)</td>
</tr>
<tr>
<td>Agent</td>
<td>Server</td>
<td>UDP</td>
<td>Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 172 (0xAC)</td>
</tr>
<tr>
<td>Agent</td>
<td>Server</td>
<td>UDP</td>
<td>Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 172 (0xAC)</td>
</tr>
<tr>
<td>Agent</td>
<td>Server</td>
<td>UDP</td>
<td>Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 172 (0xAC)</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>ARP_RARP</td>
<td>ARP: Request, Target IP: 192.168.3.1</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>ARP_RARP</td>
<td>ARP: Request, Target IP: 192.168.3.1</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>ARP_RARP</td>
<td>ARP: Request, Target IP: 192.168.3.1</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>ARP_RARP</td>
<td>Request, Target IP: 192.168.3.1</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>NET</td>
<td>Net: Registration req. for OSLO &lt;00&gt;</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>NET</td>
<td>Net: Registration req. for OSLO &lt;02&gt;</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>NET</td>
<td>Net: Registration req. for OSLO &lt;00&gt;</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>NET</td>
<td>Net: Registration req. for OSLO &lt;03&gt;</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>ARP_RARP</td>
<td>ARP: Request, Target IP: 192.168.0.20</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>ARP_RARP</td>
<td>ARP: Request, Target IP: 192.168.0.30</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>NET</td>
<td>Net: Registration req. for OSLO &lt;00&gt;</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>NET</td>
<td>Net: Registration req. for OSLO &lt;02&gt;</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>NET</td>
<td>Net: Registration req. for OSLO &lt;00&gt;</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>NET</td>
<td>Net: Registration req. for OSLO &lt;02&gt;</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>NET</td>
<td>Net: Registration req. for OSLO &lt;03&gt;</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>NET</td>
<td>Net: Registration req. for OSLO &lt;03&gt;</td>
</tr>
<tr>
<td>Server</td>
<td>*BROADCAST</td>
<td>NET</td>
<td>Net: Registration req. for OSLO &lt;03&gt;</td>
</tr>
<tr>
<td>Agent</td>
<td>Server</td>
<td>UDP</td>
<td>Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 172 (0xAC)</td>
</tr>
<tr>
<td>Agent</td>
<td>Server</td>
<td>UDP</td>
<td>Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 172 (0xAC)</td>
</tr>
<tr>
<td>Server</td>
<td>Agent</td>
<td>UDP</td>
<td>Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 11 (0x0B)</td>
</tr>
<tr>
<td>Server</td>
<td>Agent</td>
<td>UDP</td>
<td>Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 105 (0x0B)</td>
</tr>
<tr>
<td>Agent</td>
<td>Server</td>
<td>UDP</td>
<td>Src Port: Unknown, (14247); Dst Port: Unknown (14247); Length = 11 (0x0B)</td>
</tr>
</tbody>
</table>

Figure 12-68  Network trace with the server offline, then reestablishing connection to the agent

- The management server is online, but the IBM Director Server service has been stopped.

In this scenario, there is a potential for loss of the event.

The managed system sends a broadcast packet to the management server to determine its IP and MAC address, and because broadcast packets are handled by the operating system, it is returned to the managed system with the information. However, when the managed system sends the event
packet, it does not get an acknowledge packet from the management server, because they are sent by the IBM Director server application itself.

When you start the IBM Director Server service, the packets will be acknowledged by the topology server component of the IBM Director Server service. However, the event server service is not started yet, so the event itself will not be registered because the EAP is not available yet. The consequence of this is that the event will be lost.

There is a solution. If IBM Director Server or the management server itself is down, perform the following tasks:

1. Disconnect the network cable from the server before you start the IBM Director Server service or restart the server.
2. After the server boots up, log on.
3. Wait until the icon in the right corner changes to a green circle, meaning that the IBM Director server has started successfully.
4. Plug in the network cable.
5. The packets are acknowledged, and the EAP performs the tasks you have configured.

### 12.8 Recommended EAPs

This section offers general recommendations for configuring your filters and EAPs to get the most out of your IBM Director implementation. These are suggestions and can be considered as a minimum implementation, but we hope that they give you some ideas for expanding your EAP implementation in your environment.
12.8.1 Event filters

In general, we recommend that you use the Severity and Category tabs to create events based on their predefined severity. This makes the EAP less complicated to build and maintain. However, there can be situations in which you want to use the severity for most of the events, but you want to pick out some and create a custom action for these. This is an easy task if you use the exclusion event filters.

For example, to receive critical events from ServeRAID controllers, create an exclusion event filter with all of the ServeRAID events, and select Critical on the Severity menu. Then select the Exclusion Events tab and click ServeRAID Controller.Physical Drive.State.Failed. All critical events except hard drive failures will be sent based on the selection you just made.

Next, create a simple event filter, choosing only the ServeRAID Controller.Physical Drive.State.Failed event. Now you can send a generic alert for all of the critical ServeRAID events from the controller, and you can create a customized action for the hard drive failure.

Tip: An exclusion event filter without any exclusions is the same as a simple event filter.

Therefore, we recommend that you use exclusion event filters when you create filters based on severity, or if you select a filter subgroup. This makes it easier to pick out single events later if you want to create custom actions for them without having to restructure your EAP.

12.8.2 Log all events

When you install IBM Director Server, the Log All Events EAP is associated with the group All Systems and Devices, as shown in Figure 12-70.
However, it does not log absolutely all events. Even though the default simple event filter All Events has enabled the Any button, as shown in Figure 12-71, it logs all events except Windows Event Log events and CIM events.

It is a good idea to have one or two EAPs to take care of all of the logging so that you do not have to add the Add to Event Log action for all of your other EAPs. You are guaranteed that the events are logged, even if you are updating other active EAPs. Creating these logging EAPs also makes your other EAPs less complicated and easier to work with.

Figure 12-71  The default All Events filter

Selecting **Any** does not enable CIM events or Windows Event Log events. These must be explicitly selected.
To make it easier to maintain your EAPs, we recommend that you delete the default action and filter from the Log All Events action plan and create a new exclusion event filter instead of a simple event filter. One example is to create an exclusion event filter with the filter subgroups shown in Figure 12-72.

**Note:** We have not selected the Windows events on purpose. If we had selected them here and excluded them on the Exclusion tab, the managed systems would still send the events to the management server each time a registry key is changed or a Windows event log message is created, resulting in increased unnecessary network traffic.

![Exclusion Event Filter Builder: New](image)

**Figure 12-72  Example of an exclusion event filter that provides logging**

If you want to forward the Windows event logs to the management server as well, you can either activate the Windows Event Log filter in your existing All Events filter, or add a new event filter for the Windows Event Log events.
It might be a good idea to create a new EAP for the Windows Event Log events if you do not want to monitor this on all of your managed systems. Remember that doing so can increase network traffic. For example, you can monitor all events except Windows Event Log and registry changes on the client systems, then add the Windows event log action plan to a specific group of servers that you want to monitor more closely. See Figure 12-73.

Figure 12-73  Two EAPs that provide log functions and groups they are associated with
12.8.3 Hardware events for client systems and OEM hardware

Hardware events for clients and OEM hardware are easy to implement. The events are sorted under the CIM event filters. We recommend using the Severity and Category tabs to select the important events about which you want to be alerted. The CIM.System events filter informs you of many CIM events that occur on IBM and non-IBM systems, as shown in Figure 12-74.

![Event Log (CIM Hardware Events)](image)

These events are all resolution events, so if you do not want to be informed of these events, select only the **Alert** check box in the Category tab (see Figure 12-48 on page 723). If you have used the All Events filter in 12.8.2, “Log all events” on page 748, all of the events will be logged here, so it is not necessary to create a resolution event filter to log the events.

To create an event filter for the alert events, follow this procedure:

1. Right-click **Exclusion Event Filters** and click **New**.
2. In the Event Types tab, clear the Any check box and expand the CIM tree.
3. Click to select the **System** check box.
4. In the Severity tab, make sure that the Any check box is checked.

5. In the Category tab, clear the Any check box. Select the Alert check box (and clear Resolution).

6. Save the filter and give it a name. We named ours CIM hardware ALERT events.

7. Add the event filter to your desired EAP, and add the desired actions to it.

The EAP will look similar to Figure 12-75.

![Figure 12-75 Example of an EAP that will address CIM hardware events](image)

### 12.8.4 Hardware events for System x servers

The CIM.System filters described in the previous heading also work for System x servers, but there are two filter subgroups that provide more detailed information than the CIM.System:

- MPA
- Storage.ServeRAID Controller

We recommend that you use the MPA and Storage.ServeRAID Controller filters for System x servers that have a service processor and a ServeRAID adapter installed. For System x servers that do not have either of these components installed, we recommend that you use the CIM.System filters.

Here we provide an example of a simple EAP for System x servers that send the most important events to IBM Director Server. It is certainly possible to create more-sophisticated EAPs for hardware events, and this example is a good starting point for such EAPs.

1. Open the EAP Builder, right-click Event Action Plan, and click New.
2. Use xSeries Events for the action plan name.
3. Right-click Exclusion Event Filter and click New.
4. In the Event Types tab, clear the Any check box.
5. Click to select the **MPA** filter subgroup check box to select all service processor events.

6. Expand the **Storage** filter subgroup and, with the Ctrl key pressed, click to select the **ServeRAID Controller** check box to select all ServeRAID events as well.

7. In the Severity tab, clear the **Any** check box and select the **Fatal** and **Critical** check boxes (all others should be deselected).

8. Save the filter and name it **Critical and Fatal MPA and ServeRAID Events**.

9. Make a second filter based on the one you just created:
   a. In the Event Action Plan Builder, double-click the **Critical and Fatal MPA and ServeRAID Events** filter.
   b. In the Severity tab, deselect the Fatal and Critical events and select the **Minor**, **Warning**, **Harmless**, and **Unknown** events.
   c. Click **File → Save As** and name the filter **Informational MPA and ServeRAID Events**.

10. Drag the two Exclusion event filters you just created to the xSeries Events EAP.

11. Drag your desired actions to the filters. We use an e-mail and an SMS message in this example. Be certain your EAP looks similar to Figure 12-76.

![Event Action Plans](image)

**Figure 12-76** Example of an EAP for xSeries service processor and ServeRAID events
12. In IBM Director Console, drag the **xSeries Events** EAP to a group that contains all of your System x servers.

If you do not have a group for all of your System x servers, you can apply it to both the Level-1: IBM Director Core Services Systems and Level-2: IBM Director Agents groups. Together, these two groups contain all managed systems that are capable of sending events to a management server. By applying the EAP to these groups, you ensure that all hardware problems from all System x servers are reported.

### 12.8.5 Online and offline events

Two events should be issued by IBM Director whenever a managed system goes offline or comes online:

- Director.Topology.Offline
- Director.Topology.Online

Specifically, these are to be issued when IBM Director Agent is stopped or started, respectively.

**Note:** There was a bug in IBM Director 5.10, 5.10.1 and 5.10.2, where the topology.online event was not received with Server-Agent encryption is enabled. This was fixed in Version 5.10.3. The workaround was to disable encryption. See “Agent-server encryption” on page 142 for information about how to disable encryption using Add/Remove Programs (Windows) or `cfgsecurity` (Linux).

### 12.8.6 Example of an application EAP

We use Symantec AntiVirus as the application for this example. If you want to monitor an application, first you must ensure that the application is writing to the Windows Event Log since IBM Director collects events from it. In this example, we create filters based on severity. We then create custom actions for events that we want to monitor more closely using simple event filters.

1. Create a new EAP and name it *Symantec Antivirus events*.
2. Create a new exclusion event filter.
3. In the Event Types tab, deselect the Any check box.
4. Expand **Windows event log → Application**. Scroll down until you find Symantec AntiVirus.
5. Select the **Symantec AntiVirus** filter subgroup.
6. In the Severity tab, clear the Any check box.
7. Select the **Harmless** check box. This picks up both information and warning events from the Windows Event Log.
8. Save the event filter, naming it **Symantec Antivirus - Harmless Events**.
9. Drag the event filter to the event action plan Symantec Antivirus events.
10. Create a new event filter based on the one you just created.
    a. Double-click the **Symantec Antivirus - Harmless Events** exclusion filter.
    b. In the Severity tab, clear the Harmless check box and select the **Critical** check box.
    c. Click **File → Save As** and name the filter **Symantec Antivirus - Critical Events**.

**Note:** We use exclusion event filters for Symantec AntiVirus so that we can exclude some of the events later on, even for logging. We recommend that you use the action *Add to eventlog* for the harmless events and e-mail or SMS for the critical events.

11. Drag the critical events filter onto the EAP.
12. Drag your selected customized actions onto the exclusion event filters.
13. Exit the EAP Builder and apply the Symantec Antivirus Events action plan on a group that contains agents with Symantec AntiVirus installed.
14. Perform a LiveUpdate and a virus scan on one of your managed systems. Note the events in the IBM Director event log for that system.

15. In the Windows Application Event Log, note the event IDs that you do not want to monitor and exclude them:
   a. In the EAP Builder, double-click the Symantec Antivirus - Harmless filter.
   b. In the Excluded Event Type tab, deselect None.
   c. Expand Windows Event Log → Application → Symantec Antivirus and select the numbers that correspond to the events that you do not want to monitor.
   d. Save your updated exclusion event filter.

16. As a test, put a test virus file on a system and start a virus scan to verify that your EAP works for critical events. You can obtain a test virus from:
   http://www.eicar.org/anti_virus_test_file.htm

For reference, Table 12-5 lists the events that Symantec AntiVirus generates.

<table>
<thead>
<tr>
<th>ID</th>
<th>Severity</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Information</td>
<td>AntiVirus scan complete.</td>
</tr>
<tr>
<td>3</td>
<td>Information</td>
<td>AntiVirus scan started.</td>
</tr>
<tr>
<td>4</td>
<td>Information</td>
<td>Update of virus definition succeeded.</td>
</tr>
<tr>
<td>5</td>
<td>Error</td>
<td>Virus detected.</td>
</tr>
</tbody>
</table>
12.9 Exporting and importing EAPs

With the EAP Builder, you can import and export action plans to files. This enables you to move action plans quickly from one IBM Director Server to another or to import action plans that others have provided to assist in your implementation.

**Tip:** You can also use the `twgsave` and `twgrestore` commands to back up and restore an IBM Director Server configuration. See 5.6.2, “Special command-line tools” on page 277, for information.
12.9.1 Export

EAPs can be exported to three types of files:

- **Archive** backs up the selected action plan to a file that can be imported into any IBM Director Server.
- **HTML** creates a detailed listing of the selected action plans, including its filters and actions, in an HTML file format.
- **XML** creates a detailed listing of the selected action plans, including its filters and actions, in an XML file format.

To export an event action plan, follow these steps:

2. Select **File → Export**, then click the type of file you want to export to, as shown in “EAP Builder with Export option selected” on page 759.
3. Name the archive and set a location to save in the Select Archive File for Export window.

![EAP Builder with Export option selected](image)

12.9.2 Import

EAPs can be imported from a file. The file must be an Archive export of an action plan from another IBM Director Server. The steps to import an EAP are as follows:

1. Transfer the archive file to be imported to a drive on the IBM Director Server.
2. Open the Event Action Plan Builder from the main Console window.
3. Click **File → Import → Archive**.

4. From the Select File for Import window (Figure 12-78), select the archive file and location.

5. Click **OK** to begin the import process.

![Figure 12-78 Event action plan archive import](image)
6. The Import Action Plan window opens, displaying the action plan to import (see Figure 12-79). If the action plan had been assigned previously to systems or groups, you are given the option to preserve associations during the import. Select **Import** to complete the import process.

*Figure 12-79  The event action plans about to be imported*
This chapter presents several real-world scenarios that describe problems encountered by IT departments in performing daily systems management tasks. For each scenario, background information is provided to describe the situation. One or more typical problems are discussed, along with a solution using IBM Director and other readily available tools. We then give examples of how each scenario might be expanded to provide an even more complete solution.

The scenarios discussed are:

- 13.1, “IBM Director Agent on a cloned Windows system” on page 764
- 13.2, “Automated IBM Director Agent promotion” on page 776
- 13.3, “Creating status reports with DIRCLI” on page 793
- 13.4, “Quick-start implementation of IBM Director” on page 810
- 13.5, “Comparing system lists using a spreadsheet” on page 840
- 13.6, “Monitoring for prohibited applications” on page 846
- 13.7, “Monitoring for inventory changes” on page 858
- 13.8, “Data center planning using PowerExecutive” on page 867
13.1 IBM Director Agent on a cloned Windows system

This scenario discusses the issues associated with cloning a system running the IBM Director Agent under a supported Microsoft Windows operating system. These issues arise from the fact that the system name displayed in the IBM Director Console, purely a display name, is assigned to each managed system during installation of the IBM Director Agent. If the system is subsequently cloned, each clone will have the same display name, making them impossible to distinguish from each other in the management console.

To make matters more interesting, IBM Director Server keeps track of its managed systems using a unique machine identifier stored on each managed system. Of course, if a system on which the IBM Director Agent is installed is cloned, you effectively duplicate this identifier on each of the resulting clones, making it impossible even for the management server to distinguish between multiple managed systems. In this case, the first system discovered using a particular machine identifier is displayed in the management console while the remaining systems are ignored.

Tip: This scenario describes how to remove the unique identifiers from the IBM Director Agent install before the system is cloned.

IBM Director 5.10 also offers a new alternative, that is, the donor system can be imaged before the IBM Director Agent is installed. Once the cloned systems are online, IBM Director can discover them as Level-0 agentless systems and push the IBM Director Agent to them using Software Distribution and the IBM Update Assistant. See 13.2, “Automated IBM Director Agent promotion” on page 776.
IBM Director Agent

During installation of IBM Director Agent, the name of the managed system that is displayed in the management console is set. You see this at the end of the agent installation when the Network driver configuration window opens, as shown in Figure 13-1. In this window, you can specify a number of agent settings including the system name, which is the display name used by the management console. The default is the Windows system variable %ComputerName%.

![Network driver configuration](image)

Figure 13-1  IBM Director Agent network driver configuration utility

In the same window you can also configure network drivers and network time-out, as well as enable Wake on LAN if it is supported by the system’s NIC. If you choose to install the Remote Control subagent, you can also see settings associated with this option. After you click OK on this window, all settings are stored in the file `\data\netdrvri.ini`, located in the IBM Director Agent installation directory.

At the end of the IBM Director 5.10 Agent installation, the agent services are started. Note that rebooting the system after installing the agent is no longer required. Each time the IBM Director Support Program service starts, it checks to see that a unique machine identifier is present. This identifier is critical since it is what the management server uses to keep track of each managed system. If the identifier is not present when the service starts, it is created and stored in both
the Windows Registry and in `\data\twg\mach.id`, located in the IBM Director Agent installation directory.

**System cloning**

Cloning has become a popular method used by IT organizations for deploying servers, workstations, and desktop and mobile computer clients. This process uses a completely configured system as a donor. The steps associated with cloning a system running Microsoft Windows are:

1. Install the appropriate Windows operating system and applications on a computer that has hardware similar to the intended target computers. While building the computer, do not join it to a domain, because this process is reversed in step 3. This system is called the **donor** system.

2. While logged on as administrator, configure the donor system, including the Windows operating system itself and all installed applications. It is important to ensure that all appropriate drivers are installed and working properly.

3. When the computer is fully configured, prepare it for cloning by running Sysprep. The Sysprep utility is a Microsoft tool that aids in deploying cloned images by removing all system-specific operating system settings from the donor image before it is captured. For Windows XP and Windows Server 2003, Sysprep is located in the DEPLOY.CAB file, found in `\SUPPORT\TOOLS` on the installation CD. For complete details on how to use Sysprep and how it works, as well as downloading the latest version, go to the Microsoft Web site and enter `sysprep` in the search field.

   Execute `Sysprep.exe` on the donor system, according to your situation. If you want to image the donor system using Remote Deployment Manager, check the **Use Mini-Setup** box and click the **Reseal** button to begin execution. At the completion of this process, the donor system automatically shuts down.

4. Create a clone image of the donor hard drive using tools such as Remote Deployment Manager, Altiris Deployment Server, or Norton Ghost.

5. Deploy the captured image to other computers, creating clones of the donor. When a cloned system is started for the first time, it runs Plug and Play detection, creates new Windows security identifiers (SIDs), and runs the Mini-Setup Wizard.

   The Mini-Setup Wizard presents windows for final system configuration, including the following information:

   - License agreement acceptance
   - Regional and language options
   - User name and organization
   - License product key
   - Licensing modes (servers only)
   - Computer name and administrator password
Date and time settings
Network settings
Workgroup or computer domain

All of this information can be provided in a sysprep.inf file, which can be included as part of the image itself. In addition, if Remote Deployment Manager is used to create, manage, and deploy clone images, it can also be used to answer the Mini-Setup Wizard questions, completing the entire system deployment process automatically.

The cloning process is far more efficient than installing the operating system and applications from scratch on multiple systems. However, from an IBM Director perspective, potentially undesirable side effects are created by this process.
13.1.1 The problem

Although the Sysprep utility removes all system-specific operating system settings, it does nothing about application settings that must be system-unique, such as the IBM Director machine identifier or the system name stored in the netdrvr.ini file. Because all cloned systems possess the same machine identifier, only the first cloned system discovered by the management server is displayed in the console. If we fix only this problem, the management server discovers and differentiates all cloned systems, but displays all of them using the same system name in the management console, as illustrated in Figure 13-2.

Therefore, we must take certain steps before and after cloning to ensure that both the management server and system administrators are able to distinguish between the cloned systems.
13.1.2 The solution

As stated earlier, if the machine identifier is not found when the IBM Director Support Program service starts (because the twgmach.id file and the appropriate Windows Registry key have been deleted, for example), it is recreated automatically. This simplifies the first part of our solution, because we can make these deletions on the donor system before it is cloned (during step 2 on page 766).

1. Stop the IBM Director Support Program service. Because this service is set for automatic startup, it will resume automatically on each of the cloned systems after the entire process is complete.

**Important:** If the browser-based access component is installed, there are multiple additional issues that must be resolved, including the reissue of security certificates. Because we do not recommend installing this separate optional component (see 3.3.4, “IBM Director Console” on page 112, for our reasoning), we do not discuss these issues in detail. We simply recommend not cloning a system with this component installed.

Instead, clone the system with only the IBM Director Agent installed, as covered here, then use IBM Director Software Distribution and IBM Update Assistant to install the browser-based access component on each managed system after the cloning process is complete.
2. After the agent service is stopped, remove the machine identifier. To do this, delete the twgmach.id file found in C:\Program Files\IBM\Director\data (assuming the default installation directory). A record of this value is also stored in the Windows Registry. Delete the Registry key TWGMachineID found in HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName. This key is shown in Figure 13-3.

![Registry Editor](image)

Figure 13-3 The IBM Director unique machine identifier key in the Windows registry

As stated earlier, if a new IBM Director Agent system name is not assigned to each cloned system, all systems cloned from the same image and discovered by IBM Director Server display the same name in the management console. While the management server recognizes each managed system as a unique entity, they are indistinguishable from each other to the console user.

The system name can be specified by running the IBM Director Agent network driver configuration utility and manually entering the desired name and other network driver settings, but this could be a tedious, error-prone, and time-consuming process.
A far better solution is to create an automated method of specifying all the necessary settings and rebuilding the netdrvr.ini file.

1. To address this, delete the netdrvr.ini file, which is found in C:\Program Files\IBM\Director\data (assuming the default installation directory), as shown in Figure 13-4.

![Figure 13-4](C:\Program Files\IBM\Director\data)

*Figure 13-4  Windows directory showing the location of the netdrvr.ini file*
2. To prepare for its regeneration after cloning is complete, place a response file for the IBM Director Agent network driver configuration utility at the root of the C: drive, as shown in Figure 13-5. In our scenario, we call this file DirAgent.rsp.

![DirAgent.rsp file created in preparation for cloning](image)

Figure 13-5   DirAgent.rsp file created in preparation for cloning

3. We can specify all network driver settings in this response file, as seen in Example 13-1. The network driver configuration utility can target this response file when it is launched for the first time on the cloned systems, effectively achieving automated custom configuration of the IBM Director Agent network driver.

Example 13-1   DirAgent.rsp response file used for automated custom configuration

```plaintext
[Agent]=Y
Driver.TCPIP=1
WakeOnLan=1
ReqUserAuthToScreen=0
DisableScreenSaver=1
DisableWallpaper=1
;AddKnownServerAddress=TCPIP::nnn.nnn.nnn.nnn
ShutdownDoesPoweroff=0
```

For details about the syntax of the response file, see “DIRAGENT.RSP contents” on page 202.

4. Finally, we need a mechanism to launch the IBM Director Agent network driver configuration utility automatically on each cloned system during its initial boot sequence. This requires only a single command, as follows:

```
C:\Program Files\IBM\Director\bin\tgipccf.exe /R:C:\DirAgent.rsp
```

5. Because a single command is all that we want, we can create a RunOnce Registry key to execute this task.
Any command handled by the RunOnce key will be executed only the first time Windows loads, right after Plug and Play device enumeration, but before the IBM Director Program service starts for the first time. This is precisely what we want, and therefore a great application of RunOnce. Using a RunOnce key has the added benefit of cleaning up after itself. That is, after the command is executed, the RunOnce key deletes itself so that it will not execute on subsequent reboots. This is also precisely what we want.

For more information about the RunOnce Registry key see:


There are a couple of options for creating the proper Registry entry. The safest method involves creating a Registry merge file. To do this, open a text editor and enter the text in Example 13-2 exactly as it appears. Note in particular that the first line is not optional.

Example 13-2   The AgentFix.reg file

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce]
"Agent Fix"=""C:\Program Files\IBM\Director\bin\twgipccf.exe" /R:C:\\DirAgent.rsp"
Save the text file using the .reg extension, such as AgentFix.reg, as shown in Figure 13-6. After you save it, this file can be executed to insert the proper string into the RunOnce Registry key without opening the Windows Registry editor. This should result in a modified key, shown in Figure 13-9 on page 775.

![AgentFix.reg file used to insert a RunOnce Registry entry](image)

6. You can now close any open windows, including the Windows Registry editor, that might be open on the donor system and proceed to “Summary” on page 775.

7. If you prefer to work directly inside the Windows Registry editor, open the editor to HKLM/SOFTWARE/Microsoft/Windows/CurrentVersion/RunOnce. There you should find only a default entry whose value is not set, as shown in Figure 13-7.

![RunOnce Windows Registry key in its empty state](image)

Right-click the RunOnce key in the left panel and select New → String Value. A new string value is added to the right panel. Enter a name for the string value, such as Agent Fix. Then double-click the string value to open the Edit String dialog box.
Type `C:\Program Files\IBM\Director\bin\twgipccf.exe /R:C:\DirAgent.rsp` as shown in Figure 13-8, and click **OK** to save the new string value.

![Figure 13-8 The Edit String dialog box of the Windows Registry editor](image)

The RunOnce key should now look similar to Figure 13-9.

![Figure 13-9 The RunOnce Windows Registry key with the Agent Fix string value properly configured](image)

8. You can now close any open windows, including the Windows Registry editor, that may be open on the donor system.

**Summary**

With the machine identifier removed, the response file in place, and the RunOnce key set, the donor system is now ready for Sysprep and the cloning process. Here we review what we have done and summarize the steps taken:

1. Stop IBM Director Support Program service.
2. Delete the `twgmach.id` file, found in `C:\Program Files\IBM\Director\data` (assuming default installation directory).
3. Delete the Windows Registry key `TWGMachineID`, which is found in `HKLM\SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName`.
4. Delete the `netdrvr.ini` file, found in `C:\Program Files\IBM\Director\data` (assuming default installation directory).
5. Place DirAgent.rsp file at root of C: drive.

6. Add a string value to the Windows Registry key found at HKLM/SOFTWARE/
   Microsoft/Windows/CurrentVersion/RunOnce with the value of:

   C:\Program Files\IBM\Director\bin\twgipccf.exe /R:C:\DirAgent.rsp

7. Run Sysprep in the normal fashion. The donor system is now ready to be
   cloned. The IBM Director Agent will fix itself prior to starting on each of the
   resulting clones.

### 13.1.3 Extending this scenario

The DirAgent.rsp file can contain switches for all of the IBM Director Agent
network driver parameters. The syntax is exactly the same as the diragent.rsp file
on the IBM Director installation CD.

One particularly useful option is to have a management server automatically
discover the newly configured system. This is achieved by uncommenting the
AddKnownServerAddress statement by deleting the semicolon. If you choose to
do this, you must supply a valid IP address for an IBM Director Server. Substitute
this address for nnn.nnn.nnn.nnn in the same statement.

**Tip:** The management server Discovery Preferences must be set to “Auto-add
unknown agents which contact server” for automated discovery to work.

### 13.2 Automated IBM Director Agent promotion

This scenario describes how to use IBM Director software distribution to push
IBM Director Core Services or the full IBM Director Agent to any selected
managed systems in the environment, thereby automating one of the most
time-consuming processes in implementing an IBM Director environment.

One of the most challenging aspects of implementing IBM Director in an IT
environment of any size has always been getting the IBM Director Agent installed
on all managed systems. Traditionally, this has involved either manual
installation of the agent on each system, or some semi-automated approach
such as was described in the previous edition of this book.

Focused on reducing this challenge, the latest release of IBM Director supports
the promotion of managed systems. That is, a Level-0 (agentless) system can be
promoted to Level-1 (IBM Director Core Services) or Level-2 (IBM Director
Agent) functionality. In addition, Level-1 systems can be promoted to Level-2
functionality. Both types of promotions can be achieved in a completely
automated manner using the *IBM Update Assistant* wizard (previously called Director Update Assistant) under the Software Distribution task.

In this scenario we configure Level-0 system discovery and import IBM Director Core Services and Agent installation packages using IBM Update Assistant. We then push these packages to four agentless systems using the Software Distribution task built into IBM Director, thereby promoting two Level-0 systems to Level-1 functionality and two Level-0 systems to full Level-2 functionality.

### 13.2.1 The problem

For many systems management environments, the most time-consuming and challenging aspect of implementing the solution is the installation of the management agent on all endpoints. In previous versions of IBM Director, the most common method of initial installation was to manually install the IBM Director Agent on each system that was to be managed.

To be sure, other methods were used as well, but each had its own set of issues. As described in 13.1, “IBM Director Agent on a cloned Windows system” on page 764, rolling out system images that already include the agent code can be tricky because of how IBM Director Server keeps track of managed systems internally. Similarly, implementing script-based silent installation methods can be complicated and confusing.

An ideal approach might be for the IBM Director Server itself to discover all potentially manageable systems and to install appropriate managed system code on target systems selected by the administrator.

### 13.2.2 The solution

In the current version of IBM Director, you can discover all potentially manageable systems, even if the IBM Director Agent is not installed, provided the proper network ports and protocols are not blocked in the environment. IBM Director Server uses DCOM on port 137 to discover and communicate with systems running supported Microsoft Windows operating systems and SSH on port 22 to discover and communicate with all other platforms and operating systems.

It is important to ensure that these ports and protocols are usable in your infrastructure if you intend to discover agentless systems.

An easily overlooked point of blockage is the Windows Firewall included in Microsoft Windows XP Service Pack 2. This personal firewall is enabled by default and prevents IBM Director Server from discovering any systems on which it is running.
For details on how to configure Windows Firewall to allow IBM Director Server to discover and manage client systems running Windows XP with Service Pack 2, see 5.2, “IBM Director discovery” on page 229.

**Agentless system discovery**

In addition to opening the proper ports on the target systems (DCOM on port 137 and SSH on port 22), to discover Level-0 (agentless) systems you must configure IBM Director Server Discovery Preferences for Level-0 Agentless Systems. See Figure 13-10 for an example of how these preferences might be set to discover all agentless systems on a specific subnet. Note that the settings shown in this example cause the IBM Director Server to search for Level-0 systems at 254 individual IP addresses in the range from 192.168.128.1 to 192.169.128.254.

![Figure 13-10  Discovery preferences set to discover Level-0 systems](image)

When IBM Director searches an IP address range for Level-0 systems, it performs this search one at a time. With IBM Director 5.10.1, this procedure takes about five seconds for each IP address (Version 5.10 took upwards of 20 seconds), so an entire subnet takes approximately 20 minutes to process.
Unless you must search the entire subnet, it is prudent to keep the range as small as possible. One way to do this is to import a list of specific IP addresses into IBM Director Discovery Preferences. Such a list is shown in Figure 13-11. To specify a range of IP addresses, put the starting and ending addresses on the same line.

Figure 13-11   List of IP addresses to import for Level-0 system discovery
This list might come from a spreadsheet or database file containing IP addresses of systems on your network. Importing such a list not only simplifies Level-0 system discovery configuration, it also makes address entry much less error prone. Importing the list shown in Figure 13-11 on page 779 results in the discovery configuration shown in Figure 13-12.

![Discovery Preferences](image)

After setting the appropriate discovery preferences, Level-0 systems are added to the IBM Director Console during each subsequent discovery that includes Level-0 device types.

**Software distribution**

Before an agentless system can be targeted by the Software Distribution task, you must import the packages you plan to push to the targets. IBM Update Assistant is a Software Distribution import wizard and the mechanism for importing IBM Director Agent installation packages for distribution. The sequence of windows from Figure 13-13 on page 781 through Figure 13-17 on page 785 shows the progress through the IBM Update Assistant wizard for importing an IBM Director Agent for Windows installation package.
If it is practical, it makes sense to have the source installation files available locally to the IBM Director Server. To do this, you might copy the files to the hard drive of the management server, or have them ready on CD or USB flash media prior to starting the IBM Update Assistant wizard. This way, you eliminate the network traffic associated with transferring potentially large amounts of data over the local area network (LAN). This is not a critical requirement, because the copy process happens only once for each software distribution package created.

1. To begin, select your file location, as in Figure 13-13.

2. IBM Update Assistant is a wizard that imports software that is distributed by IBM into IBM Director and creates a software package for distribution. Choose your package type. IBM Update Assistant can import two types of software packages:
   - Packages in the *Solution Install* format, an architecture that provides a universal way to package and distribute software

   Solution Install packages enable software distribution to Level-0, Level-1, and Level-2 managed systems. Solution Install packages contain the following elements:
   - Installable unit (IU) of software that is self-extracting, self-installing, and runs in silent, unattended mode
   - Installable unit deployment descriptor (IUDD) XML file, the PackagedIU.xml file that describes the dependencies of the package
   - Artifact XML file that describes the installation instructions for the IU
• An XML file in xSeries format that enables Software Health Check for the package

A Solution Install package can be in the form of a JAR file, a Zip file, or a Solution Install formatted directory structure that can be accessed through the ComponentNamePackagedIU.xml file (the ComponentName prefix is optional).

– Packages in the UpdateXpress for xSeries format

UpdateXpress packages can only be distributed to Level-2 managed systems. UpdateXpress packages contain the following elements:

• The software-update is self-extracting, self-installing, and runs in silent, unattended mode.

• An XML file in xSeries format describes the software-update file and how to install it. This file must also contain Software Health Check information in order for this function to work.

IBM Director Agent installation packages are Solution Install packages and can be found on the IBM Director CD that came with your System x server. The latest version of these packages can also be downloaded from the IBM Web site. See 1.8, “IBM Director resources” on page 26.
3. To import an IBM Director Agent installation package into the Software Distribution task, point IBM Update Assistant at the xSeries XML file (such as dir5.10_agent_windows.xml), which specifies the various details of the installation process. See Figure 13-14 on page 782 and Figure 13-15.

![IBM Director Agent for Windows installation package ready for import](image)

*Figure 13-15  IBM Director Agent for Windows installation package ready for import*
4. During the final step of the import process, a detailed view of the package is displayed (Figure 13-16). Here you can see details about the package, including the version of the software to be installed, which operating systems and hardware are supported by the package, whether a reboot is required in order to complete the installation, and other information.

![Figure 13-16](image)

**Details of the IBM Director Agent for Windows installation package**

5. You can specify an alternate response file for each package, effectively creating multiple installation methods for a single installer. That is, you could
import the IBM Director Agent for Windows installation package three times, using a different response file for each import. These three response files could be configured to install the IBM Director Agent with three different sets of options. For example:

- A completely standard default installation
- An installation that has Remote Control enabled
- An installation that has both Remote Control and Wake on LAN enabled

![Screen capture of IBM Update Package/Root Directory Location](image)

Figure 13-17  Selecting an alternate response file

Note that you cannot create multiple packages with the same name. Also, you do not have the option of specifying a name for a package during the import process. Therefore, if you want to create multiple packages using different response files, you must change the package names as you go. That is, you must follow these steps:

a. Create the first package.
b. Rename the first package.
c. Create the second package.
d. Rename the second package.
e. Repeat steps 1 through 4.

After you select an alternate response file, IBM Update Assistant creates the installation package and is ready to distribute the package to any appropriate target.

The IBM Director Agent for Windows installation package can be distributed to any managed system, whether it be Level-0, 1, or 2. Be aware, however, that UpdateXpress packages can only be distributed to Level-2 systems. Plan accordingly for this (for example, make sure that you install the full IBM Director Agent on all systems to which you will later want to push UpdateXpress packages), since automated updating of xSeries firmware,
Implementing IBM Director 5.20

BIOS, and drivers provides significant value and saves considerable time and effort.

When the import is complete and the software distribution package has been created, it is added to the All Software Distribution Packages category and the IBM Update Assistant wizard closes. To see the new package, you can click the Software Distribution icon in the main toolbar of the management console, or you can expand the Tasks pane and open the Software Distribution task, as shown in Figure 13-18.

![Figure 13-18 Imported software packages ready for distribution](image)

Figure 13-18 Imported software packages ready for distribution

After the package has been successfully imported, it is a simple matter of drag-and-drop to distribute the package to any target systems that have been discovered by the management server.

6. To do this, select all systems to receive the package. You can click, Shift+click, or Ctrl+click to highlight all of the systems on which you would like to install the IBM Director Agent. Once the intended target systems are selected, expand the Software Distribution icon in the toolbar, select **All Software Distribution Packages**, select the package to distribute (in this case, the IBM Director Agent for Windows installer package), and choose to
distribute the package. Figure 13-19 shows the final selection in this process. Note that each system currently selected is listed in the drop-down menu. Make sure that each system selected has met all the hardware and operating system requirements.

Figure 13-19   IBM Director Console with target systems selected for promotion to full Level-2 functionality
You can distribute the package immediately or schedule the distribution for a more convenient time, such as after hours or over a weekend. See Figure 13-20.

Figure 13-20  Job execution window ready to promote agentless systems to Level-2
You can follow the progress of the distribution by opening the job details window shown in Figure 13-21. If you do this, make sure to enable dynamic updates by selecting View → Dynamic Update. Otherwise, the status window will not be updated unless you click the update button. Also, it is usually helpful to select the highest level of detail by selecting View → Detail → High. After distribution has completed, the status window message states:

*SystemName* client job status changed to ‘Complete’

![Figure 13-21 Status details from a distribution of the IBM Director Agent](image)

The Execution History window also shows the job complete after the package has been successfully delivered, as shown in Figure 13-22 on page 790. Note
that completion of a software distribution job indicates successful delivery and not necessarily successful installation of the software. The IBM Director Agent installer takes several minutes to complete the actual installation after the Job Complete message is received.

Figure 13-22 Software distribution package successfully delivered to all target systems

After both software distribution and installation are complete, all targeted systems show their new state in the management console:

- Quinault and Snohomish have been promoted to Level-1 (IBM Director Core Services) functionality.
- Columbia and Skagit have been promoted to Level-2 (IBM Director Agent) functionality.
The IBM Director Server detects the change in *agent type* for each of the target systems during a presence check or inventory collection and automatically updates the management console accordingly. Figure 13-23 shows the IBM Director Console before the promotion process completed. All four target systems are Level-0 agentless systems.

*Figure 13-23 IBM Director Console showing all four target systems (Columbia, Quinault, Skagit, and Snohomish) as Level-0 (agentless) systems prior to promotion (Notice that no Level-1 systems have yet been discovered by the IBM Director Server.)*
Figure 13-24 shows successful promotion of the target systems, two having been promoted to Level-1 IBM Director Core Services, and two having been promoted to Level-2 IBM Director Agent functionality.

For the first time, IBM Director includes a method to install IBM Director Agent easily and automatically on managed systems that previously did not have any agent software installed. This capability is key to a successful deployment of an IBM Director management environment.
13.3 Creating status reports with DIRCLI

In a dynamic server environment, systems come and go. Systems can be renamed or moved, and sometimes new devices are added unexpectedly on your network. In order to keep up with this, IBM Director can be used to automatically create reports of various dynamic conditions in your IT environment.

In this scenario we show how you can utilize the command-line interface of IBM Director, also known as DIRCLI, to automatically generate status reports. In particular, we demonstrate how to extract data from the IBM Director database and create a report of the following characteristics of your environment:

- Systems added this week
- Systems currently offline
- Systems offline for more than a week
- Systems not returning inventory data
- Systems currently locked
- Systems with critical hardware status
- All critical events this week
- All events for a given server

This is not a comprehensive tutorial on DIRCLI, but merely a set of examples that show how you can utilize IBM Director more fully by implementing a structured way to extract information from the IBM Director database.

13.3.1 The problem

In most organizations, IT environments are ever-changing. Even if server systems are relatively stable and constant in terms of their number, location, responsibility, and so on, the client side is often a completely different story. Many organizations struggle with identifying and summarizing changes that have occurred recently in the managed environment.

IBM Director can be used to discover and manage systems in the network. It can inventory managed devices, monitor their health, and alert you in the event of a problem. However, there is no out-of-the-box reporting mechanism that summarizes issues and changes that have occurred in the environment over a given period of time.

It is likely that all of the desired information is available and stored in the IBM Director database. However, there is no canned report that brings this information together into a concise, quickly understandable format. This is due in large part to the fact that every customer has a different view of their
environment, has different priorities and pain points, and therefore would require an individual solution.

13.3.2 The solution

Because IBM Director has collected the data, it is simply a matter of retrieving the desired information from the database and pulling it together in a report. One very efficient way to accomplish this is to use the IBM Director command-line interface to do this work for you. For DIRCLI to produce useful results, a number of items need to be taken into consideration:

- Scanning the network
- Scheduling DIRCLI commands
- Setting user authority
- Collecting inventory
- Generating reports

**Scanning the network**

To make sure the information, especially inventory data, in the final report is current, it is a best practice to scan your network to discover new systems and devices just prior to generating the report. For our weekly report we use the built-in Scheduler function in IBM Director to schedule a job to run every Sunday evening.
Figure 13-25 and Figure 13-26 on page 796 show how to set up a new scheduled job to discover all managed objects every Sunday at 11:00 p.m.

**Tip:** Remember to schedule system discovery in a time frame with no other activity, because you do not want the discovery process to interfere with other scheduled tasks, such as replication or backup.
When this scheduled job is executed, the Discover All Managed Objects task is executed based on the current discovery preferences, which are set under **Options → Discovery Preferences**. In particular, remember to specify the IP addresses or address ranges used in the discovery process, especially for Level-0 systems and SNMP devices.

### Scheduling DIRCLI commands

All DIRCLI commands must be run directly on the IBM Director Server itself. Therefore, the program scheduler must also run on the management server. For Windows-based systems you can use the built-in task scheduler to configure when your scripts will run. For Linux-based systems you can use the crontab scheduler for this configuration.

We recommend creating a master script that runs all DIRCLI commands necessary for your report. For our example, this script creates a file containing all desired information and sends this output in an e-mail message. Our final script is shown in Example 13-15 on page 805.

### Setting user authority

When starting a DIRCLI command from the command shell, the authority used must be a member of the dirsuper group. It is not enough to be a member of the
diradmin group. If the current logged-in user is not a member of the dirsuper
group, you must start the command shell with the proper authority. To do this
under Windows, use the runas command. Example 13-3 shows this technique in
practice. The shell session first fails to run DIRCLI because the user authority is
not sufficient. Then, using runas, the command completes successfully.

Example 13-3  Windows-based command line with user authorization failure


c:\>dircli lsbundle
Error: Invalid user: DIRECTORSERVER\Administrator
c:\>runas /noprofile /user:dkibmdir cmd
Enter the password for dkibmdir:
Attempting to start cmd as user "DIRECTORSERVER\dkibmdir"
...

Under UNIX-based operating systems, you can use the su or sudo command, as
shown in Example 13-4. Again, in this example DIRCLI fails to run because the
user authority is not sufficient. Then, using su, the command completes
successfully.

Example 13-4  UNIX-based command line with user authorization failure


#dircli lsbundle
Error: Invalid user: kolsen
#su dkibmdir

Enter the password for dkibmdir:
Attempting to start shell as user dkibmdir
...

Collecting inventory

By default, when IBM Director discovers an object, inventory information is
collected on the object based on inventory collection preferences. Inventory
collection is refreshed every seven days by default. Make sure to configure these
preferences to ensure up-to-date information. You can change the refresh
interval and other inventory-collection parameters using the Inventory Collection
Preferences tab of the Server Preferences window.
Implementing IBM Director 5.20

If inventory collection has not been performed in a long time, your queries into the database might not reflect the current environment. This can be especially critical when listing details such as installed software or remaining hard disk drive space. If this type of information is important to you, it would be critical to understand which systems have not responded to an inventory collection request within a reasonable period of time.

Using DIRCLI, you can create a report that enumerates all systems that have not returned inventory data for 31 days or more. The DIRCLI command we created for this purpose is shown in Example 13-10 on page 802.

Generating reports
In this scenario we use the DIRCLI command-line interface to IBM Director to extract data from the management server. This is the much-improved successor to the former DIRCMD interface of previous versions of IBM Director. DIRCLI is used to access, control, and gather information from IBM Director Server.

Although much of the same information can be retrieved from most of the database engines supported by IBM Director using standard SQL query tools, the DIRCLI method is the only way to query the default Apache Derby database.

Note that everything we show here can also be performed using IBM Director Console. However, using DIRCLI allows these processes to be automated and scheduled.

The examples shown here can be used as building blocks for setting up your own customized reports. We show the commands we used to make it easy for you to write your own scripts.

Systems added this week
When systems get added to the network by multiple administrators, it might be important to have a method to identify which systems are new. This command
described here lists all systems that have been added to the network and discovered by IBM Director during the last seven days.

To do this, we use DIRCLI to create a group based on when the object was created, then extract the members of that group. The command we use to create the group is `server createdynamicgroup`. To list the content of the group created we use `lsmo`. If this group is not deleted after our report is generated, the management console will become cluttered over time. To accomplish this cleanup we use `rmgp`.

The entire script requires only three commands, one for each of the tasks to be executed, as shown in Example 13-5. Note that the first command spans two lines in this example.

**Example 13-5  Creating group based on dates**

```bash
dircli server createdynamicgroup -f 1WeekOld
PC_INV.TWG_MANAGED_OBJECT.DATE_CREATED ">=" "1130596795000"
dircli lsmo -N 1WeekOld
dircli rmgp 1Week0ld
```

The database table "PC_INV.TWG_MANAGED_OBJECT.DATE_CREATED" is where the values are stored. The format in which to define the criteria is in milliseconds since 1970.

**Tip:** To see the current entries in the inventory for a table, issue the command:

```
dircli server listinventoryvalues "table"
```

For our example, the command is:

```
dircli server listinventoryvalues
PC_INV.TWG_MANAGED_OBJECT.DATE_CREATED
```

As the values in the table are stored in a special numeric format, we need some way of converting the date and time values to a value that we can easily interpret. Under Windows you can use the VB script `timediff` command, shown in Example 13-6, and for Linux you can use the Perl script `gmtime` shown in Example 13-7 on page 800. You can then list the content of the group, and delete the group again.

**Example 13-6  Visual Basic® script to create a group based on date and time values**

```vb
Option Explicit
'Note, chr 34 equals a quotation mark (from the ASCII table)
'objShell to run
```
Dim objShell
'Command to run (dircli.exe)
Dim Command
Command = "dircli.exe"
'The DirCli argument to run
Dim DirCliArg
'Used for time and date calculation
Dim TimeDiff
'Create Shell object.
Set objShell = WScript.CreateObject("WScript.Shell")
'Enumerate systems added in last 7 days
'Calculate current time minus 7 days, prefixing it with three zeros to add milliseconds
TimeDiff = " " & DateDiff("s","01-01-1970",DateAdd("w",-7,Now())) & "000"
'Create group based on above criteria
DirCliArg = "server createdynamicgroup -f 1WeekOld PC_INV.TWG_MANAGED_OBJECT.DATE_CREATED " & CHR(34) & ">=" & CHR(34) & TimeDiff
'Run dircli and wait for it
objShell.Run "%comspec% /c " & Command & DirCliArg,1,True

**Important:** Different tables exist for listing various attributes:

- PC systems are in PC_INV.TWG_MANAGED_OBJECT.DATE_CREATED
- UNIX systems are in UNIX_INV.TWG_MANAGED_OBJECT.DATE_CREATED
- iSeries systems are in com.tivoli.twg.inventory.as400.TWG_MANAGED_OBJECT.DATE_CREATED.

*Example 13-7 Perl script to convert date and time values*

```perl
#!/usr/bin/perl
$secDays = 60*60*24; #(sec-->min-->hour-->day)
$now = time();
$WeekAgo = $now - (7 * $secDays);
$weekAgo *= 1000; # convert secs to ms since 1970
system("dircli server createdynamicgroup 1WeekOld UNIX_INV.TWG_MANAGED_OBJECT.DATE_CREATED \">=\" $WeekAgo");
```

**Systems currently offline**

To list all systems that are currently offline, we use the lsmo command to list managed object attributes, where the attribute MO.state equals offline.
Because we only want to return Level-2 systems, we use the -t parameter to target specific object types (in this case the group Level 2: IBM Director Agents). The command is shown in Example 13-8.

**Tip:** To see all targets, run:

```
dircli lsmo -i
```

Example 13-8  All IBM Director Agents currently offline

```
dircli lsmo -w "MO.state=Offline" -t "Level 2: IBM Director Agents"
```

If there are no Level-2 systems offline, the query returns Execution Error: The select string did not resolve to any targets. This is not an error, it merely means that no objects were returned.

**Systems offline for more than a week**

The previous examples show basic uses of DIRCLI that return targets meeting a single criterion. In this section we look at creating a group of systems that meet multiple criteria.

To find systems that have been offline for more than a week, we use an inventory attribute called LAST_STAT_UPDT, which records the time/date stamp of the last state update for a given object. If combined with a parameter indicating that the current state is offline, we find exactly what we want. In other words:

All systems where (last state update <= Today - 7 days) AND (current state = Offline)

**Tip:** To list all inventory attributes, use `dircli listdynamicgroupscriteria` and use `dircli listdynamicgroupscriteria -r` to list which criteria are supported.

A Visual Basic script using this criteria is shown in Example 13-9.

Example 13-9  VB script that returns systems that have been offline for a week or more

```
Option Explicit
'Note, chr 34 equals a quotation mark (from the ASCII table)
'objShell to run
Dim objShell
```
'Command to run (dircli.exe)
Dim Command
Command = "dircli.exe"
'The DirCli argument to run
Dim DirCliArg
'Used for time and date calculation
Dim TimeDiff
'Create Shell object
Set objShell = WScript.CreateObject("WScript.Shell")
'Enumerate systems offline for more than a week
'Calculate current time minus 7 days, prefixing it with three zeros to add milliseconds
TimeDiff = " " & DateDiff("s","01-01-1970",DateAdd("w",-7,Now())) & "000"
'Create group based on LAST STATE UPDATE <= DATEDIFF
DirCliArg = "server createdynamicgroup -f 1WeekOffline PC_INV.TWG_MANAGED_OBJECT.LAST_STAT_UPDT " & CHR(34) & "\leq" & CHR(34) & TimeDiff & " AND PC_INV.TWG_MANAGED_OBJECT.STATE" & CHR(34) & " = " & CHR(34) & " Offline"
objShell.Run "%comspec% /c " & Command & DirCliArg,1,True

When the group is created, it is automatically populated. Use the previously described commands to list the members of the group. Remember to delete the group when you are finished with it. Running the command multiple times creates a new group with the same name.

**Systems not returning inventory data**

When creating groups using criteria that are not an exact match of an attribute, IBM Director also includes systems that do not match the criteria, because no inventory collection has been performed on that object. For this reason, locked systems will be included in groups, since no inventory collection has been performed on these systems.

To avoid this, we must include specific criteria when creating groups. One way of doing this is shown in Example 13-10, where we specify two criteria. We use both an upper and a lower date value, thus excluding the locked systems.

*Example 13-10  VB script that returns systems with no Inventory update for 31+ days*

Option Explicit
'Note, chr 34 equals a quotation mark (from the ASCII table)
'objShell to run
Dim objShell
'Command to run (dircli.exe)
Dim Command
Command = "dircli.exe \\
'The Dircli argument to run
Dim DirCliArg
'Used for time and date calculation
Dim TimeDiff
'Create Shell object
Set objShell = WScript.CreateObject("WScript.Shell")
'Enumerate systems not returning inventory for 31 days or more
'Calculate current time minus 31 days, prefixing it with three zeros to
add milliseconds
TimeDiff = " " & DateDiff("s","01-01-1970",DateAdd("w",-31,Now())) & 
"000"
'Create group based on PC_INV.TWG_MANAGED_OBJECT.LAST_UPDATE <= 
DATEDIFF & >= NOW
DirCliArg = "server createdynamicgroup -f 4WeeksNoInventory 
PC_INV.TWG_MANAGED_OBJECT.LAST_UPDATE " & CHR(34) & "<=" & CHR(34) & 
TimeDiff & " AND PC_INV.TWG_MANAGED_OBJECT.LAST_UPDATE " & CHR(34) & 
">=" & CHR(34) & DateDiff("s","01-01-1970",Now()) & "000"
objShell.Run "%comspec% /c " & Command & DirCliArg,1,True

Example 13-10 on page 802 only lists those systems that fulfill both criteria. This
can be seen in the dynamic group editor, as shown in Figure 13-27.

![](image)

**Figure 13-27** Two criteria, filtering out objects without inventory

**Systems currently locked**

To list all objects that are locked and have a padlock next to them in the
management console, we can use the Managed Object Attribute called
MO.accessdenied. The command to use is `lsmo` and the syntax is shown in Example 13-11.

*Example 13-11  Listing all locked systems*

```bash
dircli lsmo -w MO.accessdenied=true -A MO.IPaddrs,MO.IPhosts
```

Notice that we also return other attributes, namely the IP address and host name of the systems that are locked, using the `-A` parameter.

**Systems with hardware status critical**

IBM Director has built-in groups that might already contain the information that you want. To get a list of all objects marked as having a critical hardware status, you can use such a built-in group, simply listing the contents of the group.

*Example 13-12  Listing all systems with critical hardware status*

```bash
dircli lsmo -N "Hardware Status Critical"
```

**All critical events this week**

The command used by DIRCLI to list events is `event listevent`. You can specify three parameters:

- How many hours to go back in time
- Specific event to search for
- Object ID of the group or system

In Example 13-23 on page 844 we show how to return all critical events for the past week (168 hours).

*Example 13-13  List all critical events in the past week*

```bash
dircli event listevents -f "Critical Events" -h 168
```

**All events for a given server**

Filtering events for a given server is a bit more tricky. This is because the command takes an object ID as a parameter, so we need to use a script to get the object ID and use it as input for the event command. Such a script is shown in Example 13-14.

*Example 13-14  Perl script to list events for a specific system*

```bash
#!/usr/bin/perl
if(length(@ARGV[0]) == 0) {
    print "Usage error: Target not specified\n";
```

exit $rc;
}
$oid = `dircli lsmo -p @ARGV[0]`;
$rc = $?;
if($rc != 0) {
  exit $rc;
}
$oid = substr($oid, 2);
system "dircli event listevents -h 168 $oid";

**Putting it all together**
An example of a script that performs some of the previous examples is shown in Example 13-15.

*Example 13-15  VB script that summarizes some of the events*

```vbscript
Option Explicit
'Note, chr 34 equals a quotation mark (from the ASCII table)

'objShell to run
Dim objShell

'Command to run (dircli.exe)
Dim Command
Command = "dircli.exe 

'The DirCli argument to run
Dim DirCliArg

'Used for time and date calculation
Dim TimeDiff

'Create Shell object.
Set objShell = WScript.CreateObject("WScript.Shell")

'Start of Report

'First Report, Enumerate systems added this week
```
'Calculate current time minus 7 days, prefixing it with three zeros to add milliseconds
TimeDiff = " " & DateDiff("s","01-01-1970",DateAdd("w",-7,Now())) & "000"
'Create group based on above criteria
DirCliArg = "server createdynamicgroup -f 1WeekOld"
PC_INV.TWG_MANAGED_OBJECT.DATE_CREATED " & CHR(34) & " >= " & CHR(34) & TimeDiff
'Run dircli and wait for it
objShell.Run "%comspec% /c " & "echo These systems have been added the previously week: > 1weekold.txt",1,True
objShell.Run "%comspec% /c " & Command & DirCliArg,1,True
'Enumerate the group and pipe it to report
objShell.Run "%comspec% /c dircli lsmo -N 1WeekOld >> 1weekold.txt",1,True
'Delete the Group
objShell.Run "%comspec% /c dircli rmgp 1WeekOld",1,True

'Second Report, Level-2 Systems currently offline
'DirCliArg = " lsmo -w " & CHR(34) & "MO.state=Offline" & CHR(34) & "-t " & CHR(34) & "Level 2: IBM Director Agents" & CHR(34) & "-A MO.IPaddrs,MO.IPhosts"
DirCliArg = "lsmo -w " & CHR(34) & "MO.state=Offline" & CHR(34) & "-t " & CHR(34) & "Level 0: Agentless Systems" & CHR(34) & "-A MO.IPaddrs,MO.IPhosts"
'Run dircli and wait for it
objShell.Run "%comspec% /c " & "echo These systems are offline right now: > offline_systems.txt",1,True
objShell.Run "%comspec% /c " & Command & DirCliArg & ">>offline_systems.txt",1,True

'Third Report, Enumerate systems offline for a week or more
'Calculate current time minus 7 days, prefixing it with three zeros to add milliseconds
TimeDiff = " " & DateDiff("s","01-01-1970",DateAdd("w",-7,Now())) & "000"
'Create the group based on LAST STATE UPDATE <= DATEDIFF
DirCliArg = "server createdynamicgroup -f 1WeekOffline"
Pc_INV.TWG_MANAGED_OBJECT.LAST_STAT_UPDT " & CHR(34) & " <= " & CHR(34) & TimeDiff & " AND Pc_INV.TWG_MANAGED_OBJECT.STATE" & CHR(34) & " = " & CHR(34) & " Offline"
'Run dircli and wait for it
objShell.Run "%comspec% /c " & "echo These systems have been offline for more than a week: > 1WeekOffline.txt",1,True
objShell.Run "%comspec% /c " & Command & DirCliArg,1,True
'Enumerate the group and pipe it to report
objShell.Run "%comspec% /c dircli lsmo -N 1WeekOffline >> 1WeekOffline.txt",1,True
'Delete the Group
objShell.Run "%comspec% /c dircli rmgp 1WeekOffline",1,True

'Fourth report, Enumerate systems not returning inventory data for 31 days or more
'Calculate current time minus 7 days, prefixing it with three zeros to add milliseconds
TimeDiff = " " & DateDiff("s","01-01-1970",DateAdd("w",-31,Now())) & "000"
'Create group based on PC_INV.TWG_MANAGED_OBJECT.LAST_UPDATE <= DATEDIFF AND >= NOW
DirCliArg = "server createdynamicgroup -f 4WeeksNoInventory PC_INV.TWG_MANAGED_OBJECT.LAST_UPDATE " & CHR(34) & "<=" & CHR(34) & TimeDiff & " AND PC_INV.TWG_MANAGED_OBJECT.LAST_UPDATE " & CHR(34) & ">=" & CHR(34) & DateDiff("s","01-01-1970",Now()) & "000"
'Run dircli and wait for it
objShell.Run "%comspec% /c " & "echo These systems have not returned inventory for 31 days: > 4WeeksNoInventory.txt",1,True
objShell.Run "%comspec% /c " & Command & DirCliArg,1,True
'Enumerate the group and pipe it to report
objShell.Run "%comspec% /c dircli lsmo -N 4WeeksNoInventory >> 4WeeksNoInventory.txt",1,True
'Delete the Group
objShell.Run "%comspec% /c dircli rmgp 4WeeksNoInventory",1,True

'Fifth Report, Enumerate locked systems
DirCliArg = " lsmo -w MO.accessdenied=true -A MO.IPaddrs,MO.IPhosts"
'Run dircli and wait for it
objShell.Run "%comspec% /c " & "echo These systems are locked right now: > locked_systems.txt",1,True
objShell.Run "%comspec% /c " & Command & DirCliArg & ">> locked_systems.txt",1,True

'Sixth Report, Current critical systems
DirCliArg = " lsmo -N " & CHR(34) & "Hardware Status Critical" & CHR(34)
'Run dircli and wait for it
objShell.Run "%comspec% /c " & "echo These systems are in a critical state right now: > critical_systems.txt",1,True

objShell.Run "%comspec% /c " & Command & DirCliArg & ">>& critical_systems.txt",1,True

'Seventh Report, Critical events this week
DirCliArg = " event listevent -f " & CHR(34) & "Critical Events" & CHR(34) & " -h 168"

'Run dircli and wait for it
objShell.Run "%comspec% /c " & "echo These critical events happened in the previously week: > critical_events.txt",1,True

objShell.Run "%comspec% /c " & Command & DirCliArg & ">>& critical_events.txt",1,True

'Wrapping it all together and sending it as e-mail
objShell.Run "%comspec% /c " & "copy 1weekold.txt+offline_systems.txt+4WeeksNoInventory.txt+locked_systems.txt+critical_systems.txt+critical_events.txt weekly_status_report.txt",1,True

objShell.Run "%comspec% /c " & "blat.exe weekly_status_report.txt -to Server-Admins@company.com -server smtp.mailserver.com -f director@company.com -subject " & CHR(34) & "Weekly Status Report" & CHR(34)

objShell.Run "%comspec% /c " & "blat.exe weekly_status_report.txt -to torben@jungsberg.dk -server smtp.get2net.dk -f Director@hotmail.com -subject " & CHR(34) & "Weekly Status Report" & CHR(34)
The resulting e-mail is shown in Figure 13-28.

![Weekly Status Report - Meddelelse (Amdeligt tekst)](image)

<table>
<thead>
<tr>
<th>From: <a href="mailto:Director@hotmail.com">Director@hotmail.com</a></th>
<th></th>
<th>To:</th>
<th><a href="mailto:borhen@jungsberg.dk">borhen@jungsberg.dk</a></th>
<th>Cc:</th>
<th>Enne: Weekly Status Report</th>
</tr>
</thead>
</table>

These systems have been added the previously week:
Cisco
Himmelbjerget
Hudson
Molleboj
Server
XP
These systems are offline right now:
Hudson: ('192.168.1.34'), ('2000srv.localdomain', '2000srv.jungsberg.local')
Server: ('192.168.1.112'), ('P300')
XP: ('192.168.1.111'), ('MATRIX')
These systems have not returned inventory for 31 days:
These systems are locked right now:
Server: ('192.168.1.112'), ('P300')
XP: ('192.168.1.111'), ('MATRIX')
These systems are in a critical state right now:
These critical events happened in the previously week:

Figure 13-28 Weekly e-mail report generated using DIRCLI

**Note:** For the e-mail portion of the above example, we used Blat v2.5.0. If you use Blat as well, change settings, including the SMTP server.

### 13.3.3 Extending this scenario

Generating a weekly status report that summarizes the events during the previous week is fairly straightforward and easy using DIRCLI. You could extend this scenario by reporting on any combination of the nearly limitless variety of parameters, attributes, and conditions recognized by IBM Director.

You could also publish this information to an internal Web site, or have the reports stored in a Lotus Notes® database.
13.4 Quick-start implementation of IBM Director

You can use this scenario as a quick-start guide to get IBM Director up and running. In this scenario we show you how to use different subsets of many features in IBM Director.

For this scenario we consider a company that has a large complex heterogeneous IT environment spread out over multiple locations. This company has several objectives in implementing IBM Director as a systems management solution:

- Install IBM Director Agent on 367 servers.
- Install IBM Director Agent on 2,130 workstations.
- Provide access to IBM Director Console from separate locations, with access only to local systems.
- Decentralized failure alerts from hardware objects, including Predictive Failure Analysis alerts on fans, CPUs, memory, and VRMs.
- Alerting must vary based on the time of an event.
- Simple, single console usability.
- Use existing active directory global groups to delegate systems management authority.
- Track system downtime and uptime for a selected group of systems to document service availability.

In this scenario we show how you might achieve all of the above objectives using IBM Director in an efficient way. To prepare properly, we need to review the current environment and plan accordingly.
Network structure
The network structure of the company is displayed in Figure 13-29.

![Network structure for CP Corp](image)

Environment
The operating system is a mixture of servers running Microsoft Windows 2000 and Microsoft Windows Server 2003, and clients running either Windows 2000 or Microsoft Windows XP Professional. All machines are operating within a Windows Active Directory running in mixed mode.

Operation on servers is centralized and is controlled from the data center in Copenhagen. Operation on workstations is decentralized and is controlled from each country.
Active Directory setup
The existing group structure is shown in Figure 13-30. Access rights based on Global Groups is already in place. We reuse these groups and use them to authorize the users of IBM Director Console. For example, if a person is a member of the Greenland Global Group Helpdesk Workstations, he or she will have access only to the appropriate workstations.

13.4.1 The task
In this scenario we want to install IBM Director Agent and the System Availability extension remotely to eight servers in Greenland. Because the connectivity to Greenland is low bandwidth, we want to stage the IBM Director Agent code on a local file server. In addition, we want to automatically lock down the servers to only authorized personnel, set up appropriate alerting, and have the newly installed servers placed in an IBM Director group for ongoing management.

13.4.2 The solution
As you work your way through this scenario you can use different aspects of IBM Director in your organization.

The framework consists of the following tasks, which are accomplished before rollout of the management agent:

- Install and configure IBM Director Server.
- Create file distribution servers.
- Create installation response files.
Create Software Distribution packages.
Create dynamic groups.
Restrict access to dynamic groups.
Set groups to use proper file distribution servers.
Create event action plans for groups.

When this framework is built, we perform the following tasks:

- Install the management agent and have it contact the server so it can be discovered.
- Request access to managed systems.

After the management agents are in place, we end with these tasks:

- Distribute system availability.
- Verify systems.

Install and configure IBM Director Server
For our purposes the default installation of IBM Director Server is fine. After it is installed, however, we need to change a few parameters from their default configuration in order to satisfy the stated objectives.

First we need to enable the collection of software inventory information. By default, IBM Director collects only hardware data. To achieve this, execute the following steps:

1. Launch the management console and log on to IBM Director Server.
2. Select Options → Server Preferences.
3. Select the Inventory Collection tab to display the proper page.
4. Select All Available Data from the drop-down list next to IBM Director Agents (Level-2).
5. Click OK.
The server preferences for inventory collection in our environment are shown in Figure 13-31. IBM Director inventory collection now collects software data from all managed Level-2 systems.

![Server Preferences Window](image)

**Figure 13-31 Server preferences window set to collect full inventory from Level-2 systems**

**Create file distribution servers**

Later, when we push IBM Director Agent and other Software Distribution packages to managed systems, we want the packages to be streamed to target systems over the LAN, not through the WAN connection to our headquarters location. This is accomplished by designating file distribution servers.

For more information about file distribution servers and the Software Distribution task, refer to the publication *IBM Director Systems Management Guide*, located on the IBM Director installation CD or available on the Web.

A file distribution server is basically a file share configured on an existing server on the LAN. We decide to use a local file server named GLSRVFS01 and create
a share on it called director_distribution. This share is configured to allow full access rights to administrators and the IBM Director Service Account, as well as read access for all others.

After the share has been created, we configure IBM Director to use it. To add a file distribution server, follow these steps:

1. Select **Options → Server Preferences**.
2. Select the **File Distribution Servers** tab to display the proper page.
3. Click **Add**.
4. Enter the appropriate details for the share.
5. Click **OK**.

In our case, we added the file server in Greenland, as shown in Figure 13-32.

![Server Preferences window showing file distribution server configuration](image)

**Figure 13-32** Server preferences window showing file distribution server configuration

It is important to verify proper access to all file distribution servers before pushing a Software Distribution package to them in order to eliminate last-minute surprises. To verify that a file distribution server is accessible, follow these steps:

1. Click **Tasks → Software Distribution → Manage File Distribution Servers**.
2. Right-click the file distribution server and select **Test Access to Selected File Distribution Server(s)**.
3. If everything is working, you can see a green **Accessible** message, as in Figure 13-33.

![Figure 13-33](image)

*Figure 13-33 Verifying access to a file distribution server*

If you do not see the green accessible message, verify that the user account under which you are currently logged into IBM Director Server has write access to the share.

**Create installation response files**

Company policy states that all software installed on servers must reside on the D drive. However, for workstations there is only a single drive, the C drive, available. To address this requirement, we create two different IBM Director Agent installation response files, which are named:

- server-response-file-greenland.txt
- workstation-response-file-greenland.txt

The first response file, the one meant to install IBM Director Agent on server systems, is shown in Example 13-16.

*Example 13-16 IBM Director Agent installation response file*

```
[Agent]=Y
UseExistingTarget = N
TargetDrive = D
TargetFolder = Program Files\IBM\Director
EncryptCommunication = Y
SecureAgent = Y
Driver.TCPIP = 1
Driver.NETBIOS = 0
```
Driver.NETBIOS2 = 0
Driver.NETBIOS3 = 0
Driver.NETBIOS4 = 0
Driver.IPX = 0
NetTimeout = 30
ReqUserAuthToScreen = 0
DisableScreenSaver = 0
DisableWallpaper = 0
AddKnownServerAddress=TCP/IP::192.168.1.100
ShutdownDoesPoweroff = 0
RebootIfRequired = Y

The changes we have made from the default response file are on the following lines:

- UseExistingTarget = N
  The default setting is Y. We have changed this parameter to make sure that if for any reason IBM Director Agent has been installed previously in a non-default directory, it will not be used when upgrading. This will force the installation to always install at the location we specify by TargetDrive and TargetFolder.

- TargetDrive = D
  The default setting is C. We have changed this parameter to make sure that the management agent is installed on the D drive, in compliance with company policy.

- NetTimeout = 30
  The default setting is 15. We have changed this parameter to allow for a longer than default network time-out when attempting to communicate with the management agent. This is because we know that spikes, glitches, and time-outs are common on the fragile WAN connection to our Greenland location.

- Driver.NETBIOS = 0
  The default setting is 1. We have changed this parameter to disable NETBIOS because we are running a pure TCP/IP environment.

Create Software Distribution packages
When the response files are ready, we build two Software Distribution packages using IBM Update Assistant. The only difference in the packages is in the response file each will use. It is important to provide meaningful names to these packages so that they will not be confused in the future. For a detailed discussion of how to import the IBM Director Agent installation package see 13.2, “Automated IBM Director Agent promotion” on page 776.
Our Software Distribution packages can be seen in Figure 13-34.

These packages are later replicated to the local file distribution server in Greenland, so final streaming to target systems occurs over the Greenland LAN.

**Create dynamic groups**
We need to create dynamic groups for two purposes. First, this is an easy and effective way to authorize administration of systems, because user accounts can be configured to allow or prohibit access to all systems contained in a group. The second use of dynamic groups for our environment is to select file distribution servers, which can be assigned on a per-group basis.

We decide to build dynamic groups based on the attributes of managed systems. This ensures proper administrative authority, as well as correct assignment of File Distribution Servers, without having to keep any settings updated manually.

To create a dynamic group, select **Console → New → Group → Dynamic Group**.

Depending on our IT infrastructure and policies, there are several ways that we might create dynamic groups based on geographical location. If our IP addressing scheme is such that we can determine the location of a system by its IP address, we could build dynamic groups based on IP address range:

- Hardware → Network → IP-address → IP address > 192.168.80.1
- Hardware → Network → IP-address → IP address < 192.168.89.254

We might also be able to build dynamic groups based on the default gateway:

- Hardware → Network → IP-address → Default Gateway (router)
- OR
- Hardware → Network → IP-address → Default Gateway (router)
- OR
- etc.

For our example we have chosen to build dynamic groups based on the primary DNS server configured for each managed system, since this is the same for all systems in a given location.
We create two dynamic groups (Example 13-17 and Example 13-18) based on nearly identical sets of criteria. One will contain all workstations in the Greenland office and the other will contain only server systems located in Greenland.

**Example 13-17  Dynamic group for workstations**

Hardware → Network → IP-address → Primary Nameserver = 192.168.80.1 AND

Hardware → Operating System Specific → Operating System → Name = Windows XP

**Example 13-18  Dynamic group for servers**

Hardware → Network → IP-address → Primary Nameserver = 192.168.80.1 AND

Hardware → Operating System Specific → Operating System → Name = Windows Server 2000 OR

Hardware → Operating System Specific → Operating System → Name = Windows Server 2003

When selecting criteria for a dynamic group, remember that if the specific value does not appear in the list presented, you can add it manually as a seed value. For the primary name server criterion, this is shown in Figure 13-35.

![Dynamic Group Editor](Image)

*Figure 13-35  Adding a seed value to a dynamic group criterion*
Finally, we create a group category to contain all groups of systems we are interested in managing at the Greenland location. To do this select **Console → New → Group → Group Category**.

We label the category Greenland and add the two Greenland groups we previously created to the new category. The final result is shown in Figure 13-36.

![Figure 13-36 The Greenland group category and the two dynamic groups created](image)

**Restrict access to dynamic groups**

Next we want to configure the management console to allow a user access only to his specific job-related tasks and to perform these tasks only on the systems for which he is responsible. In addition, we want to use our existing Active Directory Global Group (ADGG) structure to implement this security policy. For example, we do not want anyone who is not a member of the Helpdesk ADGG to access our servers. To accomplish this we establish appropriate user profiles for IBM Director Console. For a detailed discussion of this topic see 3.4.4, “IBM Director Console security” on page 121.

To set authority on a by-group basis, we add the Helpdesk and Servers ADGGs into the local group DirAdmin on the management server. You can now see these added to ADGGs under the Groups tab in the User Administration window.

To configure access rights for the users in each group, select **Options → User Administration** and click the **Groups** tab, as shown in Figure 13-37.

![Figure 13-37 Active Directory Global Group user account management](image)
Carefully consider that the privileges, access rights, and restrictions you give to groups work in conjunction with specific user account rights. In addition, if a user account is a member of multiple groups, the account is granted rights that are a union of the rights associated with all groups of which it is a member. In addition, individual user account rights take precedence over those of any group. Again, these considerations are detailed in 3.4.4, “IBM Director Console security” on page 121.

For our environment, we configured privileges as shown in Figure 13-38.

---

**Figure 13-38** Global Group configuration, privileges
For our environment we configured group access rights, as shown in Figure 13-39.

![Global Group configuration, group access](image)

**Figure 13-39** Global Group configuration, group access
For our environment we configured task access rights, as shown in Figure 13-40.

Figure 13-40  Global Group configuration, task access

**Set groups to use proper file distribution servers**

As previously discussed, in order to maximize network efficiency, we must configure our managed systems to use the proper file distribution server. This ensures that when deploying packages, the target systems receive these large packages from the designated share on the LAN.

We can set this preference based on dynamic groups, once again ensuring proper assignment of file distribution servers without the need to make this setting for each individual managed system. To do this, perform these steps:

1. Right-click the dynamic group Greenland Workstations and select Distribution Preferences.
2. Select ADD to open a window displaying all file distribution servers.
3. Select the previously configured file distribution server for Greenland.
4. Click **OK**.

The finished result is shown in Figure 13-41.

![Distribution Preferences: Greenland Workstations](image)

**Figure 13-41  Specifying the file distribution server**

**Important**: Certain attributes of the members in the group must be fulfilled before the Distribution Preferences window will open. It is vital that the following conditions are met: All systems are online, all are Level-2 systems, and no systems are locked. If any of these conditions are not met for any member of the group, or the group is empty, the Distribution Preferences cannot be set for the group.

**Create event action plans for groups**
A nice feature of event action plans (EAPs) is their ability to be applied to an empty group. This allows the EAP to be configured and applied ahead of time.
Then, when a group is populated, all EAPs applied to the group are automatically applied to each managed object in that group. For more details on configuring EAPs refer to Chapter 12, “Event management” on page 675.

Based on our initial set of objectives, we configure EAPs to alert us in the event of problems in our managed environment. Our objectives included an item that called for de-centralized failure alerts from hardware objects, including PFA alerts on fans, CPUs, memory, and VRMs.

While designing our EAPs remember that:

- The management server is in one time zone (GMT+1), while the management console and managed systems are in another (GMT-3).
- All servers in Greenland are monitored 24/7.
  - From 06:00 AM local time CPH to 06:00 PM, they are monitored by the daily server staff in Copenhagen.
  - From 06:00 PM local time CPH to 06:00 AM, they are monitored by a third party outsourced company.
- All workstations in Greenland are monitored 24/7.
  - From 06:00 AM local time GL to 06:00 PM, they are monitored by the daily workstation staff in Nuuk.
  - From 06:00 PM local time GL to 06:00 AM, they are monitored by a third-party, outsourced company.

Based on these details, we create two EAPs for the servers, one for day-time alerting and one for after-hours alerting. For the workstations, we also create two EAPs, one for the day-time alerting and one for the night time alerting. However, because the daily staff is located in Greenland, we change the time zone to reflect this.

We have a total of four EAPs to configure. The easiest way to configure them is to start the EAP Wizard. Doing so will give us a baseline that we will customize to our needs. Start the wizard by clicking the magic wand inside the EAP Builder.
The Summary page of the Workstation Nightly EAP we created is shown in Figure 13-42.

When we click **Finish**, we can see the four precreated event filters already applied to the Greenland Workstations Group.
Although the EAP Wizard is useful to configure initial EAPs quickly, the wizard is not as granular as creating an EAP from scratch. However, now that we have used the wizard to create an EAP, we can modify the event filters slightly. We need to do this because the default time range for the filters covers the entire day. We want to specify that it will only process the event when it occurs between 06:00 and 18:00 in Greenland. To change the time, we open each nightly event filter and modify the Day/Time page, as shown in Figure 13-43.

![Figure 13-43 Fine tuning the time event filter](image)

Note that the time specified here is the time IBM Director Server will process the events, not the time the event actually occurs. This means that the workstation event filter needs to be customized to the Greenland time zone, which is four hours behind the home office in Copenhagen. Therefore, events occurring on Greenland systems will not be processed between 6:00 and 18:00, but between 2:00 and 14:00.

What happens is that IBM Director Server instructs the agent to monitor for the event types we have specified. Whenever an event occurs on a managed system, that event will be sent to the management server. Based on the system time of the management server, the event will trigger an action, sending an e-mail alert to the proper support staff.
After all EAPs have been created using the EAP Wizard, they will be applied to the proper groups based on the selections that we made in the wizard. It is a good idea to verify this by selecting Associations → Event Action Plans. This shows all EAPs that have been applied to each managed object. Note that you need to select a group category to see EAP associations for groups in that category, as shown in Figure 13-44.

Install the management agent
Though you can install IBM Director Agent in several ways, in this scenario we cannot use the Level-0 discovery method, then upgrade them level-2 using the Software Distribution task. The reason for this is quite clear. Software Distribution with Level-0 systems can only push out the agents. In our scenario, that would mean we would transfer an extreme amount of data over the wire.

Because only Level-2 systems can benefit from a redistributed installation, we need a way of easily deploying IBM Director Agent from a remote site. We can use the method mentioned in the previous scenario, but we can also use the power of group policy or, as we show in this section, how to start the agent-installation remotely using psexec.exe.

Here we deploy the agent. We just have one little task: to copy the response files and IBM Director Agent to the file share on the file server in Greenland. We use the Software Distribution task to do this.
For both packages, right-click and select Create Package for Delayed Delivery, as shown in Figure 13-45.

![Figure 13-45  Distributing the package](image)

This presents us with two choices, as shown in Figure 13-46. We can choose to copy it elsewhere in the network, but because we already have defined a file distribution server, it is more efficient to use that server. Click Next.

![Figure 13-46  Create package for delayed delivery](image)

Now we must choose which share to which to copy the file. Before you click Finish, open the file share we defined earlier in “Create file distribution servers” on page 814 by clicking Start → Run and entering \\glsrvfs01\director_distribution. The share should open up in Windows Explorer.
Click **Finish** and watch as the files are transferred. You should end up with a window similar to the one shown in Figure 13-47.

![Figure 13-47: The file distribution share after package delivery](image)

Each folder represents a package, and if you open up one of the folders, you can recognize the files inside. We need this exact location, so we can point all the systems at Greenland to install from this location. As you can see in Figure 13-48, the exact path to the executable is `\glsrvfs01\director_distribution\rdj6vpso\dir5.10_agent_windows.exe` and the response file for the servers is `\glsrvfs01\director_distribution\rdj6vpso\server-response-file-greenland.txt`.

![Figure 13-48: A peek inside the file distribution server](image)

The magic consists of the following ingredients:

- A list of all the servers and clients to which we want to push the agent. This will be the input to `psexec.exe`.
- A share on the local file server, which we use as the local file distribution server. This is the previously created file share on the file server in Greenland.
A customized response file, one for the servers, one for the workstations. These are the previously created response files, which now have been copied to the file share in Greenland.

The psexec.exe program from sysinternals.com. Download it from: 
http://www.sysinternals.com

Some batch-file coding.

The server list and the workstation list are just a list of the systems to which we want to install. The file is used as input to psexec, an example of the list is shown in Example 13-19.

Example 13-19  serverlist.txt - input file to psexec.exe

GLSRVAD01
GLSRVF0S01
GLSRVDHCP01
GLSRVDNS01
GLSRVMX01
GLSRVPRT01
GLSRVPRT02
GLSRVPRT03

We name the two files: serverlist.txt and workstationlist.txt.

We copy the psexec.exe and the two files to a local directory on our own machine, in our case C:\batch.

Because psexec cannot simply handle double quotation marks in its parameters, we create a batch file, and use psexec to execute it remotely. First, we copy the batch file to each server. We have two batch files, one for servers and one for workstations. These files do not need to be manually copied to the remote systems because the -c parameter on the psexec command will do that for us.

The content of batch file install-director-on-servers.cmd is shown in Example 13-20. In reality, this command is all on one line.

Example 13-20  Batch file install-director-on-servers.cmd

\\glsrvfs01\director_distribution\rdj6vpso\dir5.10_agent_windows.exe -a silent RSP="\\glsrvfs01\director_distribution\rdj6vpso\server-response-file-greenland.txt"
The content of batch file install-director-on-workstations.cmd is shown in Example 13-21. In reality, it is also all on one line.

**Example 13-21  Batch file install-director-on-workstations.cmd**

```
"\\glsrvfs01\director_distribution\rdj7bghe\dir5.10_agent_windows.exe -a silent RSP=
"\\glsrvfs01\director_distribution\rdj7bghe\workstation-response-file-greenland.txt"
```

And now we can start psexec to perform the remote installation, complete with response file. For server installs the command `psexec` command is as follows:

```cmd
C:\batch> psexec @serverlist.txt -u cpcorp\dirsvc -p aar4nahtanoJ -c install-director-on-servers.cmd
```

The result of this command is shown in Example 13-22.

**Example 13-22  Output from the psexec command**

```
PsExec v1.70 - Execute processes remotely
Copyright (C) 2001-2006 Mark Russinovich
Sysinternals - www.sysinternals.com

\\GLSRVAD01:
GLSVAD01>
C:\WINDOWS\system32>\\GLSRVFS01\director_distribution\rdj7bghe\dir5.10_agent_windows.exe -a silent RSP="\\GLSRVFS01\director_distribution\rdj7bghe\server-response-file-greenland.txt"
install-director-on-servers.cmd exited on GLSRVAD01 exited with error code 0.

\\GLSRVDHCP01:
GLSVAD01>
C:\WINDOWS\system32>\\GLSRVFS01\director_distribution\rdj7bghe\dir5.10_agent_windows.exe -a silent RSP="\\GLSRVFS01\director_distribution\rdj7bghe\server-response-file-greenland.txt"
install-director-on-servers.cmd exited on GLSRVDHCP01 exited with error code 0.
```

The parameters we specified on the `psexec` command are:

1. `@serverlist.txt` tells psexec which servernames to run on, as shown in Example 13-19 on page 831.
2. `-u cpcorp\dirsvc` specifies which administrative account to use.
3. `-p aar4nahtanoJ` specifies which password to use.
4. `-c` means to copy the batch file to the remote system for execution.
5. `install-director-on-servers-cmd` is the command we run on each server. This batch file in Example 13-20 on page 831 is the actual command we start on each server. This same command would also work if you logged on locally on each machine and typed it in from a command prompt. It starts the IBM Director Agent installation, unattended and silent, so no user interaction is required.

Request access to managed systems
As the systems start to report to IBM Director Server, they start showing up in the All Managed Objects group, all with a padlock on them. This is because of the SecureAgent option specified in the response files. The easiest way to request access to all of them is to sort them by IP address, click the top one, hold down the Shift key, and click the bottom one, then right-click and select **Request Access**, as shown in Figure 13-49.

![Figure 13-49   Request Access to multiple managed systems simultaneously](image)
When the padlock disappears, the system begins an automated inventory collection. When this inventory is complete, each system should be added to the proper dynamic group created earlier.

**Distribute System Availability**

For our managed server systems we want to take advantage of the functionality of the System Availability tool. This free add-in provides graphical summaries of system uptime and outages and can alert you to system outage patterns that might not be apparent without the tool. Note that system availability is supported only on IBM System x and BladeCenter server systems.

Installing the System Availability agent extension is a simple matter. The installer can be downloaded from the Web. Then the IBM Update Assistant wizard, part of Software Distribution, is used to create a Software Distribution package that can be pushed to our managed systems.

After the package is created, it is visible under the Software Distribution task. To start a distribution, drag the package onto the dynamic group Greenland Servers, as shown in Figure 13-50.
Because we prefer to have this installation take place after hours, we schedule the installation to take place later. To schedule this task, select **Schedule** in the dialog box that is displayed in Figure 13-51.

*Figure 13-51  Schedule or execute now*
We have chosen to start the deployment of this package at 11:00 PM, as seen in Figure 13-52. Note the message near the bottom of this window, indicating a difference between the time zones of the management server and the current console.

Figure 13-52  Schedule the package for future distribution
We choose our target systems by group. Under the Targets tab, select **Use a group as the target**, then select the **Greenland Group** object and click **Select**. The resulting window is shown in Figure 13-53.

![Figure 13-53 Schedule Targets](image-url)
There are several important options that can be configured for any scheduled job. For this particular distribution, we have specified several options, as shown in Figure 13-54.

**Figure 13-54  Scheduled job options**

Under Special Execution Options:

- **Delay execution on unavailable systems.**
  
  If a system is offline when the job begins execution, IBM Director holds the job open until that system is again available and will start the job then.

- **Execute in client time zone.**
  
  Because there is a significant time zone difference between the management server and the managed systems, selecting this option ensures that execution does not begin until 11:00 PM in Greenland.
Under Execution History check the “Limit execution status to the last 10 job executions” option. In our environment, there is no need to keep unlimited historical data on job execution, so we keep data on just the last 10 executions purely for troubleshooting.

Under Events, check these options:

- Generate an event when a job execution completes successfully.
- Generate an event when a job execution completes with errors.

It is a good idea to have IBM Director let us know whether the software distribution job succeeded, but we do not need to be notified for success or failure of each target system. Detailed information can be found in the job status window if any errors occur, as shown in Figure 13-55.

![Figure 13-55 The current status of a scheduled Software Distribution job](image)
Note in Figure 13-55 on page 839 that the scheduled Software Distribution job has a next schedule execution of 9/18/2005 at 5:00 AM. This is due to the time zone difference between the management server and the target systems. Running the job 9/18/2005 at 5:00 AM server time distributes the package on 9/17/2005 at 11:00 PM target system time, just as we specified.

There is no need to specify on an individual job basis whether the distribution should be streamed directly to the target systems or handled with a remote file distribution server. Since we have already specified a file distribution server for this particular dynamic group, the package will automatically be copied to the appropriate file distribution server before the installation takes place.

**Verify systems**

When we have managed to push the management agent out to all intended targets, it makes sense to verify that we have discovered and can manage all of these new systems. For more on how to verify that IBM Director is managing all systems in a given master list, see the scenario in “13.5, “Comparing system lists using a spreadsheet” on page 840.”

### 13.4.3 Extending this scenario

The possibilities for expanding this scenario beyond the specific features and functions discussed is limitless. In fact, during our residency, it was difficult to narrow the scope of this scenario because of the vast number of possibilities that exist.

The number and type of systems could be expanded. We used a relatively small number of systems running only three operating systems. Many of us work in a real-world environment where both of these parameters are far greater.

In addition, we covered in detail only the managed server side of the equation for a single location. Adding the workstations, as well as the other sites of the company to the discussion would greatly increase the opportunity for creative use of IBM Director. On the event action plan side alone, there are countless ways to implement event management policies, depending on technical, personnel, and political characteristics of your organization.

### 13.5 Comparing system lists using a spreadsheet

In a large IT environment, it is often useful to verify that all recently deployed systems have been discovered and are being managed appropriately by IBM Director. When rolling out tens or hundreds of systems, it is not uncommon for systems to be missed or misplaced. IBM Director Agent installation might be
overlooked, or a system might be renamed immediately after deployment, making it hard to find in the IBM Director Console.

In this scenario, we demonstrate a method that can be used to verify content inside an IBM Director management environment using a simple spreadsheet application. Given a master list from another source, we can easily compare that list with a list generated by IBM Director.

13.5.1 The problem

In a large IT environment, it can be a challenge to keep IBM Director up-to-date in terms of which systems it sees and manages. Are all systems labeled and monitored? Have any new systems been deployed in the network? Have any systems been renamed? Have any systems been reassigned or retired?

We can see a list of managed systems in IBM Director Console, but how do we know that this is a complete and accurate list? If the management console contains hundreds or thousands of systems, it can be virtually impossible to find a missing system. It is not easy to find something that is not there.

13.5.2 The solution

By configuring a spreadsheet to automatically compare a list of systems generated by IBM Director with a master list of systems we know should exist, it is quick and easy to find those systems that are unique to one list or the other. For our example we use Microsoft Excel®, but any spreadsheet with the appropriate compare function can be used to achieve these results.

We start with a master list. This list might come from the purchasing department or a shipping document that accompanied a group of new systems. It is a list that contains some unique identifier for those systems that are to be verified. For our example, we have a list of system names that have just been deployed. This list is updated as part of the deployment process for all new systems.

Because the default name displayed in IBM Director Console is that system’s computer name under Windows, it is a simple matter to compare the master list with a list generated from the IBM Director Inventory task.

Create the spreadsheet
Open a new spreadsheet document, setting it up as follows:

1. In Cell A1 type:
   "Master"
2. In Cell B1 type:
   IBM Director
3. In Cell C1 type:
   Not in IBM Director
4. In Cell D1 type:
   Not in Master
5. In Cell C2 type:
   =IF(COUNTIF(B:B, A2) = 0, A2,"")
6. In Cell D2 type:
   =IF(COUNTIF(A:A, B2) = 0, B2,"")
7. Copy Cells C2 and D2 downward for as many systems as you will likely encounter in either list.
8. Save the spreadsheet.

The formula entered in column C compares the contents in column A with the contents in column B. If they are different, the value in column A is copied to column C. If the cells are identical, the cell in column C is set to empty. This indicates that a system found in the master list does not appear in the list generated by IBM Director.

The formula entered in column D compares the contents in column A with the contents in column B. If they are different, the value in column B is copied to column D. If the cells are identical, the cell in column C is set to empty. This indicates that a system found in the list generated by IBM Director does not appear on the master list.
Our spreadsheet is shown in Figure 13-56. Note that we have stopped at nine rows of comparison to make the result easy to see.

![Figure 13-56 The compare spreadsheet](image)

**Figure 13-56** The compare spreadsheet
Paste the lists into the spreadsheet
To use the spreadsheet, paste the contents from the master list into column A. Our results are shown in Figure 13-57.

The list for column B comes from IBM Director. This can be achieved in a number of ways. You could open the Inventory task against all systems, then export the data as a CSV file and open it in Excel. Because all Inventory views include the system name in the left column, it does not matter which view we select for our example. Simply copy the system names from the exported file into the comparison spreadsheet.

You can also pull the desired data out of the IBM Director database using DIRCLI, as shown in Example 13-23.

Example 13-23 Using DIRCLI to list objects

C:\> DIRCLI lsmo -N "Greenland Servers"
GLSRVAD01
GLSRVDHCP01
GLSRVDNS01
GLSRVFS01
GLSRVMX01
GLSRVPRT01
The output from DIRCLI can easily be redirected to a file using the following syntax:

```
DIRCLI lsmo -N “Greenland Servers” > c:\serverlist.txt
```

Select and copy the list of systems from IBM Director to the clipboard. Then place the cursor in cell B2 and paste the list. Our resulting comparison spreadsheet is shown in Figure 13-58.

![Figure 13-58 Director list showing in column B](image)

It is now a simple matter to scan down columns C and D to quickly find systems that do not appear in both lists.

### 13.5.3 Extending this scenario

Using this method, you could also compare other information from a second source against data stored in the IBM Director database, such as system serial number or IP address. Any attribute stored in IBM Director Inventory could be compared against a second source of the same information for verification purposes.
For this technique to work, however, you must have consistent information between both data sources. That is, the master list must reflect information that is recorded in the IBM Director database.

For our example, we use system name, but this will not always work, especially in a mixed OS environment. Under Windows, the default IBM Director Console display name for each system is its Windows computer name, so this would likely be consistent with any master list reflecting computer names. Also, keep in mind that you must limit your IBM Director Inventory results to the systems in question. Be careful not to include data from physical platforms, SNMP devices, and so on when generating the IBM Director list for comparison.

### 13.6 Monitoring for prohibited applications

With users having access to the Internet, it is quite easy for undesirable applications such as peer-to-peer file sharing clients, instant messaging, and games to be introduced into the environment.

Many organizations have set policies as to what employees can and cannot do with company systems, but often these policies are rarely enforced.

IBM Director provides a simple method for monitoring for undesirable applications.

#### 13.6.1 The problem

Through policy management and user privileges it is possible to restrict what activities end users can perform, such as installing applications. For any number of reasons, a company might elect to provide full administrator permissions to end users, and this creates opportunity for applications to be installed without approval.

Additionally, many companies permit a certain flexibility in what users can install on their workstations. This is sometimes abused, with applications such as instant messaging and peer-to-peer file sharing being installed. This introduces undesirable issues, such as viruses, and can lead to legal implications for the company.

With IBM Director inventory functionality, it is easy to determine if any applications the organization has deemed inappropriate are present on company systems.
13.6.2 The solution

To discover any undesirable or prohibited applications that may be installed on your managed systems there are two prerequisites that must be met:

- The software inventory function must be enabled.
- The application must be in the software dictionary.

To enable the software inventory, in the IBM Director Console main menu click Options → Server Preferences. See Figure 13-59.

By default, only hardware data is collected for all agent levels. Click the drop-down for the IBM Director Agent (Level-2) and select All Available Data. This enables the software inventory collection on all IBM Director Agents.

**Note:** Inventory collection is only available for Level-1 and Level-2 managed systems.
Initiate or schedule an inventory so that software data can be collected.

IBM Director only displays program titles that match an entry in the software dictionary. If an application that you know is installed is not showing up in the software inventory, it is probably not in the dictionary, or the file parameters have changed. While this dictionary is quite extensive, newer applications might not be present, but can be added.

To edit the IBM Director Software Dictionary, click the down arrow next to the Inventory icon in the main menu, and select **Edit Software Dictionary** (see Figure 13-60).

*Figure 13-60  Inventory options from main menu icon*
When the Inventory Software Dictionary Editor is open, you can either search through the existing entries or add one (Figure 13-61).

![Inventory Software Dictionary Editor](image)

**Figure 13-61   Add Skype to the software dictionary**

To add an application, simply enter the details of the application in the Entry Description panel. Enter the name of the application and, optionally, any other information. If there are already values there, click File → New.

The software dictionary uses details of specific files to identify the application. Click Add to add a file to the list. In the Associated Files section you must specify at least one file, but you can include multiple files of any extension type. You can specify file names, file sizes, and file modification dates for the inventory criteria. Save the entry when you are finished.

When we run a software inventory collection, if Skype is installed, it will be recognized and listed in the software inventory results.
The next step is to create a dynamic group that will contain any systems that have Skype after an inventory collection. If Skype has already been discovered in an inventory collection, it will be an available option for creating this group. Create the group as follows:

1. In the main Console window, right-click in the **Groups** pane, and select **New Dynamic**. The Dynamic Group Editor window opens.

2. Expand **Software → Software → Program Title**. Scroll through the listing of known program titles and select the one you for which you want to monitor.

3. If Skype is not in the Program Title list (or there are no entries in the list), right-click **Program Titles** and click **Create Seed Value**. Enter the value Skype or whatever you entered as the title in Figure 13-61 on page 849.

4. Click **Add** to add the entry to the Selected Criteria column.
5. Click **File → Save As** and provide the group with a descriptive name such as **Systems with Skype** for this example.

If you have not done so already, initiate or schedule an inventory collection. When the software inventory has been collected, you can select the newly created group, which will show all the systems that have Skype installed.

![Figure 13-64  Skype group with showing systems with it installed](image)

### 13.6.3 Extending this scenario

There are a few things that you can do in addition to simply monitoring for the application to be present.

By using IBM Director Process Monitoring capabilities we could monitor for the installation of the application. Because Skype has a unique name for its installer (SetupSkype.exe) we could monitor for that process and create an alert based on that file name.

The only problem with this approach is that many applications use the generic setup.exe, so unless you want to monitor for any application installation, this might not be a feasible method.

Process monitoring can still be useful because applications have unique process names when they run.

In this example we monitor for Skype to run, and have multiple actions occur if that event occurs.

1. In the IBM Director Console Tasks pane, expand **Process Management**.
2. Right-click **Process Monitors** and select **Create**.

3. Enter the program name, the actual .exe process name in Task Manager, and check **Start** (Figure 13-65).

![Figure 13-65 Process monitor for skype.exe starting](image)

4. Click **File → Save As** and provide a descriptive name. Click **OK**.

5. Drag and drop the process task onto the systems or groups that you want to monitor.

**Note:** All systems in the group must support the task you are attempting to apply.

6. Click **Execute Now**.

7. To verify that the monitor is in effect, right-click the system or group and select **All Available Thresholds**. Figure 13-66 shows that the process monitor (PMON) for Skype (SKYPE.EXE) starting (START) is enabled on the single system Kananaskis.

![Figure 13-66 All available monitored thresholds showing process monitor](image)
Now that we are monitoring for Skype to start, we still need an EAP to make sure that something happens as a result of the Skype start event.

In the Event Action Plan Builder, we create an EAP that takes three actions on the start of this process:

1. Play a .wav file on the offending system.
2. Kill the offending application.
3. Send an e-mail to the administrator.

Follow these steps:


2. Create a customer filter. In the Event Filters pane, right-click and select Simple Event Filters → New.

3. Deselect Any, expand Director → Director Agent → Process Monitors → Processes Started, and check skype.exe.

![Figure 13-67  Simple filter for Skype starting](image-url)
If we had process monitors on other applications such as Kazaa, MSN IM, Solitaire, and so on, they would also be listed and we could include those applications in this EAP as well.

4. Click **File → Save As** and provide a descriptive name (Prohibited User App, for example).

5. Drag and drop this filter to our EAP.

6. Now we need to customize actions. First we create an action to play the .wav file on the system where the application launched.

7. In the Actions pane, right-click **Start a Program on the “event” System → Customize**.

8. For this example we use a small freeware application called Playwav to play the audio file, prohibitedapp.wav. Click **File → Save As** and provide a unique name.

![Figure 13-68](image)

*Figure 13-68   A customized action set to play an audio file when triggered*

9. The next action is to kill the offending application. IBM Director provides a utility called dakill.exe in the support directory of the IBM Director installation directory. For ease of use, we moved this to the C:\utils directory.
10. Following the same process we used to play the .wav file action, create an action to kill the offending application executable, as in Figure 13-69.

![Image of Customize Action: Kill Skype window]

**Figure 13-69** Action to execute the dakill command to stop the skype.exe process

11. Finally, we generate an e-mail to notify the administrator of this event.

12. If a generic e-mail action already exists, it can be reused easily. Using event-data-substitution variables allows you to create generic action plans that can be reused and still provide detailed event information.
13. To customize the e-mail action, right-click **Send an Internet (SMTP) E-mail → Customize**. Complete the configuration as appropriate (Figure 13-70).

14. We left the body of the e-mail empty because IBM Director by default will populate this body with the following information:
   - Event Text (&text)
   - Date (&date)
   - Severity (&severity)
   - Event Type (&type)
   - System name (&system)
   - Sender name (&sender)

![Figure 13-70  Generic e-mail alert configuration](image)

15. Click **File → Save As** and provide a descriptive name (Generic sysmon e-mail, for example).
16. Now we complete our EAP by dragging the actions we created and dropping them onto the Prohibited User App filter, as illustrated in Figure 13-71.

![Completed EAP for the prohibited application start](image1)

Figure 13-71  Completed EAP for the prohibited application start

Finally, we need to apply this EAP to the systems we are monitoring. In the IBM Director Console, drag and drop the EAP onto the system or group. In this example we applied this to the Systems with Windows XP group.

**Tip:** Make sure that the event action plans association is selected so that you can verify it. From the main menu click **Associations** and select **Event Action Plans**. See Figure 13-72.

![IBM Director Console](image2)

Figure 13-72  The Prohibited Application EAP applied to the whole group of XP systems

Now when someone launches that monitored application in that group, IBM Director will:

1. Play the .wav file.
2. Kill the application.
3. Send an e-mail to the administrator.
13.7 Monitoring for inventory changes

While prices have decreased on computer components such as memory and CPUs, the theft of these items from workplace desktop systems might still pose an issue. Not all systems have the capability of tamper detection devices to alert of a chassis intrusion, making them easy targets.

13.7.1 The problem

Despite best efforts, theft continues to be a problem. Systems can be deployed loaded up with memory, fast CPUs, and disks, only to have bits scavenged. Memory is reduced. CPUs are swapped for slower ones. Drives are swapped out, and so forth.

The new ability of IBM Director to compare current and previous inventory states enables you to monitor a change in any of the inventoried items.

By default, IBM Director only runs an inventory collection on a weekly basis. If the inventory is performed on Saturday night, and a change occurs on Monday morning, no event for that change will be generated until the following Saturday night on the next inventory collection.

13.7.2 The solution

For this scenario we monitor for a change in the installed memory configuration. The first thing we do is create an Inventory Monitor.

1. Right-click Inventory Monitors and select Create.
2. Enter a descriptive name for this monitor.
3. Expand the type of inventory you want to monitor (Hardware for this example).
4. Continue to drill down into the inventory tree until the specific items you want to monitor are visible.
5. Expand the items and select **Add**, **Change**, or **Remove**, and click **Add**.

For our example we monitor for a change in installed *memory*, as illustrated in Figure 13-73.

![Inventory Monitor: Memory change](image)

*Figure 13-73  New inventory monitor for change on installed memory*

**Tip:** Inventory monitors are separated with an OR statement, meaning that the first match generates the event, and the remaining items are not checked. If you want multiple items to be checked, you must create multiple monitors.

6. Click **OK**.

Now that we have the inventory monitor, we set up a Custom Inventory collection task. We do this for two reasons:

- So that we can run it at any time, and not have to wait for the default collection
- So we do not have to do a full collection, only on the monitored items

7. Right-click the **Custom Collection** task and select **Create**.
8. Similar to the Inventory Monitor, provide a name and select the corresponding items that we are monitoring (Figure 13-74).

![Custom Collection: CPU - Installed Memory](image)

*Figure 13-74  Custom inventory collection for Installed Memory*

We could have a post-collection action to generate an event on success or on errors, but for this example we do not.

9. Click **OK**. Under the Inventory task we now have additional collection and monitor tasks.

![New collection and monitor subtasks](image)

*Figure 13-75  New collection and monitor subtasks*

10. Drag and drop the custom inventory task just created onto the system or group to which you want this action to apply. This confirms that all systems
will provide the information, and ensure that the initial values are available for the monitor task to monitor.

11. When the collection is complete, right-click the system and select View Inventory.

12. Drill down to the items you want to monitor to make sure that the correct values are displayed.

13. Drag and drop the inventory monitors to the system or groups that you want to monitor. An Applied Inventory Monitors window opens, showing the systems that have applied inventory monitors, both existing and the new, as seen in Figure 13-76.

![Applied Inventory Monitors](image)

Figure 13-76   Applied Inventory Monitors

Now that the monitor is applied, we create an event action plan to send an alert if there are any changes. If all we do is monitor for the change, we might not learn about it for up to a week. We want to be notified immediately, so we create an additional EAP that performs the custom inventory collection when the agent comes online.


15. Next we create a simple filter for the IBM Director agent topology.online event. In the Event Filters pane, right-click = Simple Event Filters and select New.
16. In the Event Type tab (Figure 13-77) deselect Any, expand the **Director** item, then the **Topology** item, and check the **Online** box.

![Simple Event Filter Builder: New](image)

**Important:** There is a known bug with IBM Director 5.10 that if Agent<>Server encryption is enabled, then the `topology.online` event is not sent. This is scheduled to be fixed in 5.10.2. Until a fix is made available, you must disable this encryption by using Add/Remove Programs on the agent.

17. Click **File → Save As** and provide a name (Director Online in our example).
18. Drag and drop the Director Online filter to the EAP we created to associate the filter with the EAP.
19. Create an action that will perform the inventory collection. Right-click **Start a Task on the “event” System** and select **Customize**.
20. Click the Task field and scroll until you see the custom inventory task that you created. In our example it is `[Inventory][Custom Collections][Installed Memory].

![Customize Action: Mem Inv Collection]

*Figure 13-78 The Start a Task customization box with our custom collection task*

21. Click **File → Save As** and provide a name. We used Mem Inv. Collection for our example.

We still must create an EAP to action any change in the inventory results.

22. Create a new EAP called Inventory Change.
23. Create a new Simple Filter, deselect Any in the Event Type tab, expand **Director**, then **Inventory Monitor**, and check **Row Changed** (Figure 13-79).

![Simple Event Filter Builder: Inventory Change](image)

*Figure 13-79  Simple Event Filter for inventory changes*

24. Save it as Inventory Change.

25. Drag and drop the Inventory Change filter to the Inventory Change EAP.

The next step is to customize an action. We configure two actions that will alert us to the problem and provide a graphic indicator of the problem using a System Status icon in the management console.

First we customize the Create an Event Message to a Console User action to send a message to all users.

26. Right-click **Send an Event Message to a Console User → Customize.**
27. Configure the message according to your requirements. We used data-substitution variables in the message, and an asterisk (*) in the User(s) field, which will send the message to all IBM Director Console users. Our customization is seen in Figure 13-80.

![Figure 13-80 Event message to all console users]

28. Customize the Update the Status of the event System action, setting the status of the event system to **System Error (Generic Status)**, as shown in Figure 13-81.

![Figure 13-81 Action to set the System Status to error]

29. Finally, apply the two new customized actions to the Inventory Change filter in the EAP.
30. With all the EAPs complete, drag and drop them onto the managed system or groups that should be monitored for these changes.

Now when the target systems come online, they will trigger an inventory collection. If the new inventory collection detects changes in inventory data, a management console message will pop-up, as seen in Figure 13-82.

![Figure 13-82 Console event message for memory change](image)

In order to ensure that system administrators are made aware of this inventory change even after the Message Browser window closes, our EAP will also place a System Error icon next to each system with a changed inventory, as seen in Figure 13-83.

![Figure 13-83 System status icon for System Error now present](image)
13.7.3 Extending this scenario

The capabilities of EAPs and the EAP Builder are nearly limitless, bounded only by your experience and imagination. If you are plagued by an intermittent system failure that is not easily reproduced, IBM Director might be able to alert you immediately when the failure occurs. Better yet, it might be able to capture information leading up to the failure that could assist in troubleshooting the problem.

Many minor issues can be detected and corrected by IBM Director as well. As an example, you could configure an EAP that would detect the failure of a print spool service or daemon and restart the service or daemon automatically, before any users realized there was a problem. IBM Director could also alert you in the event that your antivirus software stopped running on a client system.

13.8 Data center planning using PowerExecutive

Planning for a new data center or introducing new hardware to an existing environment can be a challenging and costly process. Adequate provisioning for power and cooling are vital in the design and implementation stage to ensure smooth running of the data center.

13.8.1 The problem

Despite best efforts, provisioning systems for power and cooling accurately can be difficult, resulting in underestimating or over allocating data center resources.

Calculating power and cooling requirements based on nameplate values for systems can inhibit customers from installing new hardware or force customers into costly data center upgrades.

Note: The term nameplate power refers to the AC (input) power rating for the system. The difference in watts between the AC power and DC power (usable power) depends on the efficiency of the power supply.

13.8.2 The solution

Using PowerExecutive we can meter actual power usage and trend data for systems to efficiently plan and utilize available power for maximum application performance and data center resource allocation.
In this scenario we plan to provision power and cooling for 42 IBM System x3550 1U servers installed in a 42U rack running a common application.

**Provisioning new systems using nameplate values**

Provisioning new systems based on nameplate power ratings is relatively easy, but can result in over-provisioning of data center resources and increased costs. Table 13-1 provides information based on nameplate power information for a single x3550 server and also a fully populated rack of x3550 servers.

*Table 13-1 System x3550 nameplate power information*

<table>
<thead>
<tr>
<th>System x3550</th>
<th>Single server</th>
<th>42 servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nameplate Watts (AC)</td>
<td>670</td>
<td>28,140</td>
</tr>
<tr>
<td>BTU&lt;sup&gt;a&lt;/sup&gt; (heat output)</td>
<td>2,285</td>
<td>95,970</td>
</tr>
<tr>
<td>AC&lt;sup&gt;b&lt;/sup&gt; (Tonnage)</td>
<td>0.19</td>
<td>7.99</td>
</tr>
</tbody>
</table>

<sup>a</sup> BTU is a measurement of heat output from a device and can be calculated as AC wattage x 3.41 = BTU (where 3.41 is a constant).

<sup>b</sup> AC (Tonnage) is a measurement of the air conditioning capacity needed for cooling and can be calculated as BTU / 12,000 = AC tons to cool (where 12,000 is a constant).

**Provisioning new systems using PowerExecutive**

Provisioning new systems with PowerExecutive enables you measure actual power usage and trend data for systems. Using PowerExecutive requires more effort, but results of power consumption are much more accurate.
We used an IBM System x3550 server to run a simulated workload and stress tests on the system over a period of time. Based on workload we simulated on the server, we can view current power usage (Figure 13-84) or, more importantly, historical power usage in the Trend Data pane (Figure 13-85 on page 870).

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>12/14/06 12:14:54 PM</td>
</tr>
<tr>
<td>Name</td>
<td>Nitrogen</td>
</tr>
<tr>
<td>Power Meter</td>
<td>Version 2.1</td>
</tr>
<tr>
<td>Metering Level</td>
<td>Capping</td>
</tr>
<tr>
<td>Power Savings Supported by Platform</td>
<td>Yes</td>
</tr>
<tr>
<td>Nameplate Watts (ac)</td>
<td>670</td>
</tr>
<tr>
<td>Average Watts (ac)</td>
<td>223</td>
</tr>
<tr>
<td>Average Watts (dc)</td>
<td>180</td>
</tr>
<tr>
<td>Pcap (dc)</td>
<td>510</td>
</tr>
<tr>
<td>Pmax (dc)</td>
<td>510</td>
</tr>
<tr>
<td>Pmin (dc)</td>
<td>438</td>
</tr>
<tr>
<td>°C Ambient</td>
<td>25.0</td>
</tr>
<tr>
<td>°C Exhaust</td>
<td>36.0</td>
</tr>
<tr>
<td>Effective CPU Speed (%)</td>
<td>100.1</td>
</tr>
<tr>
<td>Last Policy</td>
<td>Console Applied</td>
</tr>
</tbody>
</table>

*Figure 13-84  PowerExecutive Current Data pane (point-in-time) power usage*
From PowerExecutive trend data we can view power usage over time, identify peak workloads, and use this data to accurately provision our data center resources.

**Important:** As workloads can differ between systems and application usage may grow over time, you should plan sufficient power resources for systems.
Table 13-2 indicates values observed while stress testing the x3550 server and running a simulated workload.

Table 13-2  System x3550 PowerExecutive workload testing

<table>
<thead>
<tr>
<th>System x3550</th>
<th>Single server (min)</th>
<th>Single server (max)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watts (ac)</td>
<td>~190</td>
<td>~380</td>
</tr>
<tr>
<td>BTU (heat output)</td>
<td>~648</td>
<td>~1296</td>
</tr>
<tr>
<td>AC (Tonnage)</td>
<td>~0.05</td>
<td>~0.11</td>
</tr>
</tbody>
</table>

We can also observe the minimum (Pmin) and maximum (Pmax) power capping levels for the x3550 server, as shown in Table 13-3. Pmin and Pmax values are indicated by solid black bars in the PowerExecutive trend data chart view or as values in the trend data tabular view.

Table 13-3  System x3550 PowerExecutive power capping information

<table>
<thead>
<tr>
<th>System x3550</th>
<th>Single server (Cap)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pmin Watts</td>
<td>438</td>
</tr>
<tr>
<td>Pmax Watts</td>
<td>510</td>
</tr>
</tbody>
</table>

**Note:** Pmin and Pmax are only available on systems that support power capping.

Pmin indicates the minimum power capping level we can apply, while Pmax indicates the maximum power capping level we can apply. Once we set a capping limit, the system cannot exceed the defined threshold. Any attempt to exceed the cap will result in CPU throttling (reduced performance).

Setting a power cap of Pmax is the maximum power the system can consume without CPU throttling or performance impact. Pmax allows maximum performance based on the hardware configuration of the system which is dynamically calculated by the server BMC or IBM BladeCenter management module.
Analyzing the results

By implementing PowerExecutive and simulating workloads we can allocate datacenter resources based on actual power consumption rather than nameplate power values. Using PowerExecutive to trend power usage over time shows that our simulated workload requires significantly less power than the nameplate value implies, as shown in Table 13-4.

Table 13-4  System x3550 power consumption

<table>
<thead>
<tr>
<th>System x3550</th>
<th>Single server (nameplate) max</th>
<th>42 servers (nameplate) max</th>
<th>Single server (PowerExec) measured max</th>
<th>42 servers (PowerExec) measured max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watts (ac)</td>
<td>670</td>
<td>28,140</td>
<td>380</td>
<td>15,960</td>
</tr>
<tr>
<td>BTU (heat output)</td>
<td>2,285</td>
<td>95,970</td>
<td>1,296</td>
<td>54,424</td>
</tr>
<tr>
<td>AC (Tonnage)</td>
<td>0.19</td>
<td>7.99</td>
<td>0.11</td>
<td>4.54</td>
</tr>
</tbody>
</table>

**Important:** As workloads can differ between systems and application usage may grow over time, you should plan sufficient power resources for systems.

To ensure that you do not under-provision power to systems, we recommend that you base values on Pmax if the systems support capping. Pmax allows for maximum system performance while still being significantly lower than the nameplate value (Table 13-5).

In cases where power is extremely limited you may decide to provision systems based on Pmin and set a cap to ensure that systems cannot go beyond the Pmin threshold.

For systems that do not support Pmax you should provision power based on the nameplate value.

Table 13-5  System x3550 power consumption (Pmax values)

<table>
<thead>
<tr>
<th>System x3550</th>
<th>Single server (nameplate) max</th>
<th>42 servers (nameplate) max</th>
<th>Single server (PowerExec) Pmax</th>
<th>42 servers (PowerExec) Pmax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Watts (ac)</td>
<td>670</td>
<td>28,140</td>
<td>510</td>
<td>21420</td>
</tr>
<tr>
<td>BTU (heat output)</td>
<td>2,285</td>
<td>95,970</td>
<td>1,739</td>
<td>73042</td>
</tr>
<tr>
<td></td>
<td>Single server (nameplate) max</td>
<td>42 servers (nameplate) max</td>
<td>Single server (PowerExec) Pmax</td>
<td>42 servers (PowerExec) Pmax</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------</td>
<td>---------------------------</td>
<td>-------------------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>AC (Tonnage)</td>
<td>0.19</td>
<td>7.99</td>
<td>0.14</td>
<td>6.07</td>
</tr>
<tr>
<td>System x3550</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
13.9 Provisioning test systems with z/VM complexes

The work involved to separately install and configure four test systems to support a production application environment is daunting. In a distributed server environment this can take weeks just to get the hardware installed, let alone the software and network configuration.

13.9.1 The problem

The existing production environment is four Linux servers on the company mainframe. They run an application that has not been meeting its service level requirements due to inadequate testing before moving new code into development.

It has been determined that four new systems must be deployed as a test bed. These four systems must be on the private test network, yet have network connectivity to the production systems. The production systems currently are only on the production network, so they will also need connectivity to the test systems. Testing on the test systems should not impact the resources available to the existing production systems.

13.9.2 The solution

The solution is:

1. Create two new z/VM networks and define them to the Complex.
2. Alter the properties of the production server complex.
3. Create a new server complex.
4. Provision four new systems.

Create two new z/VM networks and define them to the Complex

Do the following:

1. Define a new vswitch called VSWITCHT that the test systems will use to communicate with the test network. In our example, OSA devices 2CE0 - 2CE3 are available and are on the test network, so issue the command shown in Example 13-24 as MAINT.

*Example 13-24 Define vswitch*

```
def vswitch vswitcht rdev 2ce0
VSWITCH SYSTEM VSWITCHT is created
Ready; T=0.01/0.01 16:55:39
HCPSWU2830I VSWITCH SYSTEM VSWITCHT status is ready.
```
HCPSWU2830I VSWCTL1 is VSWITCH controller.

This vswitch will be used to allow the test systems to communicate with the test network.

2. Now define a new z/VM Guest LAN called TEST2PRD for the test systems to use to communicate with the production systems. Type the following command shown in Example 13-25 as MAINT.

```
Example 13-25   Define TEST2PRD

def lan test2prd type qdio
LAN MAINT TEST2PRD is created
Ready; T=0.01/0.01 16:58:54
```

This network will allow the test systems to push the tested code to the production systems.

3. In the server complexes task, define the properties for both networks so that they can be used. From the main Server Complexes window, click **Action** → **z/VM Networking Properties**.

4. In the window that opens, click **Action** → **Refresh from z/VM**.
   
This will add the two new networks so that their properties can be set in Server Complexes.

![Figure 13-86   New TEST2PRD LAN](image)

*Figure 13-86   New TEST2PRD LAN*
5. Double-click the **TEST2PRD** entry in the LAN tab to open its properties window.

![Connection Properties]

Figure 13-87   TEST2PRD properties
6. Define the IP addresses and range to be used on TEST2PRD.

We only need eight systems, four test and four production, so we limit the range to 8, and choose a base IP address of 10.0.0.2 with a netmask of 255.255.255.0. We do not really need a default gateway on this network, but the field is mandatory here and can be ignored later. IP addresses 10.0.0.2–10.0.0.9 will be used on this network. Click **OK**.

![New VSWITCH](image)

*Figure 13-88 New VSWITCHT*
7. Double-click the VSWITCHT entry in the VSWITCH tab to open its properties window.
8. Define the IP addresses and range to be used on VSWITCHT.

We only need four systems for the test group, but we expect this to grow in the future and are leaving room for more by choosing 15. We choose a base IP address of 192.168.15.2 with a netmask of 255.255.255.0. The default gateway is 192.168.15.1. Click OK.

![z/VM Networking Properties]

9. In the z/VM Networking Properties window, click **Action → Save**, then **Action → Exit**.
Alter the properties of the production server complex

Do the following steps:

1. In the Main Server Complexes window, select the existing server complex that contains the production systems and click **Action → Edit Properties** to open the properties window.

*Figure 13-91  Set the VMRM properties for the production SC*
2. Click the **VMRM** tab. Enter 35 for the CPU goal, and 10 for the importance. A CPU goal of 35 means that when these systems are ready to run, they get to run immediately 35% of the time. This may seem low, but setting the CPU goal too high will almost immediately set the relative share to 10000 for all systems in this group. An importance of 10 means that this work is important.

![nucleus Properties](image)

*Figure 13-92  Production server complex network properties*
3. Click the **Network** tab. Select the new **LAN TEST2PRD** network for interface #1, and do not change the default gateway. Click **OK**.

![Guest Selection](image1)

*Figure 13-93  Verify the network change*

4. Server complexes ask you to verify the change it is about to make. Click **Yes**.

**Attention:** Server complexes will restart the Linux systems as part of making the network configuration change. Do not use server complexes to make network changes to running systems without scheduling a maintenance window.

![Properties being changed](image2)

*Figure 13-94  Network properties are changed*
5. Once all of the systems have been restarted, click **Close**.

**Create a new server complex**

Now we need to create a new server complex for the test systems.

1. In the main Server Complexes task window, click the existing server complex that contains the production systems to highlight it. Then click **Action** → **Duplicate** to create a copy of it with the same set of preferences.

2. Enter a name for the test server complex. Click **OK**.
3. Click **Close** in the status window once the green check mark appears.

---

**Figure 13-96  New server complex shows in main SC window**
4. The new server complex now shows in the main server complexes window. Select it and click **Action → Edit Properties** to open its properties window.

5. Click the **VMRM** tab and set a CPU goal of 15 and an importance of 1.

   A CPU goal of 15 means that a test system will run immediately on the CPU 15% of the time when it is ready. An importance of 1 means that this work is not important.
6. Click the **Network** tab.

![testnc Properties window](image)

**Figure 13-98 Test SC Network properties**

7. Set interface #0 to use VSWITCH VSWITCHT, and change the default gateway to VSWITCHT's default gateway of 192.168.15.1.

8. Click **OK**. Then when the status window indicates that setting preferences is complete, click **Close**.

The test server complex is now ready to host new systems. The total time invested to do this setup work is less than 30 minutes.
Provision four new systems
To provision four new systems:

1. In the main server complexes window. Click Refresh to get the latest set of VS and OS templates.

2. Choose the VS template and Disk Pool, then drag and drop the desired OS template into the new test server complex.
3. Enter 4 clones, then click OK.

![Cloning progress window](image)

Figure 13-101 Cloning progress window

Server complexes then create the four new systems and provision them, then set their network and VMRM properties.

4. Click Close when the process indicates that it is complete.

The total amount of time to do the setup and clone four systems is less than an hour if a fast copy service is available in the storage subsystem.

### 13.9.3 Extending this scenario

The minidisk and scripts preferences also allow for powerful options:

- Install an application on a disk that can be shared as read-only among several servers. Add that disk to the minidisk list to be mounted read-only among every system in the server complex.

- Add a script to be run *On the Entering Guest* that will copy configuration data from the read-only disk and place it on a read-write space somewhere else. The application can then be started and pointed to the customized configuration that was generated by the script.

Not only does this provide drag-and-drop provisioning of operating systems, it also can provide customized and ready-to-run applications in the same action.
Event actions

This appendix lists the actions that are available for use in the Event Action Plan Builder, as described in Chapter 12, “Event management” on page 675.

In addition to the standard IBM Director event actions available for all installations of IBM Director, a number of special actions are added by the IBM Virtualization Manager extension. These are covered in “Virtualization Manager event actions” on page 920.
Event Action Plan Builder actions

The Event Action Plan Builder is shown in Figure A-1. Table A-1 lists the action descriptions.

**Table A-1** Summary of event actions

<table>
<thead>
<tr>
<th>Event actions</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/remove event system to static group</td>
<td>894</td>
<td>Adds a managed system to or removes a managed system from a specified static group when the managed system logs a specific event.</td>
</tr>
<tr>
<td>Event actions</td>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Add/remove source group members to a target static group.</td>
<td>895</td>
<td>Adds all managed systems in a source group to a target group or removes all specified managed systems from the target group.</td>
</tr>
<tr>
<td>Add a message to the console ticker tape.</td>
<td>896</td>
<td>Displays a message in red type that scrolls from right to left at the bottom of IBM Director Console.</td>
</tr>
<tr>
<td>Add to the event log.</td>
<td>897</td>
<td>Adds a description of the event to the event log.</td>
</tr>
<tr>
<td>Define a timed alarm to generate an event.</td>
<td>898</td>
<td>Generates an event only if IBM Director does not receive an associated event within the specified interval.</td>
</tr>
<tr>
<td>Define a timed alarm to start a program on the server.</td>
<td>899</td>
<td>Starts a program on the management server if IBM Director does not receive an associated event within the specified interval.</td>
</tr>
<tr>
<td>Log to textual log file.</td>
<td>900</td>
<td>Generates a text log file for the event that triggers this action.</td>
</tr>
<tr>
<td>Post to a newsgroup (NNTP).</td>
<td>901</td>
<td>Sends a message to a newsgroup using the NNTP protocol.</td>
</tr>
<tr>
<td>Resend modified event.</td>
<td>902</td>
<td>Creates or changes an event action that modifies and resends an original event.</td>
</tr>
<tr>
<td>Send an alphanumeric page (through TAP).</td>
<td>904</td>
<td>Sends a message to a pager using the Telocator Alphanumeric Protocol (TAP).</td>
</tr>
<tr>
<td>Send an event message to a console user.</td>
<td>905</td>
<td>Displays a pop-up message on the management console of one or more specified users.</td>
</tr>
<tr>
<td>Send an e-mail via SMTP.</td>
<td>906</td>
<td>Sends an e-mail message.</td>
</tr>
<tr>
<td>Send an SNMP inform to an IP Host.</td>
<td>907</td>
<td>Sends an SNMP inform request to a specified IP Host.</td>
</tr>
<tr>
<td>Send an SNMP trap to a NetView host.</td>
<td>908</td>
<td>Generates an SNMP trap and sends it to a specified NetView host using a TCP/IP connection to the host. If delivery of the SNMP trap fails, a message is posted in the history log of the managed system.</td>
</tr>
<tr>
<td>Send an SNMP trap to an IP host.</td>
<td>909</td>
<td>Generates an SNMP trap and sends it to a specified IP address or host name.</td>
</tr>
<tr>
<td>Send a numeric page.</td>
<td>910</td>
<td>Sends a numeric-only message to the specified pager.</td>
</tr>
<tr>
<td>Send a TEC Event to a TEC Server.</td>
<td>911</td>
<td>Sends a Tivoli Enterprise Console event to a TEC Server.</td>
</tr>
<tr>
<td>Set an event system variable.</td>
<td>912</td>
<td>Sets the managed system variable to a new value or resets the value of an existing system variable.</td>
</tr>
</tbody>
</table>
Add/Remove event system to static group

This option (Figure A-2) is used to add a system to a specified static group (or remove the system from the static group) when it logs a specified event.

<table>
<thead>
<tr>
<th>Event actions</th>
<th>Page</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start a program on a system.</td>
<td>914</td>
<td>Starts a program on any managed systems on which IBM Director Agent is installed.</td>
</tr>
<tr>
<td>Start a program on the event system.</td>
<td>915</td>
<td>Starts a program on the managed system that generated the event.</td>
</tr>
<tr>
<td>Start a program on the server.</td>
<td>916</td>
<td>In response to an event, starts a program on the management server that received the event.</td>
</tr>
<tr>
<td>Start a task on the event system</td>
<td>917</td>
<td>In response to an event, starts a non-interactive task on the managed system that generated the event.</td>
</tr>
<tr>
<td>Update the status of the event system.</td>
<td>918</td>
<td>When the selected resource status generates an event, the status of the managed system associated with the resource is set or cleared according to your specification.</td>
</tr>
</tbody>
</table>

Figure A-2  Add/remove event system to static group

Parameters

The parameters for add/remove event system to static group are:

- Target Group Name: Specifies the name of the static group to which the system is added or from which it is removed when a specified event occurs. If
you are adding the system to a group that does not already exist, then that group is created when the event occurs.

- **Add/Remove Option**: Choose one of the following options for adding or removing systems when an event occurs:
  - Add system to target group: Adds the system to the target group specified in the Target Group Name field.
  - Remove system from target group: Removes the system from the target group specified in the Target Group Name field.
  - Remove all systems from target group: Removes all systems from the target group specified in the Target Group Name field.

### Add/remove source group members to target static group

Use the dialog box shown in Figure A-3 to add all systems in a source group to a target group or to remove all specified systems from the target group.

![Figure A-3 Add/Remove source group members to target static group](image-url)
**Parameters**

The parameters for add/remove source group members are:

- **Source Group**: Specifies the name of the source group whose members are to be added or removed when a specified event occurs.

- **Target Static Group**: Specifies the name of the target group to which source group members are added. If the target group does not already exist, then that group is created when the specified event occurs.

- **Add/Remove Option**: Choose one of the following options for adding or removing systems when an event occurs:
  - Add source group members to target group: Adds all source group members to the target group specified in the Target Static Group field.
  - Remove source group members from target group: Removes all source group members from the target group specified in the Target Static Group field.
  - Remove all systems from target group: Removes all systems, regardless of group membership, from the target group specified in the Target Static Group field.

**Add a message to the console ticker tape**

When the event occurs, an informational message opens (Figure A-4 and Figure A-6 on page 898) and scrolls from right to left at the bottom of the IBM Director main console.

![Figure A-4 Add a Message to the Console Ticker Tape](image)
Parameters

The parameters for Add a Message to the Console Ticker Tape are:

- **Message**: the body of the message that will be displayed. Event-data-substitution variables supported.

- **User**: the ID of the users who will be able to see the message. Multiple IDs should be separated by a comma or a space. An asterisk (*) means anybody.

![IBM Director Console ticker tape](image)

Figure A-5  IBM Director Console ticker tape

Add to the Event Log

A description of an event will be added to the IBM Director event log.

**Note**: This should always be used to keep track of what happened on managed systems.
Define a Timed Alarm to Generate an Event

Use this dialog to define a timed event that is generated and sent only if IBM Director does not receive the associated event. The event must be received within the specified interval to reset the alarm timer.

![Figure A-6  Define a Timed Alarm to Generate an Event](image)

If the event type defined by this event action is correlated with another instance of this same action (Define a Timed Alarm to Generate an Event) in an event action plan, when IBM Director receives an event that matches the event type, the timed alarm defined in the action is triggered.

Parameters

The parameters are:

- **Timed Alarm ID**: Enter the ID of the timed alarm. You can use event data substitution to include text of the event that generates this action.
- **Time until Alarm Triggers**: Enter the interval, in seconds, during which the event associated with this action must be received to avoid triggering this
action. If the associated event is received within the specified interval, this action is not triggered and the timer is reset to begin countdown again.

- Event Text: Enter the event text you want to associate with this action. You can use event data substitution to include the text of the event that generates this action.

- Alarm Event Subtype: Enter a user-defined subtype. When you save this action, the event type is defined to the IBM Director as Director.Alarm Triggered, and the text subtype entered in this field specifies the subtype portion of Director.Alarm Triggered.subtype. When the IBM Director server becomes aware of this event type, you can select it when creating an event filter.

- Problem Severity: Select either to keep the severity assigned to the event that triggers this action (Use Event Severity) or to choose another severity level from the pull-down list.

Define a Timed Alarm to Start a Program on the Server

Use this dialog to define or reset a timed alarm for executing a program on the IBM Director Server.

![Customize Action: Define a Timed Alarm to Start a Program on the Server](image)

Figure A-7 Define a Timed Alarm to Start a Program on the Server
Parameters

The parameters are:

- **Timed Alarm ID**: specifies the ID of the timed alarm. You can use event data substitution to include text of the event that generates this action.
- **Time until Alarm Triggers**: specifies the interval, in seconds, during which the event associated with this action must be received to avoid triggering this action. If the associated event is received within the specified interval, this action is not triggered and the timer is reset to begin countdown again.
- **Command Line**: specifies the command to execute if the Time until Alarm Triggers interval elapses without being reset.
- **Working Directory**: specifies the directory on the IBM Director server in which to execute the command.

Log to a Textual Log File

Use this dialog to log in a textual log file the event data that triggers this action. All fields are logged, including the event details.

*Figure A-8  Log to a Textual Log File*
Parameters

The parameters are:

- Log File Name: specifies the path and name of the log file. The log is formatted as a plain text file and located on the IBM Director Server. No default location is used. You must specify a file path.
- Maximum Log Size: specifies the maximum size of the log file in kilobytes.
- Log Comment Field: displays comments that you want to include in the log entry.

Post to a News Group (NNTP)

An information message will be sent to a newsgroup using the NNTP protocol.

This action may be useful as an additional logging mechanism outside of IBM Director.

Figure A-9   Post to a News Group
Parameters

The parameters are:

- **News Group**: fully qualified name of the destination newsgroup.
- **Reply-to-address**: e-mail address of the administrator who has set this action.
- **News Host**: news server name (for example, news.server.com).
- **Port**: port number to be used for NNTP protocol (default is 119).
- **Subject**: subject of the message. Event-data-substitution variables supported.
- **Body of News Posting**: some text you want to be added with the description of the event. Event-data-substitution variables are supported.

Resend Modified Event

This is used to create or change an event action that modifies and resends an original event.

![Customize Action: Resend Modified Event](image)

*Figure A-10  Resend Modified Event*

Parameters

The parameters are:

- **New Event Text**: displays the new event text. You can use event data substitution in the text to include the attributes of the event associated with this action.
► New Event Severity: Select to either keep the severity assigned to the event that triggers this action (Use Event Severity) or choose another severity level from the pull-down list.

► Detail Slot Settings: Use this field to enter a slot ID and its value. To specify multiple slot IDs and values, separate each entry with a space.

For example, by default an IBM Director Agent Topology Offline event has a severity of harmless. If you have created a simple EAP to handle critical events and would like Topology Offline to be treated as such, you could use this to change the severity of this particular event in the New Severity section.

We would use IBM Director Agent Topology Offline filter, then have the resend modified event action resend the event, but change the severity to critical.

![Diagram](image.png)

*Figure A-11  EAP to change IBM Director Agent offline to critical severity*

Now the critical event filter will catch the event and perform the prescribed action.
Send an Alphanumeric Page (via TAP)

Send a message on a pager. This one must comply with the Telocator Alphanumeric Protocol (TAP).

![Figure A-12  Send an Alphanumeric Page](image)

Parameters

The parameters are:

- Serial Port Device Name: the COM port on which the modem is connected.
- Paging Network’s Access Number: the number to dial with the modem (35 digits maximum).
- Pager ID or PIN: a number (usually seven digits) identifying the person we want to page.
- Message to send: the message itself we want the person to be informed of.
- Modem Initialization string: Here we can enter some AT commands to configure the modem.

**Note:** A typical mistake involves using the wrong phone number. Nearly all paging systems have one phone number for computers to dial and another number for humans to dial.
Send an Event Message to a Console User

A pop-up message will appear on the console of a specified user.

Figure A-13  Send an Event Message to a Console User

Parameters

The parameters are:

- **Message**: the body of the information message we want to send. Event-data-substitution variables supported
- **User**: the name of one or more IBM Director users who we want to be informed of the message
- **Delivery criteria**: whether to send the message just to those management console users that are logged on right now, or to all users. (Those who are not logged on now will get the messages the next time they are logged on.)

**Note**: Use commas or a space to separate several entries in the user field. Use an asterisk (*) to warn anyone who is connected.
Send an Internet (SMTP) E-mail

The description of the event will be sent via e-mail.
This can be used to send a typical e-mail or to send a message to an e-mail enabled phone. Consider the use of an outside SMTP provider if you are concerned about availability of the internal mail server.

Parameters

The parameters are:

- Internet E-mail address: the address where we send the e-mail.
- Reply-To: the name of the administrator who has set this action.
- SMTP E-mail server: name of the SMTP server (name or IP).
- SMTP Port: port number where the SMTP daemon runs on the e-mail server (default 25).
- Subject of E-mail message: the subject line. Event-data-substitution variables supported.
- Body of E-mail Message: the message that will be added to the description of the event. Event-data-substitution variables supported.

**Tip:** Use of data substitution variables makes the reuse of a single action easy, while providing very specific event details.

Send an SNMP Inform to an IP Host

This sends an SNMP inform request to a specified IP host. SNMP traps do not require an acknowledgement of receipt from the manager, making them somewhat unreliable. Informs, however, do require a response from the manager. If an inform is sent and no response is received, it can send another inform, making them more reliable than simple traps.

![Customize Action: Send an SNMP Inform to an IP Host](image)

*Figure A-16  Send an SNMP Inform to an IP Host*
Send an SNMP Trap to a NetView Host

This is used to generate an SNMP trap and send it to a specified NetView host using a TCP/IP connection to the host. If delivery of the SNMP trap fails, a message is posted in the system's history log.

Figure A-17 Send an SNMP Trap to a NetView Host

Parameters

The parameters are:

- **Destination IP Address or Hostname**: specifies the IP address or host name of the NetView host to which you want to send an SNMP trap when an associated event occurs. Enter either an IP address in dotted decimal format or a host name. To enter multiple locations (addresses and host names), use a comma or a space to separate the destinations.

- **Community Name**: specifies the community name used by the destination host. The default value is public, indicating that the target host is using a public community name.
Send an SNMP Trap to an IP Host

An SNMP trap will be generated and sent to the specified host.

![Figure A-18  Send an SNMP Trap to an IP Host](image)

**Parameters**

The parameters are:

- Destination IP Address or Hostname: name or IP address of the SNMP manager or gateway
- Community Name: name of the SNMP community
- SNMP Trap Version: SNMPv1 or SNMPv2c
Send a Numeric Page

A numeric-only message will be sent to the specified pager. This action requires a modem to be attached to the IBM Director Server.

Figure A-19  Send a Numeric Page

Parameters

The parameters are:

- Serial Port Device Name: the COM port where the modem is connected
- Pager Number: the number to dial with the modem
- Numerical Message: the numbers that represent the message
- Modem Initialization String: a set of AT commands that will override the default string
Appendix A. Event actions

Send a TEC Event to a TEC Server

This action can be used to send Tivoli Enterprise Console events to a TEC server.

![Image: Customize Action: Send a TEC Event to a TEC Server]

**Parameters**

The parameters are:

- **Server Location**: the Tivoli Enterprise Console that will receive the events.
- **Server Port**: the port used to communicate with the TEC server (default 5529).
- **Event Caching**: Enable or disable event caching in case the TEC server cannot be reached.
- **Configuration Parameters**: additional parameters that can be sent with the event.
Set an Event System Variable

IBM Director provides user-defined system variables to help you test and track the status of network resources according to the needs of your organization. System variable names and values can be referenced wherever event data substitution is allowed.

For example, assume that you need to monitor a bottleneck in the network that can cause network congestion. You can create an event action plan to specify an SNMP event that indicates network congestion, and initiate the Set Event System Variable task when the event occurs. Assume that you have specified:

- NetStatus in the Variable Name field
- Congested in the New Value field
- Normal in the Value to Reset to if Server is Restarted field
- 10 in the Time until Automatic Value Reset field

If 10 seconds elapse before the IBM Director server receives the event that triggers this action or before the IBM Director server stops and restarts, the NetStatus system variable is reset to normal.
Instead of using a specific event that signals that your NetStatus is normal, you have used a system variable that automatically resets to normal when the events that cause this action to trigger are not received within the interval. If the IBM Director server continues to receive the events before the interval expires, this action continues to trigger, signaling that the network is congested. If the timer interval expires, NetStatus is reset to normal.

**Figure A-21  Set an Event System Variable**

**Parameters**

The parameters are:

- **Variable Name**: Enter the name of the system variable.

- **New Value**: Enter the value assigned to the system variable when this action is initiated.

- **Value to Reset to if Server is Reaunched (optional)**: Enter the value the system variable should be set to if the interval specified in Time until Automatic Value Reset expires or if the IBM Director server is restarted. If you do not specify a value, the value resets to null (no value).

- **Time until Automatic Value Reset**: Enter the interval, in seconds, that is to elapse before the system variable’s value is reset. The interval begins when this action is initiated (when the value is reset).
Start a Program on a System

As a response to an event, a program will be launched on any system with the IBM Director Agent installed. This includes command-line operations.

Parameters

The parameters are:

- **System Address**: network address of the system on which the program will be launched. The rule for addressing is:
  
  `transport_protocol::address`

- **Program Specification**: name of the program to launch.

- **Working Directory**: If necessary, specify the directory the application will use.

- **Valid transport protocols** are TCP/IP, IPX, and NetBIOS.

Examples

- TCPIP::192.168.128.110
- TCPIP::jk1-srv.raleigh.ibm.com
- IPX::A1:1234567890AB
- NETBIOS::CLARK
Start a program on the event system

A program will be launched on the system where the event has occurred. This includes command-line operations that can start or stop programs on the event systems.

Parameters

The parameters are:

- Program specification: name of the program to launch.
- Working Directory: If necessary, specify the directory the application will use.

An example of this is the use of the dakill.exe that is provided with IBM Director, located in the support directory. We can use this to kill processes by simply passing the process name.

In Figure A-23 we have configured this action to start dakill.exe (relocated to c:\utils) and to kill skype.exe.

When this action is combined with a process monitor configured to generate an event when skype.exe starts, it will kill the skype.exe process on that system.

Figure A-23   Start a program on the event system
Start a Program on the Server

A program will be launched on the IBM Director server (the one that gets the event). This includes command-line operations that can start or stop programs on the event systems.

![Image of Customize Action: Start a Program on the Server]

**Parameters**

The parameters are:

- Program specification: name of the program to launch.
- Working Directory: If necessary, specify the directory the application will use.

For example, if your IBM Director Server is configured with an audio card, you could have it launch an audio player and play a specified file to alert you to an event.
Start a Task on the “event” System

An IBM Director non-interactive task will be performed on the system that has generated the event. Non-interactive tasks are tasks that do not require user input. All tasks created in the process task will appear here.

![Customize Action: Start a Task on the “event” System](image)

*Figure A-25   Start a Task on the “event” System*

Parameters

The parameter is: Task: designation of the task to launch. The list of non-interactive tasks is dynamic and is constructed when you create the customized action. Once you save the action, the list is frozen. Only creating a new customized action will refresh the list.

Non-interactive tasks are tasks that do not require user input and may be added at any time. New tasks can be created via the customized Inventory Tasks, Process Management Process Tasks or a Software Distribution.

An example of this could be used in monitoring for a change in CPU and memory configurations.

The system would have to go offline to perform a change on these components. We could have an EAP that has an action of a custom inventory collection task preformed on those components (CPU and memory) when the agent comes online.

By having an inventory monitor on those components, any change since the last inventory could generate and event, and thus an alert.

**Tip:** The task you want to use must be in the Tasks pane in IBM Director Console before it becomes an available task for this action.

We discuss the use of this in a scenario. See 13.7, “Monitoring for inventory changes” on page 858.
Update the Status of the “event” System

Use this dialog to select the type of resource status that is to be set or cleared. When the selected resource status generates an event, the status of the system associated with the resource is set or cleared according to your selection.

The status is displayed as an icon next to the managed object in the IBM Director Console. This can be used to visually alert to events that have occurred.

For example, if we had established a resource monitor for available disk space, and the warning threshold was passed, part of the EAP could set the system status to Disk Warning, as in Figure A-26. The system with Disk Warning status set is shown in Figure A-27 on page 919.

The status icons can be cleared from either with another event to clear the status, or right-click the managed system Set Status at the bottom of the menu and deselect where applicable.

![Figure A-26](image.png)  Update the Status of the “event” System

Parameters

The parameters are:

- Status to be set: used to select the association of the status that you want to change. There is an information, warning, and error status for the following items:
  - Application
  - Disk
  - Network
  - Operating system
Action: Set the status to be set or cleared.

Figure A-27  System with a disk warning status
Virtualization Manager event actions

IBM Virtualization Manager adds several event action templates to IBM Director Event Action Plan Builder. Virtualization Manager event actions are easily identified by the Virtualization Manager icon they use ( ), as highlighted in Figure A-28. To use these templates, from the Event Action Plan Builder window, right-click the template name and select Customize to create a custom event action.

![Event Action Plan Builder showing event actions added by Virtualization Manager](image)

*Figure A-28  Event Action Plan Builder showing event actions added by Virtualization Manager*
Add a Host to a Virtual Farm

This is used to add a host to a farm by specifying the name or IP address of the host to be added and the farm name.

![Add a Host to a Virtual Farm](image)

Figure A-29  Add a Host to a Virtual Farm

Parameters

The parameters are:

- **Host**: designates the IP address or the name of the host that is to be added to the virtual farm

  **Note**: Before you type a host name, make sure that the network environment is able to determine the IP address from the host name. Otherwise, the operation to add a host will fail. If you cannot determine the IP address of a host by using the `ping` command, type the IP address instead of the host name.

- **Virtual Farm**: identifies the virtual farm to which the host is added
Add a Host to VirtualCenter

Used to add a host to VMware VirtualCenter by specifying the name or IP address of the host to be added, as well as login credentials (user ID and password) and port number for communicating with the VirtualCenter Server.

![Image of Add a Host to VirtualCenter]

**Parameters**

The parameters are:

- **Host**: designates the IP address or the name of the host that is to be added to the virtual farm that is defined in VMware VirtualCenter.

  **Note**: Before you type a host name, make sure that the network environment is able to determine the IP address from the host name. Otherwise, the operation to add a host will fail. If you cannot determine the IP address of a host by using the `ping` command, type the IP address instead of the host name.

- **User ID**: designates the user name for the administrator of the system. Generally, this is `root` for hosts that are running VMware ESX Server. This user name is used by the VMware VirtualCenter server to communicate with the host that is running the VMware ESX Server or the VMware GSX Server.
Appendix A. Event actions

- Password: designates the password for the user name that you used.
- Port: designates the address of the port that VMware VirtualCenter server will use for communication with VMware ESX Server. By default, virtual uses port 902 for this communication. If the system that is running VMware ESX Server is configured to use a port address other than 902, type that port address in this field. Hosts that are running the VMware GSX Server do not use the port number.
- VirtualCenter Farm: identifies the farm in VMware VirtualCenter to which the host is added.

Manage a Host

This is used to perform power management actions on virtual hosts by specifying the name or IP address of the virtual host to be managed and the action to be performed.

![Customize Action: Manage a Host](image)

*Figure A-31  Manage a Host*

Parameters

The parameters are:
- Host: identifies the host that you want to manage.
- Action: identifies the function that you want to perform on the host. The supported actions are:
  - Start (Microsoft Virtual Server only): starts Microsoft Virtual Server services on the host. You can use this event action only for hosts that are currently stopped.
– Stop (Microsoft Virtual Server only): stops Microsoft Virtual Server services on the host. You can use this event action only for hosts that are currently started.

– Power off all virtual servers: turns off all running virtual servers that are associated with a single host without an orderly shutdown of any guest operating systems.

– Power on all virtual servers: turns on all stopped virtual servers that are associated with a single host.

– Resume all virtual servers: resumes all suspended virtual servers that are associated with a single host.

– Suspend all virtual servers: suspends all running virtual servers that are associated with a single host.

Manage a Virtual Server

This is used to perform power management actions on virtual servers by specifying the name or IP address of the virtual server to be managed and the action to be performed.

![Customize Action: Manage a Virtual Server](image)

Figure A-32   Manage a Virtual Server

Parameters

The parameters are:

– Virtual Server: identifies the virtual server that you want to manage.

– Action: identifies the function that you want to perform on the virtual server.

  The supported actions are:

  – Power on: The virtual server is turned on.
– Shut down and power off (Microsoft Virtual Server only): If the guest operating system is a Windows operating system and if Microsoft Virtual Server Additions is installed on the guest operating system, action performs an orderly shutdown of the guest operating system and then turns off the virtual server.

– Power off now: The virtual server is turned off without an orderly shutdown of its guest operating system. This will immediately stop all applications that are in use on that guest operating system.

– Suspend: The virtual server remains turned on, but is suspended from use.

– Resume: The virtual server resumes operation and is no longer suspended.

– Restart now: The virtual server is restarted immediately, which means that it is restarted without an orderly shut down of its guest operating system. This will immediately stop all applications that are in use on that guest operating system.

### Remove a Host from a Virtual Farm

This is used to remove a host from a virtual farm by specifying the name or IP address of the host to be removed and the farm name.

![Figure A-33   Remove a Host from a Virtual Farm](image)

**Parameters**

The parameters are:

- Virtual Farm: identifies the virtual farm from which you want to remove a host.
Host: identifies the host to remove from the virtual farm.

When you customize an event action to remove a host from a virtual farm in VMware VirtualCenter and then test this customized event action, IBM Director displays the following error message:

Error communicating with server. If the problem persists, you may need to restart the server.

You can ignore this message. It is displayed when a test action takes longer than 15 seconds to complete. Additionally, you do not need to restart the server.

Instead, check the event log and IBM Director Console to confirm that the test action was performed as expected.

To permanently prevent this error message from occurring, increase the network time-out value for IBM Director:

- Windows: Run `twgipccf.exe`.
- Linux: Using an ASCII text editor, open the `ServiceNodeLocal.properties` file (located in the `/opt/IBM/director/data` directory) and modify the value of `ipc.timeouts`.

By default, the network time-out value is set to 15 seconds.

Stop and restart IBM Director Server to ensure that the new time-out value takes effect. To do so, enter the following commands from the management server:

```
net stop twgipc
net start twgipc
```

**Important:** Increasing the network time out can have performance implications. You should reset the time-out value to the default 15 seconds after testing this action.

---

**Migration tasks**

In addition to the event actions listed above and easily identified in the Event Action Plan Builder window, the migration tasks that you create with Virtualization Manager are also available in the Event Action Plan Builder window, under the **Start a Task on the “event” System** event action template.

Complete the following steps to access the saved migration tasks under this event action template:

2. In the Actions pane, double-click the **Start a Task on the “event” System**
event action. The Customize Action window opens.

The list on the Customize Action window contains several noninteractive IBM
Director tasks that can be performed on the system for which the event is
generated. Any saved migration tasks are in the following formats:

[Migrate All Virtual Server Tasks][Virtualization
Manager][saved_task][Execute]
[Migrate Single Virtual Server Tasks][Virtualization
Manager][saved_task][Execute]

saved_task is the name of the saved migration task.

3. Select the desired migration task from the drop-down list, as shown in
Figure A-34.

![Customize Action window with virtual server migration task selected](image)

*Figure A-34  Customize Action window with virtual server migration task selected*
4. Select **File → Save As**, give the event action a name, and click **OK** to save it. The new event action now shows up in the *Start a Task on the “event” System* event action template, as shown in the highlighted box in Figure A-35.

![Customized event action to migrate a virtual server](image-url)
CIM subscriptions

This appendix lists the CIM handlers, filters, and subscriptions that are predefined in IBM Director Agent. The use of these with the cimsubscribe command are discussed in 5.5, “Using cimsubscribe to process local events” on page 254.

There are three tables in this appendix:

- “Predefined CIM handlers” on page 930
- “Predefined CIM filters” on page 930
- “Predefined CIM subscriptions” on page 935
Predefined CIM handlers

Table B-1 lists the handlers (actions) that are predefined when IBM Director Agent is installed.

Table B-1  Predefined CIM handlers

<table>
<thead>
<tr>
<th>Handler name</th>
<th>Handler destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health</td>
<td><a href="http://localhost:6988/CIMListener/HealthConsumer">http://localhost:6988/CIMListener/HealthConsumer</a></td>
</tr>
<tr>
<td>Log</td>
<td><a href="http://localhost:6988/CIMListener/LogConsumer">http://localhost:6988/CIMListener/LogConsumer</a></td>
</tr>
<tr>
<td>PopUp</td>
<td><a href="http://localhost:6988/CIMListener/PopupConsumer">http://localhost:6988/CIMListener/PopupConsumer</a></td>
</tr>
<tr>
<td>SMS</td>
<td><a href="http://localhost:6988/CIMListener/SMSConsumer">http://localhost:6988/CIMListener/SMSConsumer</a></td>
</tr>
<tr>
<td>SNMP</td>
<td><a href="http://localhost:6988/CIMListener/SnmpConsumer">http://localhost:6988/CIMListener/SnmpConsumer</a></td>
</tr>
<tr>
<td>TEC</td>
<td><a href="http://localhost:6988/CIMListener/TivoliConsumer">http://localhost:6988/CIMListener/TivoliConsumer</a></td>
</tr>
<tr>
<td>2f7c756f26b00121 (See note)</td>
<td><a href="http://localhost:6988/CIMListener/DirectorConsumer/192.168.128.51">http://localhost:6988/CIMListener/DirectorConsumer/192.168.128.51</a></td>
</tr>
<tr>
<td>7f6e6daa36b2e3e5 (See note)</td>
<td><a href="http://localhost:6988/CIMListener/DirectorConsumer/9.42.171.174">http://localhost:6988/CIMListener/DirectorConsumer/9.42.171.174</a></td>
</tr>
</tbody>
</table>

Note: The last two handlers are created when a management server first discovers a managed system. One handler is created for each IBM Director Server that contacts the agent. The handler name is the unique ID (UID) of the IBM Director Server and will vary from installation to installation. ipaddress in the handler destination is the IP address of that particular IBM Director Server system. See 5.5.5, “Subscriptions to IBM Director Server” on page 264, for more information.

Predefined CIM filters

Table B-2 on page 931 lists all of the filters defined by default. All filters are of the following form:

SELECT * from cim_indication where PerceivedSeverity = sev

Where cim_indication and sev are listed in Table B-2 on page 931. When you list all filters using the cimsubscribe -lf command, each filter is displayed as shown in Example B-1 (using the first one as an example).

Example: B-1  Portion of output from the cimsubscribe -lf command

CIM_IndicationFilter.CreationClassName="CIM_IndicationFilter",Name="ASR Criticals",SystemCreationClassName="CIM_ComputerSystem",SystemName="fs2-vm-xp"
Caption =
CreationClassName = CIM_IndicationFilter
Description =
**Table B-2  Predefined CIM filters**

<table>
<thead>
<tr>
<th>CIM filter name</th>
<th>CIM indication</th>
<th>Sev</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR Criticals</td>
<td>IBMx_AutomaticServerRestartEvent</td>
<td>6</td>
</tr>
<tr>
<td>ASR Normals</td>
<td>IBMx_AutomaticServerRestartEvent</td>
<td>2</td>
</tr>
<tr>
<td>ASR Warnings</td>
<td>IBMx_AutomaticServerRestartEvent</td>
<td>4</td>
</tr>
<tr>
<td>Chassis Criticals</td>
<td>IBMPSG_ChassisEvent</td>
<td>6</td>
</tr>
<tr>
<td>Chassis Normals</td>
<td>IBMPSG_ChassisEvent</td>
<td>2</td>
</tr>
<tr>
<td>Chassis Warnings</td>
<td>IBMPSG_ChassisEvent</td>
<td>4</td>
</tr>
<tr>
<td>IPMI Log Criticals</td>
<td>IBM_MgmtHwLogStatus</td>
<td>6</td>
</tr>
<tr>
<td>IPMI Log Normals</td>
<td>IBM_MgmtHwLogStatus</td>
<td>2</td>
</tr>
<tr>
<td>IPMI Log Warnings</td>
<td>IBM_MgmtHwLogStatus</td>
<td>4</td>
</tr>
<tr>
<td>Lease Criticals</td>
<td>IBMPSG_LeaseExpirationEvent</td>
<td>6</td>
</tr>
<tr>
<td>Lease Normals</td>
<td>IBMPSG_LeaseExpirationEvent</td>
<td>2</td>
</tr>
<tr>
<td>Lease Warnings</td>
<td>IBMPSG_LeaseExpirationEvent</td>
<td>4</td>
</tr>
<tr>
<td>Memory PFA Criticals</td>
<td>IBMPSG_MemoryPFEvent</td>
<td>6</td>
</tr>
<tr>
<td>Memory PFA Normals</td>
<td>IBMPSG_MemoryPFEvent</td>
<td>2</td>
</tr>
<tr>
<td>Memory PFA Warnings</td>
<td>IBMPSG_MemoryPFEvent</td>
<td>4</td>
</tr>
<tr>
<td>Network Adapter Criticals</td>
<td>IBMPSG_NetworkAdapterFailedEvent</td>
<td>6</td>
</tr>
<tr>
<td>Network Adapter Normals</td>
<td>IBMPSG_NetworkAdapterFailedEvent</td>
<td>2</td>
</tr>
<tr>
<td>Network Adapter Offline Criticals</td>
<td>IBMPSG_NetworkAdapterOfflineEvent</td>
<td>6</td>
</tr>
<tr>
<td>Network Adapter Offline Normals</td>
<td>IBMPSG_NetworkAdapterOfflineEvent</td>
<td>2</td>
</tr>
<tr>
<td>Network Adapter Offline Warnings</td>
<td>IBMPSG_NetworkAdapterOfflineEvent</td>
<td>4</td>
</tr>
<tr>
<td>Network Adapter Online Criticals</td>
<td>IBMPSG_NetworkAdapterOnlineEvent</td>
<td>6</td>
</tr>
<tr>
<td>CIM filter name</td>
<td>CIM indication</td>
<td>Sev</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Network Adapter Online Normals</td>
<td>IBMPSG_NetworkAdapterOnlineEvent</td>
<td>2</td>
</tr>
<tr>
<td>Network Adapter Online Warnings</td>
<td>IBMPSG_NetworkAdapterOnlineEvent</td>
<td>4</td>
</tr>
<tr>
<td>Network Adapter Warnings</td>
<td>IBMPSG_NetworkAdapterFailedEvent</td>
<td>4</td>
</tr>
<tr>
<td>POST Memory Criticals</td>
<td>IBMx_PhysicalMemoryEvent</td>
<td>6</td>
</tr>
<tr>
<td>POST Memory Normals</td>
<td>IBMx_PhysicalMemoryEvent</td>
<td>2</td>
</tr>
<tr>
<td>POST Memory Warnings</td>
<td>IBMx_PhysicalMemoryEvent</td>
<td>4</td>
</tr>
<tr>
<td>POST Processor Criticals</td>
<td>IBMx_ProcessorEvent</td>
<td>6</td>
</tr>
<tr>
<td>POST Processor Normals</td>
<td>IBMx_ProcessorEvent</td>
<td>2</td>
</tr>
<tr>
<td>POST Processor Warnings</td>
<td>IBMx_ProcessorEvent</td>
<td>4</td>
</tr>
<tr>
<td>Power Supply Criticals</td>
<td>IBMPSG_PowerSupplyEvent</td>
<td>6</td>
</tr>
<tr>
<td>Power Supply Normals</td>
<td>IBMPSG_PowerSupplyEvent</td>
<td>2</td>
</tr>
<tr>
<td>Power Supply SP Criticals</td>
<td>IBMPSG_SP_PowerSupplyEvent</td>
<td>6</td>
</tr>
<tr>
<td>Power Supply SP Normals</td>
<td>IBMPSG_SP_PowerSupplyEvent</td>
<td>2</td>
</tr>
<tr>
<td>Power Supply SP Warnings</td>
<td>IBMPSG_SP_PowerSupplyEvent</td>
<td>4</td>
</tr>
<tr>
<td>Power Supply Warnings</td>
<td>IBMPSG_PowerSupplyEvent</td>
<td>4</td>
</tr>
<tr>
<td>Processor PFA Criticals</td>
<td>IBMPSG_ProcessorPFEvent</td>
<td>6</td>
</tr>
<tr>
<td>Processor PFA Normals</td>
<td>IBMPSG_ProcessorPFEvent</td>
<td>2</td>
</tr>
<tr>
<td>Processor PFA Warnings</td>
<td>IBMPSG_ProcessorPFEvent</td>
<td>4</td>
</tr>
<tr>
<td>RAID Criticals</td>
<td>IBMPSG_StorageRAIDEEvent</td>
<td>6</td>
</tr>
<tr>
<td>RAID Normals</td>
<td>IBMPSG_StorageRAIDEEvent</td>
<td>2</td>
</tr>
<tr>
<td>RAID System Health Criticals</td>
<td>IBMPSG_StorageRAIDHealthEvent</td>
<td>6</td>
</tr>
<tr>
<td>RAID System Health Normals</td>
<td>IBMPSG_StorageRAIDHealthEvent</td>
<td>2</td>
</tr>
<tr>
<td>RAID System Health Warnings</td>
<td>IBMPSG_StorageRAIDHealthEvent</td>
<td>4</td>
</tr>
<tr>
<td>RAID Warnings</td>
<td>IBMPSG_StorageRAIDEEvent</td>
<td>4</td>
</tr>
<tr>
<td>Redundant NIC Switchback Criticals</td>
<td>IBMPSG_RedundantNetworkAdapterSwitchbackEvent</td>
<td>6</td>
</tr>
<tr>
<td>Redundant NIC Switchback Normals</td>
<td>IBMPSG_RedundantNetworkAdapterSwitchbackEvent</td>
<td>2</td>
</tr>
<tr>
<td>CIM filter name</td>
<td>CIM indication</td>
<td>Sev</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Redundant NIC Switchback Warnings</td>
<td>IBMPSG_RedundantNetworkAdapterSwitchbackEvent</td>
<td>4</td>
</tr>
<tr>
<td>Redundant NIC Switchover Criticals</td>
<td>IBMPSG_RedundantNetworkAdapterSwitchover Event</td>
<td>6</td>
</tr>
<tr>
<td>Redundant NIC Switchover Normals</td>
<td>IBMPSG_RedundantNetworkAdapterSwitchover Event</td>
<td>2</td>
</tr>
<tr>
<td>Redundant NIC Switchover Warnings</td>
<td>IBMPSG_RedundantNetworkAdapterSwitchover Event</td>
<td>4</td>
</tr>
<tr>
<td>Service Processor DASD Backplane Criticals</td>
<td>IBMPSG_DASDBackplaneEvent</td>
<td>6</td>
</tr>
<tr>
<td>Service Processor DASD Backplane Normals</td>
<td>IBMPSG_DASDBackplaneEvent</td>
<td>2</td>
</tr>
<tr>
<td>Service Processor DASD Backplane Warnings</td>
<td>IBMPSG_DASDBackplaneEvent</td>
<td>4</td>
</tr>
<tr>
<td>Service Processor Error Log Criticals</td>
<td>IBMPSG_ErrorLogEvent</td>
<td>6</td>
</tr>
<tr>
<td>Service Processor Error Log Normals</td>
<td>IBMPSG_ErrorLogEvent</td>
<td>2</td>
</tr>
<tr>
<td>Service Processor Error Log Warnings</td>
<td>IBMPSG_ErrorLogEvent</td>
<td>4</td>
</tr>
<tr>
<td>Service Processor Generic Fan Criticals</td>
<td>IBMPSG_GenericFanEvent</td>
<td>6</td>
</tr>
<tr>
<td>Service Processor Generic Fan Normals</td>
<td>IBMPSG_GenericFanEvent</td>
<td>2</td>
</tr>
<tr>
<td>Service Processor Generic Fan Warnings</td>
<td>IBMPSG_GenericFanEvent</td>
<td>4</td>
</tr>
<tr>
<td>Service Processor Generic Volatge Criticals</td>
<td>IBMPSG_GenericVoltageEvent</td>
<td>6</td>
</tr>
<tr>
<td>Service Processor Generic Volatge Normals</td>
<td>IBMPSG_GenericVoltageEvent</td>
<td>2</td>
</tr>
<tr>
<td>Service Processor Generic Volatge Warnings</td>
<td>IBMPSG_GenericVoltageEvent</td>
<td>4</td>
</tr>
<tr>
<td>Service Processor PFA Criticals</td>
<td>IBMPSG_PFAEvent</td>
<td>6</td>
</tr>
<tr>
<td>Service Processor PFA Normals</td>
<td>IBMPSG_PFAEvent</td>
<td>2</td>
</tr>
<tr>
<td>Service Processor PFA Warnings</td>
<td>IBMPSG_PFAEvent</td>
<td>4</td>
</tr>
<tr>
<td>Service Processor Remote Login Criticals</td>
<td>IBMPSG_RemoteLoginEvent</td>
<td>6</td>
</tr>
<tr>
<td>Service Processor Remote Login Normals</td>
<td>IBMPSG_RemoteLoginEvent</td>
<td>2</td>
</tr>
<tr>
<td>Service Processor Remote Login Warnings</td>
<td>IBMPSG_RemoteLoginEvent</td>
<td>4</td>
</tr>
<tr>
<td>SMART Drive Criticals</td>
<td>IBMPSG_SMARTEvent</td>
<td>6</td>
</tr>
<tr>
<td>SMART Drive Normals</td>
<td>IBMPSG_SMARTEvent</td>
<td>2</td>
</tr>
<tr>
<td>SMART Drive Warnings</td>
<td>IBMPSG_SMARTEvent</td>
<td>4</td>
</tr>
<tr>
<td>CIM filter name</td>
<td>CIM indication</td>
<td>Sev</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td>Storage Criticals</td>
<td>IBMPSG_StorageEvent</td>
<td>6</td>
</tr>
<tr>
<td>Storage Normals</td>
<td>IBMPSG_StorageEvent</td>
<td>2</td>
</tr>
<tr>
<td>Storage Warnings</td>
<td>IBMPSG_StorageEvent</td>
<td>4</td>
</tr>
<tr>
<td>Tachometer Normals</td>
<td>IBMPSG_FanEvent</td>
<td>2</td>
</tr>
<tr>
<td>Tachometer Sensor Criticals</td>
<td>IBMPSG_FanEvent</td>
<td>6</td>
</tr>
<tr>
<td>Tachometer Sensor Warnings</td>
<td>IBMPSG_FanEvent</td>
<td>4</td>
</tr>
<tr>
<td>Temperature Sensor Criticals</td>
<td>IBMPSG_TemperatureEvent</td>
<td>6</td>
</tr>
<tr>
<td>Temperature Sensor Normals</td>
<td>IBMPSG_TemperatureEvent</td>
<td>2</td>
</tr>
<tr>
<td>Temperature Sensor Warnings</td>
<td>IBMPSG_TemperatureEvent</td>
<td>4</td>
</tr>
<tr>
<td>Voltage Sensor Criticals</td>
<td>IBMPSG_VoltageEvent</td>
<td>6</td>
</tr>
<tr>
<td>Voltage Sensor Normals</td>
<td>IBMPSG_VoltageEvent</td>
<td>2</td>
</tr>
<tr>
<td>Voltage Sensor Warnings</td>
<td>IBMPSG_VoltageEvent</td>
<td>4</td>
</tr>
<tr>
<td>Warranty Criticals</td>
<td>IBMPSG_WarrantyExpirationEvent</td>
<td>6</td>
</tr>
<tr>
<td>Warranty Normals</td>
<td>IBMPSG_WarrantyExpirationEvent</td>
<td>2</td>
</tr>
<tr>
<td>Warranty Warnings</td>
<td>IBMPSG_WarrantyExpirationEvent</td>
<td>4</td>
</tr>
<tr>
<td>2f7c756f26b00121 (See note)</td>
<td>CIM_AlertIndication</td>
<td>Any</td>
</tr>
<tr>
<td>7f6e6daa36b2e3e5 (See note)</td>
<td>CIM_AlertIndication</td>
<td>Any</td>
</tr>
</tbody>
</table>

**Note:** The last two filters are created when a management server first discovers a managed system. The CIM filter name is the unique ID (UID) of IBM Director Server and will vary from installation to installation. See 5.5.5, “Subscriptions to IBM Director Server” on page 264, for details.
Predefined CIM subscriptions

Table B-3 on page 936 lists all combinations of filters and handlers that have been used to create the predefined subscriptions. You can see, for example, that no predefined subscriptions use the Popup handler to display a pop-up on the managed system. This default is different from the one with IBM Director 4.x.

When you list all subscriptions using the `cimsubscribe -ls` command, each subscription is displayed as shown in Example B-2 (using the first one in the Table B-3 on page 936, ASR Criticals/Log as an example).

Example: B-2 Portion of output from the `cimsubscribe -ls` command

```plaintext
CIM_IndicationSubscription.Filter="CIM_IndicationFilter.CreationClassName="CIM_IndicationFilter",Name="ASR Criticals",SystemCreationClassName="CIM_ComputerSystem",SystemName="fs2-vm-xp",Handler="CIM_IndicationHandlerCIMXML.CreationClassName="CIM_IndicationHandlerCIMXML",Name="Log",SystemCreationClassName="CIM_ComputerSystem",SystemName="fs2-vm-xp"
FailureTriggerTimeInterval = Filter = CIM_IndicationIntervalFilter.CreationClassName="CIM_IndicationFilter",Name="ASR Criticals",SystemCreationClassName="CIM_ComputerSystem",SystemName="fs2-vm-xp"
Handler = CIM_IndicationHandlerCIMXML.CreationClassName="CIM_IndicationHandlerCIMXML",Name="Log",SystemCreationClassName="CIM_ComputerSystem",SystemName="fs2-vm-xp"
OnFatalErrorPolicy = OtherOnFatalErrorPolicy = OtherRepeatNotificationPolicy = OtherSubscriptionState = RepeatNotificationCount = RepeatNotificationGap = RepeatNotificationInterval = RepeatNotificationPolicy = SubscriptionDuration = SubscriptionStartTime = SubscriptionState = SubscriptionTimeRemaining = TimeOfLastStateChange =
```
In Table B-3, if a subscription exists by default for a given filter and handler, then the corresponding cell contains Yes. If a subscription is not defined, then the cell contains No.

<table>
<thead>
<tr>
<th>CIM filter name</th>
<th>CIM handler</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Health</td>
</tr>
<tr>
<td>ASR Criticals</td>
<td>No</td>
</tr>
<tr>
<td>ASR Normals</td>
<td>No</td>
</tr>
<tr>
<td>ASR Warnings</td>
<td>No</td>
</tr>
<tr>
<td>Chassis Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>Chassis Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>Chassis Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>IPMI Log Criticals</td>
<td>No</td>
</tr>
<tr>
<td>IPMI Log Normals</td>
<td>No</td>
</tr>
<tr>
<td>IPMI Log Warnings</td>
<td>No</td>
</tr>
<tr>
<td>Lease Criticals</td>
<td>No</td>
</tr>
<tr>
<td>Lease Normals</td>
<td>No</td>
</tr>
<tr>
<td>Lease Warnings</td>
<td>No</td>
</tr>
<tr>
<td>Memory PFA Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>Memory PFA Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>Memory PFA Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Adapter Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Adapter Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Adapter Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Adapter Offline Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Adapter Offline Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Adapter Offline Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Adapter Online Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>Network Adapter Online Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>CIM filter name</td>
<td>CIM handler</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td></td>
<td>Health</td>
</tr>
<tr>
<td>Network Adapter Online Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>POST Memory Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>POST Memory Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>POST Memory Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>POST Processor Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>POST Processor Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>POST Processor Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>Power Supply Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>Power Supply Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>Power Supply Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>Power Supply SP Criticals</td>
<td>No</td>
</tr>
<tr>
<td>Power Supply SP Normals</td>
<td>No</td>
</tr>
<tr>
<td>Power Supply SP Warnings</td>
<td>No</td>
</tr>
<tr>
<td>Processor PFA Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>Processor PFA Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>Processor PFA Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>RAID Criticals</td>
<td>No</td>
</tr>
<tr>
<td>RAID Normals</td>
<td>No</td>
</tr>
<tr>
<td>RAID Warnings</td>
<td>No</td>
</tr>
<tr>
<td>RAID System Health Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>RAID System Health Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>RAID System Health Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>Redundant NIC Switchback Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>Redundant NIC Switchback Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>Redundant NIC Switchback Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>Redundant NIC Switchover Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>CIM filter name</td>
<td>CIM handler</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Health</td>
</tr>
<tr>
<td>Redundant NIC Switchover Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>Redundant NIC Switchover Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>Service Processor DASD Backplane Criticals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor DASD Backplane Normals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor DASD Backplane Warnings</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Error Log Criticals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Error Log Normals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Error Log Warnings</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Generic Fan Criticals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Generic Fan Normals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Generic Fan Warnings</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Generic Voltage Criticals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Generic Voltage Normals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Generic Voltage Warnings</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor PFA Criticals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor PFA Normals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor PFA Warnings</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Remote Login Criticals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Remote Login Normals</td>
<td>No</td>
</tr>
<tr>
<td>Service Processor Remote Login Warnings</td>
<td>No</td>
</tr>
<tr>
<td>SMART Drive Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>SMART Drive Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>SMART Drive Warnings</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage Criticals</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage Normals</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage Warnings</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### CIM subscriptions

<table>
<thead>
<tr>
<th>CIM filter name</th>
<th>Health</th>
<th>Log</th>
<th>Popup</th>
<th>SMS</th>
<th>SNMP</th>
<th>TEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tachometer Normals</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tachometer Sensor Criticals</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tachometer Sensor Warnings</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Temperature Sensor Criticals</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Temperature Sensor Normals</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Temperature Sensor Warnings</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Voltage Sensor Criticals</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Voltage Sensor Normals</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Voltage Sensor Warnings</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Warranty Criticals</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Warranty Normals</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Warranty Warnings</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2f7c756f26b00121 (See note)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>7f6e6daa36b2e3e5 (See note)</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note:** The last two subscriptions are created when a management server first discovers a managed system. The CIM filter name is the unique ID (UID) of IBM Director Server and will vary from installation to installation. See 5.5.5, “Subscriptions to IBM Director Server” on page 264, for details.
### Abbreviations and acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAS</td>
<td>Advanced Administrative System</td>
</tr>
<tr>
<td>ADGG</td>
<td>Active Directory Global Group</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>APMI</td>
<td>Advanced Power Management Interface</td>
</tr>
<tr>
<td>ASCII</td>
<td>American National Standard Code for Information Interchange</td>
</tr>
<tr>
<td>ASF</td>
<td>Alert Standard Format</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application-specific integrated circuit</td>
</tr>
<tr>
<td>ASM</td>
<td>Advanced System Management</td>
</tr>
<tr>
<td>ASR</td>
<td>Automatic server restart</td>
</tr>
<tr>
<td>BIOS</td>
<td>Basic input output system</td>
</tr>
<tr>
<td>BMC</td>
<td>Baseboard management controller</td>
</tr>
<tr>
<td>CD</td>
<td>Compact disk</td>
</tr>
<tr>
<td>CD-ROM</td>
<td>Compact disk read only memory</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge-Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CIM</td>
<td>Common Information Model</td>
</tr>
<tr>
<td>CIMOM</td>
<td>Common Information Model Object Manager</td>
</tr>
<tr>
<td>CLP</td>
<td>Command Line Protocol</td>
</tr>
<tr>
<td>CMOS</td>
<td>Complementary metal oxide semiconductor</td>
</tr>
<tr>
<td>COM</td>
<td>Component Object Model</td>
</tr>
<tr>
<td>CPU</td>
<td>Central processing unit</td>
</tr>
<tr>
<td>CSV</td>
<td>Comma separated variable</td>
</tr>
<tr>
<td>DCOM</td>
<td>Distributed Component Object Model</td>
</tr>
<tr>
<td>DEA</td>
<td>Data Encryption Algorithm</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DIP</td>
<td>Development-Integration-Production</td>
</tr>
<tr>
<td>DMI</td>
<td>Desktop Management Interface</td>
</tr>
<tr>
<td>DMTF</td>
<td>Distributed Management Task Force</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defence</td>
</tr>
<tr>
<td>DSA</td>
<td>Digital signature algorithm</td>
</tr>
<tr>
<td>EAP</td>
<td>Event action plan</td>
</tr>
<tr>
<td>ESA</td>
<td>Electronic Service Agent</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>FRU</td>
<td>Field replaceable unit</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer Protocol</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>GPO</td>
<td>Group Policy Object</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphical user interface</td>
</tr>
<tr>
<td>HATS</td>
<td>Host Access Transformation Services</td>
</tr>
<tr>
<td>HBA</td>
<td>Host bus adapter</td>
</tr>
<tr>
<td>HKLM</td>
<td>HKEY Local Machine</td>
</tr>
<tr>
<td>HMC</td>
<td>Hardware Management Console</td>
</tr>
<tr>
<td>HTML</td>
<td>Hypertext Markup Language</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transmission Protocol</td>
</tr>
<tr>
<td>I/O</td>
<td>Input/output</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>IBM</td>
<td>International Business Machines Corporation</td>
</tr>
<tr>
<td>ID</td>
<td>Identifier</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IM</td>
<td>Instant messaging</td>
</tr>
<tr>
<td>IMAPI</td>
<td>Image Mastering Application Programming Interface</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPC</td>
<td>Interprocess communication</td>
</tr>
<tr>
<td>IPMI</td>
<td>Intelligent Platform Management Interface</td>
</tr>
<tr>
<td>IPX</td>
<td>Internetwork packet exchange</td>
</tr>
<tr>
<td>ISM</td>
<td>Integrated system management</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standards</td>
</tr>
<tr>
<td>IT</td>
<td>Information technology</td>
</tr>
<tr>
<td>ITSO</td>
<td>International Technical Support Organization</td>
</tr>
<tr>
<td>IU</td>
<td>Installable unit</td>
</tr>
<tr>
<td>IUDD</td>
<td>Installable unit deployment descriptor</td>
</tr>
<tr>
<td>JDBC™</td>
<td>Java Database Connectivity</td>
</tr>
<tr>
<td>JVM™</td>
<td>Java Virtual Machine</td>
</tr>
<tr>
<td>LAN</td>
<td>Local area network</td>
</tr>
<tr>
<td>LED</td>
<td>Light emitting diode</td>
</tr>
<tr>
<td>LPAR</td>
<td>Logical partitions</td>
</tr>
<tr>
<td>LUN</td>
<td>Logical unit number</td>
</tr>
<tr>
<td>MAC</td>
<td>Media access control</td>
</tr>
<tr>
<td>MB</td>
<td>Megabyte</td>
</tr>
<tr>
<td>MIB</td>
<td>Management information base</td>
</tr>
<tr>
<td>MMC</td>
<td>Microsoft Management Console</td>
</tr>
<tr>
<td>MOM</td>
<td>Microsoft Operations Manager</td>
</tr>
<tr>
<td>MPA</td>
<td>Management Processor Assistant</td>
</tr>
<tr>
<td>MPCLI</td>
<td>Management processor command line interface</td>
</tr>
<tr>
<td>MSCS</td>
<td>Microsoft Cluster Server</td>
</tr>
<tr>
<td>MSDE</td>
<td>Microsoft SQL Server Desktop Engine</td>
</tr>
<tr>
<td>MSI</td>
<td>Microsoft Installer</td>
</tr>
<tr>
<td>MSN</td>
<td>Microsoft Network</td>
</tr>
<tr>
<td>NAS</td>
<td>Network addressable storage</td>
</tr>
<tr>
<td>NIC</td>
<td>Network interface card</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NNTP</td>
<td>NetNews transfer protocol</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NTFS</td>
<td>NT file system</td>
</tr>
<tr>
<td>OEM</td>
<td>Other equipment manufacturer</td>
</tr>
<tr>
<td>OS</td>
<td>Operating system</td>
</tr>
<tr>
<td>PAM</td>
<td>Pluggable authentication module</td>
</tr>
<tr>
<td>PC</td>
<td>Personal computer</td>
</tr>
<tr>
<td>PCI</td>
<td>Peripheral component interconnect</td>
</tr>
<tr>
<td>PET</td>
<td>Platform Event Trap</td>
</tr>
<tr>
<td>PFA</td>
<td>Predictive Failure Analysis</td>
</tr>
<tr>
<td>PID</td>
<td>Process ID</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal identification number</td>
</tr>
<tr>
<td>PMON</td>
<td>Process monitor</td>
</tr>
<tr>
<td>POE</td>
<td>Proofs of Entitlement</td>
</tr>
<tr>
<td>PPO</td>
<td>Physical Platform Object</td>
</tr>
<tr>
<td>PPMO</td>
<td>Physical Platform Managed Object</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-point protocol</td>
</tr>
<tr>
<td>PXE</td>
<td>Pre-boot-execution</td>
</tr>
<tr>
<td>RAID</td>
<td>Redundant array of independent disks</td>
</tr>
<tr>
<td>RAS</td>
<td>Remote access services; row address strobe</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
</tr>
<tr>
<td>RDM</td>
<td>Remote Deployment Manager</td>
</tr>
<tr>
<td>RPM</td>
<td>Red Hat Package Manager</td>
</tr>
<tr>
<td>RSA</td>
<td>Remote Supervisor Adapter</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage area network</td>
</tr>
<tr>
<td>SATA</td>
<td>Serial ATA</td>
</tr>
<tr>
<td>SCSI</td>
<td>Small computer system interface</td>
</tr>
<tr>
<td>SDK</td>
<td>Software Developers' Kit</td>
</tr>
<tr>
<td>SLP</td>
<td>Service Location Protocol</td>
</tr>
<tr>
<td>SMASH</td>
<td>Systems Management Architecture for Server Hardware</td>
</tr>
<tr>
<td>SMBIOS</td>
<td>System management BIOS</td>
</tr>
<tr>
<td>SMI-S</td>
<td>Storage Management Initiative Specification</td>
</tr>
<tr>
<td>SMS</td>
<td>System Managed Space</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple mail transfer protocol</td>
</tr>
<tr>
<td>SNIA</td>
<td>Storage Networking Industry Association</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SOA</td>
<td>Service Oriented Architecture</td>
</tr>
<tr>
<td>SOL</td>
<td>Serial over LAN</td>
</tr>
<tr>
<td>SPP</td>
<td>Server Plus Pack</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured query language</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>SWMA</td>
<td>Software Maintenance Agreement</td>
</tr>
<tr>
<td>TAP</td>
<td>Telocator Alphanumeric Protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TCP/IP</td>
<td>Transmission Control Protocol/Internet Protocol</td>
</tr>
<tr>
<td>TEC</td>
<td>Tivoli Enterprise Console</td>
</tr>
<tr>
<td>TME</td>
<td>Tivoli Management Environment®</td>
</tr>
<tr>
<td>TTL</td>
<td>Time to live</td>
</tr>
<tr>
<td>TWG</td>
<td>Tivoli Workgroup</td>
</tr>
<tr>
<td>UDP</td>
<td>User datagram protocol</td>
</tr>
<tr>
<td>UID</td>
<td>Unique ID</td>
</tr>
<tr>
<td>URL</td>
<td>Uniform Resource Locator</td>
</tr>
<tr>
<td>USB</td>
<td>Universal serial bus</td>
</tr>
<tr>
<td>VB</td>
<td>Visual Basic</td>
</tr>
<tr>
<td>VE</td>
<td>Virtualization Engine</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VMM</td>
<td>Virtual Machine Manager</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual private network</td>
</tr>
<tr>
<td>VRM</td>
<td>Voltage regulator module</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide area network</td>
</tr>
<tr>
<td>WBEM</td>
<td>Web-Based Enterprise Management</td>
</tr>
<tr>
<td>WINS</td>
<td>Windows Internet Naming Service</td>
</tr>
<tr>
<td>WMI</td>
<td>Windows Management Instrumentation</td>
</tr>
<tr>
<td>WQL</td>
<td>WMI Query Language</td>
</tr>
<tr>
<td>XML</td>
<td>Extensible Markup Language</td>
</tr>
</tbody>
</table>
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

For information about ordering these publications see “How to get IBM Redbooks” on page 949. Note that some of the documents referenced here may be available in softcopy only.

- *IBM eServer xSeries and BladeCenter Server Management*, SG24-6495
- *Planning and Installing the IBM eServer X3 Architecture Servers*, SG24-6797
- *Remote Supervisor Adapter II Family — Firmware and Drivers Quick Reference*, TIPS0534
- *IBM @server xSeries BMC — Firmware and Drivers Quick Reference*, TIPS0532
- *Service Processors Supported in IBM System x Servers*, TIPS0146

Other publications

These publications are also relevant as further information sources:

- IBM Director product publications
  - *IBM Director Planning, Installation, and Configuration Guide*
  - *IBM Director Systems Management Guide*
  - *IBM Director Capacity Manager Installation and User’s Guide*
  - *IBM Director Events Reference*
  - *IBM Director System Availability Installation and User’s Guide*
  - *IBM Director Upward Integration Modules Installation Guide*
  - *IBM Director Web-based Access Installation and User’s Guide*
  - *IBM Director Troubleshooting Guide*
- IBM Director Commands Reference
- IBM Director Upward Integration Module for HP OpenView Installation and User's Guide
- IBM Director Upward Integration Module for Microsoft Systems Management Server Installation and User's Guide
- IBM Director Upward Integration Module for Microsoft Operations Manager Installation and User's Guide
- IBM Director Upward Integration Module for Tivoli Management Framework Installation and User's Guide
- IBM Director Upward Integration Module for Tivoli NetView Installation and User's Guide
- ServeRAID Management Installation and User's Guide

These are available from:
http://www.ibm.com/systems/management/director/resources

or through the online InfoCenter at:
http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/diricinfo_5.20/fqm0_main.html

► Microsoft Whitepaper, Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2

► Microsoft Whitepaper, Using the Windows Firewall INF File in Microsoft Windows XP Service Pack 2

► Microsoft Whitepaper, Managing Windows XP Service Pack 2 Features Using Group Policy
Online resources

The following Web sites and URLs are also relevant as further information sources.

IBM Web sites

- IBM Director home page

- IBM Director downloads

- IBM Director product publications
  http://www.ibm.com/systems/management/director/resources

- IBM Director user forum

- IBM Support site
  http://www.ibm.com/support

- IBM Director Support Tools

- UpdateXpress Server

- UpdateXpress CD

- IBM Director SDK
  http://publib.boulder.ibm.com/infocenter/dirinfo/toolkit

- IBM Virtualization Engine and IBM Director
  http://www.ibm.com/servers/eserver/about/virtualization/enterprise/director.html

- IBM Remote Deployment Manager
IBM Director Subscription Services
http://www.ibm.com/servers/eserver/xseries/systems_management/
subscription_services.html

System x Lab Services
http://www.ibm.com/eserver/services/xseriesservices.html

IBM Remote Technical Support Services - ServicePac
http://www.ibm.com/systems/support/supportsite.wss/docdisplay?
brandind=5000016&ndocid=MIGR-43272

Non-IBM Web sites

Microsoft Whitepaper, Deploying Windows Firewall Settings for Microsoft
Windows XP with Service Pack 2:
http://www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-
61fa-447a-bdcd-499f73a637d1&DisplayLang=en

Microsoft Whitepaper, Using the Windows Firewall INF File in Microsoft
Windows XP Service Pack 2
97-4e63-a581-bf25685b4c43&DisplayLang=en

Microsoft Whitepaper, Managing Windows XP Service Pack 2 Features Using
Group Policy
bd-4c50-bdab-96ff9f00e007&DispalyLang=en

Alert Standard Format Specification
http://www.dmtf.org/standards/asf

Common Information Model Standards
http://www.dmtf.org/standards/cim

How to use the **reset session** command to a terminal server
library/ServerHelp/fe39192e-0cb5-47da-9e00-26d864e51b0d.mspx

Virus test file
http://www.eicar.org/anti_virus_test_file.htm

Using the RunOnce key in the registry
help/html/xereconrunoncerequest.asp
- Download the `psexec` command
  
  http://www.sysinternals.com

- Distributed Management Task Force
  
  http://www.dmtf.org

- SMBus home page
  
  http://www.smbus.org

- i2c information
  
  http://www.philipslogic.com/i2c

- LifeKeeper for IBM Director
  
  http://www.steeleye.com/partners/technology/ibm/director.html

### How to get IBM Redbooks

You can search for, view, or download Redbooks, Redpapers, Hints and Tips, draft publications and Additional materials, as well as order hardcopy Redbooks or CD-ROMs, at this Web site:

ibm.com/redbooks

### Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services
Index

Symbols
& variables 734

Numerics
5648-DR1 21
5722-DR1 21
5765-DIR 21

A
actions 731–742, 893–921
add/remove from static group 896
alphanumeric pager 906
data substitution variables 734
e-mail notification 738, 857, 908
event log 899
history 741
log to a text log 902
message to a console user 866, 907
newsgroup 903
numeric pager 912
pop-up message 736
resend modified event 904
send an e-mail 738, 857, 908
set a system variable 914
SNMP inform to IP host 909
SNMP trap to IP host 911
SNMP trap to NetView 910
source group members to static group 897
start a program 856, 916–918
start a task 919
static group, add/remove 896
status update 867, 920
summary 732, 894
TEC event 913
text file 902
ticker tape 898
timed alarm start a program 901
timed alarm to generate an event 900
update the status 867, 920
variables 734
Virtualization Manager 561
write to text log 902

Active Directory
Firewall configuration 233
Global Groups 47, 118
group access 822
scenario 814
service account 122
use in logon 123
Active PCI Manager 180
AddKnownServerAddress parameter 207, 778
admin share 220
administrator privileges 45
AES
about 98
Server-Agent communications 111
Agent
See IBM Director, Agent
agent-initiated discovery 55
agentless discovery 778, 780
agentless tasks 289
AIX
InstallP packages 407
pluggable authentication module 103
tasks supported 288
Alert Standard Format 26
alerts
See also events
alert forwarding (SP) 186, 193
IBM Director 77
troubleshooting 225
allowedAddress 124
allowedRange 125
alphanumeric pager action 906
Apache Derby 48
APC PowerChute 18
application priority 80
Applied Inventory Monitors window 863
Asset ID task 291
profile builder 369
associations
Console view 190
event action plans 688
authentication
concept 96
LDAP 104
implementing ibm director 5.20

pluggable authentication module 103
server-agent 140
automatic logon 230
automatically secure unsecured systems 141
automation 203

b
backup 267
battery voltage 390
bios updates 403, 788
bladecenter 2
configuration 379
management module ports 61–62
bladecenter configuration manager 15, 378
create a profile 380
event filters 704
existing configuration 379
ip address pool 378
network device manager 382
profiles 380
switch configuration 378
block diagram 5
block queued events 724, 747
blue indicator led 193
bmc 181
adding to ibm director 186
alert forwarding 186, 193
block diagram 5
bmc_cfg 186
default ip address 187
drivers 183
ibm director 182
openipmi driver 201
padlock icon 187
pet 5, 183
pet filters 711
ports 60
power control 193
security 110
server configuration manager 192
showing in console 190
standard 4
broadcast discovery 56, 241
broadcast relay agents 57, 244

c
capacity management 72
capacity manager 18, 72, 401
event types 702
server plus pack 180
ups performance 390
category tab, event action plan 725
cd-rom 21
certmgr command 138
changes in inventory 313, 860
changes to your environment 795
chap 98
choosing the right agent 51
cim 4
see also cimsubscribe
event types 702
events not logged 747, 751
handlers 257
subscriptions 931, 937
cim browser 292
cim_alertindication 266
cimom 12
cimsubscribe 256, 931–941
filters 257, 932–936
handlers 257, 932
interactive mode 265
namespace 265
subscriptions 259, 937–941
client 11
cloning 53, 208
scenario 766
cluster browser task 316
clustering technology 168
cmd /c command 737
cmdext file 304
cmdtask file 304
code download 21
collect inventory 312
collect software data 759
collection services 23
command prompt task 320
command-line tools 931–941
bmc_cfg 186
certmgr 138
cimsubscribe 256
cmd 737
dakill 277, 856
dirclean 226
dirci 795–811, 846
dirgather 227
dirstop 227
filechek 226
genevent 222
MPCLI 186, 193–194
playwav 856
psexec 834
runas 798
telnet 104
twgconw 230
twgpccf 223
twglstsr 224
twgrepair 226
twgreset 280
twgrestore 279
twgsave 279
community name (SNMP) 101, 373
components 10
configuration 229–281
Configure SNMP Agent task 293
Console
   See IBM Director, Console
Core Services 11–12
   installation 52
CPU monitoring 321
cross-platform 2
custom inventory collection 312
Custom Inventory task 861

D
dakill command 277, 856
data substitution variables 734, 867
database
   by operating system 48
default 49
   Express installation 152
   planning 48
day/time tab, event action plans 723
DB2 48
DCOM 12, 137
DEA 97
default IP addresses 187
deployment
   RDM 402
   Software Distribution Premium Edition 407
Derby 48
DES 97, 144
Development-Integration-Production 40
dictionary, software 850
Diffie-Hellman 100, 144
digital signatures 99, 141
DirAdmin 45, 116–117, 123
diragent.rsp file 204
DirClean 226
dircli 795–811, 846
   5.20 updates 24
   LDAP 107
   Update Manager 452
   Virtualization Manager 567
Director
   See IBM Director
Director (event type) 705
director.topology.online/offline events 757
DirectorConsumer handler 267
directory monitoring 327
DirGather command 227
dirinst.log file 220
DirMaint 579–580
DirStop command 227
DirSuper 45, 116–117, 123
DisableScreenSaver parameter 207
DisableWallpaper parameter 207
discovery 231–244
   about 55
   agent-initiated 55, 113
   agentless 780
   broadcast 241
   Discovery Preferences window 191
   firewalls 232
   Level-0 780
   multicast 241
   Physical Platform naming template 192
   relay agents 244
   security 140
   server-initiated 56
   SLP 7
   SNMP devices 253
   troubleshooting 225
   types 240
   unicast 243
   unknown agents 778
disk space monitoring 324
Distribution Preferences 214
distribution server
   architecture 211
   create 816
   scenario 814
DMTF 4
Domain Policy 236
donor systems 768
downloads 21
Driver parameter 206
drivers 788
    service processors 183
DSA 99
DSA*.PUB files 141
DSA*.PVT files 142
duplicate event filter 696
dynamic groups 32, 820
    event action plans 90
    seed value 852
    software 852
    Windows 2000 SP3 group 246

E
Electronic Service Agent 73, 392, 461–486
    configure 467
data sent 463
download 464
    ECI ID 475
    enrollment 479
event filters 710
events 486
    filters 710
history 483
implementation 463
installation 464
Linux install 465
overview 16, 462
PMR tab 485
process 462
proxy 471
see also ESA 462, 488
sent data 463
setup 467
test connection 472
using 479
Windows install 464
wizard 468
electronic support 28
e-mail notification 738, 857, 908
encoding 96
EncryptCommunication parameter 205
encryption 96
    AES 98, 111
    DES 97
    DSA 140
    Encryption Administration 147
implementing 143
resending keys 147
response file parameter 205
    RSA II 110
Server-Agent communications 111
SSL 100
summary 147
error logs 220
ESA 943
ESX Server
    OpenIPMI driver 202
    service processor driver 196
tasks supported 288
    Virtualization Manager 515
Event Action Plan Builder 686–689
    actions 731–742
    applying plans 745
    associations 688
    event action plans 687
    example 742
    filters 689–730
    SNMP trap forwarding 255
    starting 687
Event Action Plan Wizard 679–686
    actions 684
    change 686
    edit 686
    event filters 683
    example 827
    name screen 681
    starting 680
time range 685
event action plans
    action history 734, 741
    actions 731–742
    pop-up message 736
    APC UPSes 391
    applying 88–89, 745
    associations 688
    block queued events 724
    Capacity Manager events 702
category 725
    CIM event type 702
components 678
customize actions 733
data substitution variables 734, 867
day/time tab 723
Director event type 705
dynamic groups 90
Index

955

e-mail notification 738
Event Action Plan Builder 686–689
Event Action Plan Wizard 679–686
Event Text tab 727
Event Type tab 690, 698
event 742, 826
exporting 273, 761
extended attributes 729
frequency tab 696
history of actions 741
HTML export 277
importing 274, 761
inventory changes 863
Log All Events 750
naming 687
planning 77–78
process monitor events 855
queued events 724
recommendations 749
scenario 826
sender name 725
ServeRAID event type 713
severity 722
show implementations 733
Skype 855
SNMP event type 712
static groups 89
storage event type 713
Symantec AntiVirus 757
System Variables tab 729
terms 77
UPSes 391
Windows Event Log event type 719
event log (action) 899
Event Log tasks 294
Event Text tab, event action plan 727
Event Type tab 698
events 677–763
See also actions
See also event action plans
See also filters
actions 82
APC UPSes 391
block queued events 724, 747
CIM events 257
client system recommendations 91, 754
day/time 723
definitions of terms 679
duplication event filter 696
Electronic Service Agent 486
Event Action Plan Builder 686
Event Action Plan Wizard 679–686
exclusion event filter 692
Extended Attributes tab 693
filter types 690
recommendations 750
filters 689–730
frequency tab 696
groups 87
management 30
planning 78
plans 77
process monitor 855
queued events 724, 747
server system recommendations 755
severities 82, 721
severity 722
simple event filter 691
Symantec AntiVirus 759
threshold event filter 694
troubleshooting 225
TWGType.ini file 702
Update Manager 450
UPSes 391
Virtualization Manager 561
what happens 679
Windows Event Log 719
examples 765–869
cloning 766
dircli 795
Event Action Plan Builder 742
Event Action Plan Wizard 827
groups 246
inventory changes 860
PowerExecutive 869
promotion 778
remote install 778
report creation 795
rollout 812
rollout status 842
spreadsheet 842
Symantec AntiVirus 757
unauthorized applications 848
upgrade Agent level 778
Excel spreadsheet 843
exclusion event filter 692
execution history window 791
export
Implementing IBM Director 5.20

EAP as HTML 277
event action plans 273, 761
groups 268
IBM Director configurations 268
Express installation 152–167
comparison with standard install 152
converting to standard 161
database 152, 166
discovery preferences 159
Event Action Plan wizard 159
installing 154
overview 23
planning 51
procedure 154
security 153
tasks 153
user access 167
Express Start window 159
extended attributes tab, event action plan 729
extensions 14, 285
agent level support 287
APC PowerChute 18
BladeCenter Configuration Manager 15
Capacity Manager 18, 72, 401
Electronic Service Agent 16, 73, 392, 461–486
fee-based 18, 287, 400
free 16, 286, 386
HMC Manager Tools 16
install time 15
install-time 378
Network Device Manager 15
PowerChute 386
PowerExecutive 16, 73, 393, 487–512
Rack Manager 15, 383
RDM 19
remote control 15
Remote Deployment Manager 74, 402
ServeRAID Manager 17, 393
Software Distribution Premium Edition 19
SteelEye LifeKeeper 18
System Availability 17
deployment 836
System x 15
Update Manager 63, 413–460
Virtualization Manager 17, 75, 400, 515–569
z/VM Center 19, 75, 411, 571
External Application Launch
dircli 309
hints & tips 307
remote consoles 306
External Application Launch task 294
External Application Launch Wizard 294–304

F
fee-based extensions 18
file distribution
architecture 211
create 816
scenario 814
file monitoring 326
File Transfer task 309
Filecheck command 226
filters 689–730
APC UPSes 391
BladeCenter Configuration Manager 704
block queued events 724
Capacity Manager 702
category 725
CIM 257, 702
Configuration Manager 704
day/time 723
deleting event types 699
Director 705
duplication event filter 696
dynamic entries 700
Electronic Service Agent 710
Event Text 727
event type 698
exclusion event filter 692
extended attributes 729
Extended Attributes tab 693
frequency tab 696
MassConfig 710
MPA 711
PET 711
recommended 750
sender name 725
Server Configuration Manager 704
severities 721
severity 722
simple event filters 691
SNMP 712
storage 713
System Variables tab 729
threshold event filter 694
types 690
UPSes 391
Virtualization Manager 561, 714
firewalls 232
forum 28
free extensions 16
frequency (power) 390
frequency tab 696

G
genevent command 56, 222
geography 78
graphs 396
group categories 245
Group Policy Object editor 233
groups 245–252
  about 71
  access to 119
  APC UPSes 388
  categories 35, 245
dynamic 388
dynamic groups 247, 820
examples 246
exporting 268
importing 270
operating system group 247
patch level example 248
planning 71
restricting access to 129
security 822
tips 88
types 32
types of 87
UPSes 388
  Windows 2000 SP3 group 246
groups of groups 35

H
handlers 257
hardware status 30
Hardware Status task 310
health, CIM handler 258
high availability 69
  SteelEye LifeKeeper 168
history of actions 741
HMC
  HMC Manager Tools 16
  Virtualization Manager 520
home page 26
HTML output of an EAP 277
HTTP 103
humidity 390

I
I2C 7
i5/OS
  Collection Services 23
  message queues 25
  restore packages 407
  tasks supported 288
  user accounts considerations 45
IBM DB2 48
IBM Director
  actions 731–742
  AddKnownServerAddress parameter 207
Agent 12
  CIM subscriptions 259, 266
  clearing 225
  cloning 208, 766
  comparison 51
  installation 52
  licenses 20
  listing servers 224
  name 767
  resetting 225
  response file 818
  security 111, 135
  system name 767
  unique ID 767
  upgrading 67
alerting 77
architecture 11
block diagram 5
block queued events 747
blocked queued events 724
BMC 182
BMC driver check 184
broadcast discovery 241
broadcast relay agents 244
cimsubscribe
  See cimsubscribe
cloned installations 53
communications 746
components 10–11
configuration 229–281
Console 13
  access 119, 125
  associations 190
software inventory 759
streamed installations 211
subscriptions 22
support offerings 28
Support Tools 226
system variable 914
tasks 283–411
See also tasks
TCP/IP ports 57
ticker tape 898
troubleshooting 217
TWGIPCCF.EXE 223
TWGRas log 190
unicast discovery 243
upgrading 66
user accounts 45, 116
user logon security 125
user profiles 126
version number 219
what's new in V5.20 23
IBM Systems Director 3
IBM Update Assistant 357
icons
padlock
See padlock icon
question mark 146
red x 311
system error 868
system status 866
yellow bang 311
IETF 7
importing
event action plans 274, 761
groups 270
in-band communication 182
Indication Notification message 264
input line frequency 390
Insight Manager, migrating from 68
installation 53, 151–226
Agent 52
agentless systems 782
BladeCenter Management 378
diragent.rsp file 204
extensions, optional 378
file distribution 211
log files 220
redirected installation 211
ServeRAID 216
service processors 181
silent uninstall 226
Software Distribution task 355
Software Health Check 366
streamed installation 211
Sysprep 209
System Availability 836
troubleshooting 217
unattended 203
uninstall 226
upgrade Agent level 778
Installed Patches 250
InstallP packages 407
InstallShield 54, 162, 217, 407
introduction 1
inventory 30
changes 860
collecting 799
custom collection 861
discovery 799
Inventory Monitors task 313, 860
task 312
UPS data 389
IP addresses
allowed to logon 124
IPC 267
IPMI
block diagram 5
standard 4

J
Java 121
Jet 48

L
LDAP 104
configuration 105
dircli commands 107
enabling 105
planning 46
user groups 106
Level-0
agent 12
connectivity 779
discovery 778, 780
Level-1 agent 11
Level-2 agent 11
licensing 20
upgrades 22
LifeKeeper
   See SteelEye LifeKeeper
line frequency 390
Linux
   pluggable authentication module 103
tasks supported 288
   unattended installation 55
Linux on z/VM
   See z/VM Center
listing servers 224
LM chip 8
loadedmibs.dat file 352
locked systems 805
log, CIM handler 259
logon
   automatically 230
   process 123
logs
dirinst.log 220
Event Log task 294
troubleshooting 220
TWGRAs.log 220

M
machine identifier 770
maintenance 22
managed system 11
   See also IBM Director, Agent
management console 11
   See also IBM Director, Console
management module
   configuration 379
   ports 61–62
management processor assistant
   BladeCenter Configuration Manager 378
event filters 711
   Server Configuration Manager 337
management server 11
   See also IBM Director, Server
mass configuration 31, 368
Asset ID 291
Configure SNMP Agent 373
event filters 710
   network configuration 375
Message Browser
   Virtualization Manager 566
MI B files 350
   compiling 254, 352
loading into memory 255, 353
Microsoft Cluster Browser task 316
Microsoft SQL Server 48
Microsoft Systems Management Server
   CIM handler 258
Microsoft Virtual Server
   Virtualization Manager 515
migration from Insight Manager 68
MPCLI 193
   alert forwarding 186, 194
MSDE 48
MSI packages 407
multicast discovery 56, 241

N
nameplate power 869
namespace 265
net send command 736
netdrvr.ini file 209, 767
NetTimeout parameter 206
NetView
   SNMP trap action 910
NetWare
   scripted installations 55
tasks supported 288
network
   drivers 767
   planning 44
   ports 779
      BMC 60
      IBM Director 59
      management module 61–62
      RSA II 59
   trace 748
Network Configuration task 316, 375
Network Device Manager 15, 382
newsgroup (action) 903
NNTP (action) 903
numeric pager (action) 912

O
online/offline events 757
OpenIPMI driver 201
OpenPower 2
operating system query 246
Oracle 48
outages 396
out-of-band communications 183, 185
Restricting access 124
rollout example 812
root account 45
RSA II 181
  adding to IBM Director 186
  alert forwarding 186, 193
  block diagram 5
  default IP address 187
  drivers 183
  encryption 110
  ESX Server installation 196
  IBM Director 182
  padlock icon 187
  ports 59
  power control 193
  security 109
  Server Configuration Manager 192
  showing in Console 190
  SNMP 101, 110
  Web interface 192
runas command 798
RunOnce registry key 774
Scenarios 765–869
  cloning 766
dircli 795
  inventory changes 860
PowerExecutive 869
promotion 778
remote install 778
report creation 795
rollout 812
rollout status 842
spreadsheet 842
Symantec AntiVirus 757
unauthorized applications 848
upgrade Agent level 778
Scheduler 76, 330
  calendar view 337
example of use 837
new job 332
options 334, 840
repeating 332
targets tab 839
tasks tab 333
screen saver 207
SECIN.INI file 141
SecureAgent parameter 206, 835
security 95–149
  access to IBM Director 119
  AES 98, 111
  Agent security 135
  authentication 140
  automatically secure unsecured systems 141
  BMC 110
  certmgr command 138
  challenge 142
  CHAP 98, 142
  concepts 96
  Console access 125
  DES 97, 144
  Diffie-Hellman 100, 144
  digital signatures 141
  diragent.rsp file 205
  DSA 99, 140
  DSA*.PUB files 141
  dynamic groups 822
  encryption
    See also encryption
defined 96
    IBM Director 143
  events 701
  Express installation 153
  groups, access to 119, 129
  HTTP 103
  IBM Director Agent 111
  IBM Director Console 114
  IBM Director Server 110
  keys 138
  LDAP 104
  padlock icon 141
  planning 109
  privileges 119, 127
  protocols 98
  public/private keys 138
  RSA II 109
  service processors 109
  SNMP 100–101, 147
  SSH 103
  SSL 100, 143–144
  task access 120, 131
  telnet 104
  Triple-DES 97
  unsecured systems 141
  user logon 125
  user profiles 126
  z/VM Center 120
  seed value 852
  sender name tab, event action plan 725
Server
  See IBM Director, Server
Server Configuration Manager 192, 337
  Alerts Configuration 341
  applying a profile 347
  automatic deploy 348
  deploy 348
  Detect & Deploy 348
  DHCP addresses 346
  event filters 704
  existing configuration 338
  IP Address Pool 340
  Login Profile 344
  Network Configuration 346
  profiles 339
  Quick Start 338
  untargeted launch 338
  user accounts 344
  server management 5
Server Plus Pack 179
  uninstalling 180
ServeRAID
  event types 713
  installation 216
  ServeRAID Manager 17, 393
  Update Manager 445
  server-initiated discovery 56
  service account 46, 122
  service processors
    adding to IBM Director 186
    blue indicator LED 193
    BMC 181
    default IP addresses 187
    drivers 183
    IBM Director 182
    naming template 191
    padlock icon 187
    power control 193
    RSA II 181
    security 109
    Server Configuration Manager 192
    showing in Console 190
ServicePac 28
  services 317
  severities 82
  Severity tab 722
share name 213
ShutdowndoesPoweroff parameter 207
signatures, digital 99
silent uninstall 226
simple event filter 691
Skype 853
SLP 7, 12, 104
SMASH 9
SMBIOS 3, 8
SMBus 7
SMI-S 8
SMS, CIM handler 258
SMTP
  IBM Director action 738, 908
SNMP 7, 100, 252–256, 348
  CIM handler 258
  compiling MIBs 254, 352
  configuration task 373
  Configure SNMP Agent task 293
discovery 253
Discovery Preferences 253
event types 712
IBM Director action 910–911
loading MIBs 255, 353
recompileImports 254
recompileOnStartup 254
RSA II 110
security 147
security issues 101
SNMP Browser 254, 348–349
SNMPserver.properties file 254
SNMPv3 101
trap forwarding 255
Windows configuration 148
SNMP management 31
SNMPserver.properties file 254, 351
software dictionary 850
software distribution 64, 355
  agentless systems 782
BIOS 355
delayed delivery 831
file distribution server 816
Health Check 355
IBM Director packages 358, 819
Level-0 systems 355
package editor 365
Premium Edition 407
report 357
scenario 778
Software Health Check 355, 366
static group 355
streaming packages 355
System Availability extension 836
Update Assistant 357
Update Manager 355
UpdateXpress 359
Software Distribution Premium Edition 19
Software Health Check 366
software inventory 759, 815, 849
Software Rejuvenation 180
Solution Install format 357, 784
SQL Server 48
SSH 103, 137
SSL
  Console-Server 143
defined 100
  Level-1 systems 137
  Use SSL checkbox in Console 115, 144
standards 3
BMC 4
CIM 4
CIMOM 12
DCOM 12
DMTF 4
IETF 7
IPMI 4
PET 5
PFA 6
SLP 7, 12
SMASH 9
SMBIOS 8
SMBus 7
SMI-S 8
SNMP 7
WMI 12
start and stop processes 317
static address 225
static groups 35
event action plans 89
static IP address 267
SteelEye LifeKeeper 18, 168–179
disk resources 169
failover 174
HA setting 171
introduction 69
IP addresses 169
overview 168
protected resources 169
services 169
status of systems 174
TWGServer.prop file 172
user interface 170
storage
  event types 713
storage monitoring 324
streamed installations 211
streamed software distribution 65, 73
su command 799
subscriptions 22
substitution variables 734
superuser access 45
support
  electronic support 28
Support Line 29
support offerings 28
Symantec AntiVirus 757
Symantec Antivirus
  events 759
Sysprep 209, 768
System Accounts 367
System Availability 17, 180, 395
System Pack 415
system processes 317
System Variables tab 729
System z9 2
SystemName parameter 206
Systems Director 3

T
TargetDrive parameter 205
TargetFolder parameter 205
task-based groups 34
tasks 283–411
  Active PCI Manager 180
  agent level support 287
  agentless tasks 289
  APC UPS browser 388
  Asset ID 291–292, 369
  base tasks 284
  BladeCenter Configuration Manager 378
  Capacity Manager 180, 401
  CIM Browser 292
  command prompt 320
  Configure SNMP Agent 293, 373
  Electronic Service Agent 392, 461–486
  Event Action Plans 293
  Event Log 294
  Express installation 153
  External Application Launch 294
  External Application Launch Wizard 294–304
  File Transfer 309
  Hardware Status 310
  Inventory 312
  Inventory Monitors task 860
  level of agent 284
  mass configuration 368
  Microsoft Cluster Browser 316
  Network Configuration 316, 375
  Network Device Manager 382
  operating system support 288
  PowerChute 386
  PowerExecutive 393, 487–512
  Process Management 317
  Process Monitors 318
  Rack Manager 180, 383
  Remote Control 319
  Remote Deployment Manager 402
  Remote Session 320
  Resource Monitors 320
  restricting access to 131
  Scheduler 330
  Server Configuration Manager 192, 337
  ServeRAID Manager 393
  SNMP Agent 293
  SNMP Browser 254, 348–349
  Software Distribution 64, 355, 359, 782
  Software Rejuvenation 180
  System Accounts 367
  System Availability 180, 395
  Update Manager 63, 413–460
  UPS browser 388
  Virtualization Manager 400, 515–569
  z/VM Center 411, 571
TCP/IP ports
  BMC 60
  IBM Director 59
  management module 61–62
  RSA II 59
TCP/IP.INI file 242
TEC, CIM handler 258
telnet 104
temperature 390
threshold event filter 694
thresholds 323
ticker tape 898
tiered agents
  comparison, Agent comparison 51
timediff VB script 801
timeout parameter 206
Tivoli Enterprise Console 258
Tivoli Management Framework 25
Tivoli System Automation for Multiplatforms 70
topology.online/offline events 757
trace 748
trap forwarding 255
Triple-DES 97
troubleshooting 217
twgconw command 230
twgpccf command 223
TWGIPCCF.EXE 223
twglstsr command 224
twgmach.id file 209, 768, 772
TWGMachineID registry key 209, 772
TWGRas log 190
TWGRas log file 220
twgreset 280
twgrepair command 226
uwgreset 279
twgrestore 279
twgsave command 279
TWGServer.prop file 124
TWGType.ini file 702

U
unattended installations 54
unauthorized applications 848
unicast discovery 56, 243
uninstall 226
unique ID 767
unique identifiers 766
Update Assistant 63, 76, 357, 783
update management 31
Update Manager 413–460
  bundles 418
cleanlib command 452
commands 452
create a profile 417
dircli 452
downloading updates 421, 425
duplicate systems 431
Event Action Plans 415
events 450
example of use 417
Execution History window 427
exportprof command 459
hints 444
IBM Director Server systems 430
importup command 458
individual updates 418
inventory collection 427
inventory data 419
library 421
local repository 420
log 427
machine type
  verify 419
machine types
  adding new 447
maintenance 445
management servers 430, 435
multi-node systems 430
Not Applicable message 425
order of updates 438
overview 24
planning 63
process 414
Profile Compliance Report 428, 443
profile name 433
profiles 414–415
reboot 435
report 428
scheduler 415, 422
sequence of updates 438
ServeRAID tips 445
Software Distribution
  creating a package 432, 434
deploying packages 441
use of 415
Software Health Check 427, 442
static groups 431–432, 446
steps 417
System Pack 415
tips 444
Update Assistant comparison 63
updatePlatforms.txt file 448
updates library 420
UpdateXpress System Pack 415
using 417
wizard 417
UpdateXpress 357, 359, 407, 788
UpdateXpress packages 784, 787
UpdateXpress System Pack 63, 415
upgrades 22, 66
upward integration 32
UseExistingTarget parameter 205
user accounts 45, 116
   i5/OS special considerations 45
   LDAP 104
User Administration 126
user authority, example 798
User Editor 129–130
user guides 27, 37
user logon security 125
user profiles 126

variables 734
   data substitution variables 734
   system 914
version.key file 219
Virtual Machine Manager
   See Virtualization Manager
Virtualization Engine 23
Virtualization Manager 17, 400, 515–569
   agent component 517
   area chart 544
   bar chart 540
   chvsmauth command 567
   chvsmfarm command 568
   chvsmhost command 568
   chvsmvs command 568
   chvsmvsreg command 568
   components 517
   configuration 521
   console component 517
   dial format 540
   dircli 567
   ESX Server 518
   event actions 561
   event filters 714
   events 561
   features 516
   filters 714
   gauges 539
   groups 553
   GSX Server 519
   guest operating system 532
   health 529
   Health Summary 539
   HMC 520
   host object 532
   IBM Director Console 532
   installation 521
   line chart 543
   lsvsm command 567
   Message Browser 566
   Microsoft Virtual Server 518
   migration tasks 564
   mkvsmfarm command 567
   mkvsmmigratetask command 568
   mkvsmvs command 568
   overview 516
   planning 75
   platform manager 532, 536
   ports 522
   relationship table 546
   relationships 537
   Request Access 558
   Resource Favorites 542
   Resource Monitors 543
   resource view 546
   scatter chart 545
   server component 517
   Setup Advisor 525
   Start Vendor Software 535
   starting 523
   table view 546
   terminology 516
   Threshold Favorites 542
   thresholds 528
   topology map 546
   user interfaces 531
   virtual farm 534
   virtual server 534
   virtual server object 532
   VirtualCenter 519
   Web interface 523, 538
   Xen 516, 520
   virus test file 759
   Visual Basic script
      report of activities 807
   Visual Basic script timediff 801
   VMware ESX Server
      tasks supported 288
   voltage 390

W
   WakeOnLan parameter 206
wallpaper 207
WAN connections 212
WAV file 856
Web-based Access 26
what’s new 23

Windows
cloning scenario 766
domains 122
Event Log
security events 701
registry key 772
SNMP configuration 148
SP3 dynamic group 246
tasks supported 288
unattended installation
IBM Director 54, 203
Windows Firewall 232, 779

Windows NT Event Log
event types 719
events not logged 747, 751
WMI 12, 138

X
Xen 516

Z
z/VM Center 19, 411, 571
allocate minidisks 588
cimserver 606
cloning 669
components 572–573
connectivity 620
CRYPTO settings 586
custom user class 590
DASD pool 588
Deactivate 645
Director Agent 606
Director Agent install 609
directory prototype 586, 633
DirMaint 579–580
disk pool 623
downloads 572, 603, 606
EXTENT CONTROL file 588
FastCopy 646
hosts file entries 605
how it works 575
installation 614
IP addresses 649
key 616
license key 616
Management Access Point 573
MAP Agent 606
MAP installation 603, 613
MAPAUTH user 593
MAPSERVE user 591
Master Linux image 642
minidisk allocation 651
minidisks 588
network interfaces 604
networking properties 656
NOLOG 587
Operating System Template 639
operating systems 634
OSA devices 587
overview 572
personalization rpm 640
planning 75, 578
PORTMAP 598
process 575
provisioning 648
purchase 614
registration 634
Request Access 617
security 120
Server Complexes task 654
ShopzSeries 614
SYSTEM DTCPARMS file 598
tagged comments 581
tasks 574
templates 627, 639
tiers 654
usage 625
User ID Pattern 633
verify install 617
virtual server
creation 631
template 627
Virtual Server Deployment task 619, 626
VM Resource Manager 601
VMRM 601, 654
VMRMSVM 602
VSMERVE 594
VSWITCH 598
z9 2
zSeries 2
Implementing IBM Director 5.20
Implementing IBM Director 5.20

IBM Director is a comprehensive systems manager designed for use across the full IBM Systems server family. An integrated, easy-to-use suite of tools, IBM Director provides clients with flexible systems-management abilities to help maximize system availability and lower IT costs. With IBM Director, IT administrators can view and track the hardware configuration of remote systems and monitor the component performance of processors, disks, and memory.

This IBM Redbooks publication describes how to implement systems management with IBM Director 5.20, discussing IBM Director architecture, its adherence to industry standards, and the planning required for a solution.

This book covers how IBM Director integrates with the IBM System x service processors and the options available to deploy agents. Tasks include configuring events and alerting subsystems. The book also describes several real-life scenarios employing IBM Director.

This book helps you tailor and configure IBM Director while showing you how best to maximize your investment in IBM technology. This book is a companion to the IBM Director online publications and the product CD-ROM.

For more information: ibm.com/redbooks